Prolexic Releases DDoS Protection Infographic: What to Look for in a DDoS Mitigation Provider Portal

FORT LAUDERDALE, FL – (December 30, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a DDoS protection infographic that provides guidance for evaluating the web portals offered by DDoS mitigation providers. The infographic can be viewed and downloaded at http://www.prolexic.com/ddosportal.

"Outdated information and limited customer visibility into a vendor's DDoS mitigation efforts can increase downtime due to a DDoS attack," said Stuart Scholly, president at Prolexic. "Web portals are a strategic decision-making tool, and businesses need to be rigorous in evaluating the offerings of DDoS mitigation providers."

The DDoS mitigation portal infographic recommends that businesses focus on six key areas when evaluating a mitigation provider's web portal:

- Access from mobile devices
- Log-in security
- Data refresh rate
- Network visibility
- Real-time analytics
- DDoS forensics and intelligence

According to Scholly, a high-quality web portal should play a critical role in DDoS mitigation vendor selection and DDoS defense. "A robust DDoS defense requires the mitigation provider and customer work together in a coordinated way. When the customer can see the same network and DDoS attack data as the mitigation provider at the same time, it allows for more informed decision making and faster mitigation," he said.

Prolexic's infographic, *What to Look for in a DDoS Mitigation Provider Portal,* can be viewed and downloaded at http://www.prolexic.com/ddosportal.

To take a video tour of PLXportal, Prolexic's DDoS attack monitoring and mitigation customer portal, visit http://www.prolexic.com/plxportal.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Fort Lauderdale, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases DDoS Protection Infographic: How to Select a DDoS Mitigation Provider

FORT LAUDERDALE, FL – (December 18, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a DDoS protection infographic to help organizations choose the right DDoS mitigation service provider and DDoS protection. The infographic can be viewed and downloaded at www.prolexic.com/choose.

"DDoS attacks are now a mainstream issue and, as a result, more providers are entering the DDoS mitigation market, making it difficult for organizations to distinguish the quality of service," said Stuart Scholly, president at Prolexic. "This infographic can help businesses see through the hype and choose the best provider and level of DDoS protection for their needs."

Prolexic's DDoS protection infographic highlights a number of critical areas that organizations should evaluate when selecting a DDoS mitigation provider:

- Bandwidth capacity for DDoS mitigation
- Ability to stop multiple DDoS attacks at once
- Specialist versus generalist DDoS mitigation service providers
- A documented time-to-mitigate service level agreement (SLA)
- Flat-rate pricing for any number of attacks
- Quick access to DDoS mitigation experts
- Evidence of attack mitigation expertise
- A secure online portal

"When it comes to DDoS, organizations need to avoid surprises – like the service provider failing to mitigate the attack, lack of access to the DDoS mitigation experts, or large overage charges," said Scholly. "Following the advice in our infographic can help ensure a better DDoS customer experience."

Prolexic's DDoS protection infographic can be viewed at www.prolexic.com/choose.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Fort Lauderdale, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Hosts DDoS Survival Webcast featuring Gartner

***"How to Survive a DDoS Attack"* Defines the Latest Cyber Threats**
and Offers Best Practices for DDoS Protection

HOLLYWOOD, FL – (December 16, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today released a webcast titled, "*How to Survive a DDoS Attack,*" featuring Gartner analyst Lawrence Orans, Research Director, Prolexic President Stuart Scholly and SpaFinder Chairman and CEO Pete Ellis. Attendees can register to view the free, 30-minute webcast at www.prolexic.com/survive-ddos.

Gartner's Lawrence Orans introduces the webcast with insights into the current DDoS landscape and how DDoS attack methods have evolved during the past 12 months. He also discusses several different approaches to DDoS mitigation and explores the advantages and disadvantages of each. Orans has been with Gartner for 16 years and has more than 30 years of experience in the IT field. He assists chief information security officers and other security professionals in developing network-based strategies for mitigating security threats. His recent research notes and presentations have addressed vulnerabilities in the Internet infrastructure and how enterprises can mitigate these risks.

Prolexic President Stuart Scholly follows Orans and provides specific recommendations on how online companies can prepare for a DDoS attack. He shares best practices for taking a strong, proactive defense against DDoS and discusses several key warning signs that a website may be vulnerable to imminent attack.

"Anyone who does business on the Internet is at risk of DDoS attack, but they do not have to be victims," said Scholly. "Surviving a DDoS attack requires knowledge of the different types of DDoS threats and the motivations of cyber attackers, and most importantly, depends on having strong and proven DDoS protection in place. This webcast is a must-attend for any online business that needs a good blueprint for building a proactive DDoS defense strategy."

The webcast concludes with SpaFinder Chairman and CEO, Pete Ellis. He provides a firsthand perspective on what it is like to experience and recover from a DDoS attack. "Until SpaFinder was attacked, I never would have thought that we needed DDoS protection," Ellis said. "The proliferation of cyberattacks on all types of companies is becoming more serious. I think any company with any type of e-Commerce platform should have a dedicated DDoS mitigation service in place."

Attendees can register to view the free webcast at www.prolexic.com/survive-ddos.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

FOR IMMEDIATE RELEASE

Contacts:

Jeff Young
Media Relations
617-444-3913
jyoung@akamai.com

--or--

Tom Barth
Investor Relations
617-274-7130
tbarth@akamai.com

Akamai to Acquire Prolexic

- *Akamai aims to extend its leading Web optimization and security offerings by adding cloud-based security solutions for protecting data centers and enterprise applications*
- *Akamai to host related conference call today, December 2nd at 8:45 a.m. ET.*

CAMBRIDGE, MA and HOLLYWOOD, FL – December 2, 2013 – Akamai Technologies, Inc. (NASDAQ: AKAM) and Prolexic Technologies, Inc. announced today that the two companies have signed a definitive agreement for Akamai to acquire Prolexic, a provider of cloud-based security solutions for protecting data centers and enterprise IP applications from distributed denial of service (DDoS) attacks.

Faced with an ever-changing threat landscape, organizations require comprehensive security solutions that address many different protection scenarios. These include securing mission-critical Web properties and applications from attack, as well as protecting the full suite of enterprise IP applications – including email, file transfers, and VPN – across a data center.

Akamai provides leading solutions for defending Web sites and Web applications by leveraging the scale and intelligence of its global platform to protect against even the largest and most sophisticated DDoS and application-layer attacks. Prolexic combines DDoS mitigation solutions with security operations expertise for protecting data centers and enterprise IP applications.

By acquiring Prolexic, Akamai intends to provide customers with a comprehensive portfolio of security solutions designed to defend an enterprise's Web and IP infrastructure against application-layer, network-layer and data center attacks delivered via the Internet.

"Any company doing business on the Internet faces an evolving threat landscape of attacks aimed at disrupting operations, defacing the brand, or attempting to steal sensitive data and information," said Tom Leighton, CEO of Akamai. "By joining forces with Prolexic, we intend to combine Akamai's leading security and performance platform with Prolexic's highly-regarded DDoS mitigation solutions for data center and enterprise applications protection. We believe that Prolexic's solutions and team will help us achieve our goal of making the Internet fast, reliable, and secure."

"Today, business is defined by the availability, security and latency of Internet-facing applications, data and infrastructure," said Scott Hammack, CEO at Prolexic. "Being able to rely on one provider for Internet performance and security greatly simplifies resolution of network availability issues and offers clients clear lines of accountability. We believe that, together, we will be able to deliver an unprecedented level of network visibility and protection."

Under terms of the agreement, Akamai will acquire all of the outstanding equity of Prolexic in exchange for a net cash payment of approximately $370 million, after expected purchase price adjustments, plus the assumption of outstanding unvested options to purchase Prolexic stock. The closing of the transaction, which is subject to customary closing conditions, including regulatory approvals, is expected to occur in the first half of 2014. Therefore, Akamai's Q4 2013 existing guidance remains unchanged. The Prolexic acquisition is expected to be slightly dilutive to Akamai's Non-GAAP net income per share in the first full year post closure in the range of $0.06 to $0.08. Once the acquisition closes, the Company will include Prolexic in its guidance going forward.

Conference call scheduled today, Monday, December 2 at 8:45 a.m. ET
Akamai will host a conference call to discuss the acquisition of Prolexic today, December 2, 2013, at 8:45 a.m. Eastern time. The call may include forward-looking financial guidance from management. The call can be accessed through 1-800-706-7749 (or 1-617-614-3474 for international calls) using conference ID No. 19279933. A live Webcast of the call may be accessed at www.akamai.com in the Investor section. In addition, a replay of the call will be available for two weeks following the conference through the Akamai Website or by calling 1-888-286-8010 (or 1-617-801-6888 for international calls) and using conference ID No. 55460617.

Use of Non-GAAP Financial Measures
In addition to providing financial measurements based on generally accepted accounting principles in the United States of America (GAAP), Akamai provides additional financial metrics that are not prepared in accordance with GAAP (non-GAAP). Management uses non-GAAP financial measures, in addition to GAAP financial measures, to understand and compare operating results across accounting periods, for financial and operational decision making, for planning and forecasting purposes and to evaluate Akamai's financial performance. The non-GAAP financial measures included in this press release are Adjusted EBITDA margin and non-GAAP net income per share.

Management believes that the use of non-GAAP financial measures allows for meaningful comparisons and analysis of trends in the business, as they exclude expenses and gains that may be infrequent, unusual in nature and not reflective of Akamai's ongoing operating results. Management also believes that non-GAAP financial measures provide useful information to investors in understanding and evaluating Akamai's operating results and future prospects in the same manner as used by management and in comparing financial results across accounting periods and to those of peer companies.

The non-GAAP financial measures do not replace the presentation of Akamai's GAAP financial results and should only be used as a supplement to, not as a substitute for, Akamai's financial results presented in accordance with GAAP. Akamai has not provided a reconciliation of each non-GAAP financial measure used in this press release to the most directly comparable GAAP financial measure because it is not practicable to do so at this time.

Akamai's definitions of the non-GAAP financial measures used in this press release are outlined below:

- **Non-GAAP net income** – GAAP net income adjusted for the following tax-effected items: amortization of acquired intangible assets; stock-based compensation; amortization of capitalized stock-based compensation; restructuring charges; acquisition related costs; certain gains and losses on investments; gains and other activity related to divestiture of a business; loss on early extinguishment of debt; gains and losses on legal settlements and other non-recurring or unusual items that may arise from time to time.

- **Non-GAAP net income per share** – Non-GAAP net income divided by the basic weighted average or diluted common shares outstanding used in GAAP net income per share calculations.

- **Adjusted EBITDA** – GAAP net income excluding the following items: interest; income taxes; depreciation and amortization of tangible and intangible assets; stock-based compensation; amortization of capitalized stock-based compensation; restructuring charges; acquisition related costs; certain gains and losses on investments; gains, losses and other activity related to divestiture of a business; foreign exchange gains and losses; loss on early extinguishment of debt; gains and losses on legal settlements and other non-recurring or unusual items that may arise from time to time.

- **Adjusted EBITDA margin** – Adjusted EBITDA stated as a percentage of revenue.

The non-GAAP adjustments, and Akamai's basis for excluding them from non-GAAP financial measures, are outlined below:

- **Amortization of acquired intangible assets** – Akamai has incurred amortization of intangible assets, included in its GAAP financial statements, related to various acquisitions the Company has made. The amount of an acquisition's purchase price allocated to intangible assets and term of its related amortization can vary significantly and are unique to each acquisition. Therefore, Akamai excludes amortization of acquired intangible assets to provide investors with a consistent basis for comparing pre- and post-acquisition operating results.

- **Stock-based compensation and amortization of capitalized stock-based compensation** – Although stock-based compensation is an important aspect of the compensation to Akamai's employees and executives, the expense varies with changes in the stock price and market conditions at the time of grant, varying valuation methodologies, subjective assumptions and the variety of award types. This makes the comparison of Akamai's current financial results to previous and future periods difficult to interpret. Therefore, Akamai believes it is useful to exclude stock-based compensation and amortization of capitalized stock-based compensation in order to better understand the performance of Akamai's core business performance and to be consistent with the way the investors evaluate its performance and comparison of its operating results to peer companies.

- **Restructuring charges** – Akamai has incurred restructuring charges, included in its GAAP financial statements, primarily due to workforce reductions and estimated costs of exiting facility lease commitments. Akamai excludes these items when evaluating its continuing business performance as such items are not consistently recurring, do not reflect expected future operating expense, nor provide meaningful insight into the current and past operations of its business.

- **Acquisition related costs** – Acquisition related costs include transaction fees, due diligence costs and other one-time direct costs associated with strategic activities. In addition, subsequent adjustments to the Company's initial estimated amount of contingent consideration associated with specific acquisitions are included within acquisition related costs. These amounts are impacted by the timing and size of the acquisitions. Akamai excludes acquisition related costs and benefits to provide a useful comparison of the Company's operating results to prior periods and to its peer companies because such amounts vary significantly based on magnitude of its acquisition transactions.

- **Gain and other activity related to divestiture of a business** – Akamai recognized a gain and other activity associated with the divestiture of its Advertising Decision Solutions business. Akamai excludes gains and other activity related to divestiture of a business because sales of this nature occur infrequently and are not considered part of the Company's core business operations.

- **Income tax-effect of non-GAAP adjustments** – The non-GAAP adjustments described above are reported on a pre-tax basis. The income tax effect of non-GAAP adjustments is the difference between GAAP and non-GAAP income tax expense. Non-GAAP income tax expense is computed on non-GAAP pre-tax income (GAAP pre-tax income adjusted for non-GAAP adjustments) and excludes certain discrete tax items (such as recording or release of valuation allowances), if any. Akamai believes that applying the non-GAAP adjustments and their related income tax effect allows the Company to more properly reflect the income attributable to its core operations.

About Prolexic
Prolexic is one of the largest, most trusted Distributed Denial of Service (DDoS) mitigation providers in the world. Designed to absorb large and complex attacks, Prolexic aims to restore mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Some of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as a leading cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about Prolexic, please visit www.prolexic.com and @Prolexic on Twitter.

About Akamai
Akamai® is the leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the Company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

# # #

The release contains information about future expectations, plans and prospects of Akamai's management that constitute forward-looking statements for purposes of the safe harbor provisions under The Private Securities Litigation Reform Act of 1995, including statements about expected benefits to Akamai from the acquisition. Actual results may differ materially from those indicated by these forward-looking statements as a result of various important factors including, but not limited to, inability to successfully integrate the technology and personnel of Prolexic, failure to achieve expected post-closing margins or revenue contributions, inability to develop products based on the technology, failure of the parties to secure regulatory approvals of the transaction, and other factors that are discussed in the Company's Annual Report on Form 10-K, quarterly reports on Form 10-Q, and other documents periodically filed with the SEC.

In addition, the statements in this press release or conference call represent Akamai's expectations and beliefs as of the date of this press release. Akamai anticipates that subsequent events and developments may cause these expectations and beliefs to change. However, while Akamai may elect to update these forward-looking statements at some point in the future, it specifically disclaims any obligation to do so. These forward-looking statements should not be relied upon as representing Akamai's expectations or beliefs as of any date subsequent to the date of this press release.

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Video Provides Insights into DDoS Mitigation

Explains DDoS attack and protection basics, from the experts

HOLLYWOOD, FL – (November 25, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today released a new video that offers an overview of DDoS attacks and the DDoS threat landscape, as well as a guided tour of Prolexic's industry-leading approach to DDoS mitigation.

"As the DDoS threat grows increasingly widespread, it is becoming critical for business leaders in every industry to educate themselves about DDoS attacks. If a business relies on the Internet to communicate, to market itself, or to provide goods and services to their customers, then it needs to be prepared for DDoS attacks," said Scott Hammack, CEO of Prolexic.

"This video clearly illustrates the DDoS threat and how Prolexic fights back against DDoS attacks, successfully, on a daily basis," he added.

In less than six minutes, *Fighting Back Against DDoS Attacks* provides a helpful overview of DDoS attacks the DDoS protection service provided by Prolexic, the largest and most trusted DDoS mitigation service provider.

It answers the questions:

- What is a DDoS attack?
- Why are DDoS attacks such a threat?
- Who is responsible for DDoS attacks?
- What is the financial impact of DDoS attacks?
- How have DDoS attacks evolved?
- How does Prolexic fight back against DDoS attacks?

Fighting Back Against DDoS Attacks can be viewed at: http://bit.ly/1dwtcrR

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic’s Scott Hammack Named CEO of the Year by Camden Partners

HOLLYWOOD, FL – (November 21, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that Prolexic’s Chief Executive Officer, Scott Hammack, was honored as 2013 CEO of the Year by Camden Partners, a private equity firm and Prolexic investor.

Hammack is the seventh chief executive officer to receive the CEO of the Year award, which Camden Partners established in 2007 to recognize the outstanding accomplishments of CEOs at companies within the Camden investment management portfolio. As the 2013 recipient, Hammack was recognized for his success in best executing Camden’s investment thesis and growth strategy through his leadership over the past 12-18 months at Prolexic.

“All of our partners were in agreement that Scott Hammack has assembled a great team at Prolexic and has led the company in revolutionizing the future of cyber security,” said Jason R. Tagler, managing member, Camden Partners. “We were impressed by Scott’s strong leadership, especially as Prolexic attained organic growth on top of the successful execution of its growth strategy over the past 12 months. Camden Partners is pleased to add Scott Hammack’s name to our roster of whom we consider to be the nation’s most successful and innovative chief executives.”

Scott Hammack joined Prolexic in 2011 and brings a wealth of experience managing and growing start-up and publicly held companies. Most recently he was CEO of e-dmz, which was acquired by Quest Software in 2011. Previously, he has served as CEO of Cyberguard Corporation, which was acquired by Secure Computing in 2005, and CEO of MasterChart, Inc., which was purchased by Allscripts in 2001. He is a graduate of Northwestern University with a degree in biomedical engineering.

"I am honored and humbled to be chosen,” said Scott Hammack, CEO at Prolexic. “While my name is on the award, it reflects the incredible dedication and hard work of the entire senior management team and all our employees.”

About Camden Partners

Camden Partners, founded in 1995, operates private equity funds that provide growth capital to emerging companies in the technology-enabled Business Services, Healthcare and Education sectors. For more information, please go to: www.camdenpartners.com

###

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Survey Results for DDoS Protection Services:
What Really Matters to e-Commerce Companies

HOLLYWOOD, FL – (November 20, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today the results of a survey of global e-Commerce companies who were asked about DDoS protection and the effectiveness of different types of DDoS mitigation services. The industry report, *DDoS Protection Services: What Really Matters to e-Commerce Companies,* is available at www.prolexic.com/ecommerce-report.

A cross-section of retail companies with e-Commerce websites participated in the survey, spanning many business sectors, including consumer electronics, healthcare, online payment processing, fashion and apparel, toys and gifts, heating and plumbing, and software-as-a-service. The respondents, a statistically significant subset of Prolexic customers, included online retailers from the United States, Europe and Asia.

“There was a nearly unanimous belief among respondents that their company websites are at mid-to-high risk of being targeted by DDoS attacks over the next 12 months,” said Stuart Scholly, president at Prolexic. “Moreover, the majority of respondents indicated DDoS mitigation services from ISPs and content delivery networks were ineffective in providing the preferred level of protection e-Commerce companies require and expect.”

Key findings

Survey responses show that online retailers:

- Find content delivery networks (CDNs) and Internet service providers (ISPs) to be the least effective of DDoS protection services, and especially ineffective against direct-to-origin DDoS attacks and application-layer attacks.
  - ISPs were ranked least effective for mitigating DDoS attacks by 42 percent of respondents, while 8 percent ranked ISPs as most effective.
  - CDNs were ranked least effective for mitigating DDoS attacks by 58 percent of respondents. No respondents ranked CDNs as most effective.
  - On-site DDoS mitigation appliances were ranked least effective by 33 percent of respondents. No respondents ranked appliances as most effective.
- Prefer a mature, pure-play DDoS mitigation service provider with proven competence and capabilities that can scale to stop the largest DDoS attacks on the Internet, with low false positives, and the fastest mitigation backed by a service level agreement (SLA).

They also want a mitigation provider with a proven track record of ensuring the client's site availability and business continuity during a DDoS attack.

- Seek a total DDoS protection solution that only a specialist in DDoS mitigation services can provide. e-Commerce companies want network protection for all IPs with a single DDoS mitigation solution, not add-on services from multiple ISPs or CDNs. They want a total-protection provider that sits in front of all IPs and carriers and provides routed protection against all avenues of attacks.

A complimentary copy of Prolexic's report, *DDoS Protection Services: What Really Matters to e-Commerce Companies*, can be downloaded from prolexic.com/ecommerce-report.

Prolexic has also made available an e-commerce white paper, Safeguarding e-Commerce Revenues from DDoS Attacks in Q4, and an e-Commerce DDoS protection infographic.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Infographic Details how to Safeguard Q4 e-Commerce Revenues from DDoS Attacks

HOLLYWOOD, FL – (November 19, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a new DDoS infographic illustrating how retailers can protect their websites and safeguard revenues from cyber attacks this holiday season. The infographic can be viewed and downloaded at www.prolexic.com/safeguardrevenues.

Safeguarding e-Commerce Revenues from DDoS Attacks this Holiday Season
4 warning signs your website could be targeted
Others in your industry have been attacked. Pay attention!
Hackers sometimes announce their targets on social media sites. Monitor!
You receive an extortion or blackmail attempt. Don't ignore!
Your network has experience undiagnosed problems. Investigate!
4 ways to ensure Q4 site availability
Learn how different types of DDoS threats can affect your IT infrastructure.
Keep up with trends in DDoS attack signatures and toolkits.
Have a single source for DDoS mitigation services.
Make DDoS part of your disaster recovery plan.
Follow these tips and you're likely to have a happy – and prosperous – online holiday shopping season.
+1 (954) 620 6005
www.prolexic.com
PROLEXIC
DDoS Attacks End Here.

According to Prolexic's quarterly global ddos attack reports, Q4 is typically one of the most active quarters for DDoS attacks. Because DDoS perpetrators attempt to cause the most financial damage and disruption, the number of cyber attacks directed against e-Commerce websites tends to peak during the critical Q4 sales period.

Prolexic's infographic highlights four key warning signs that can indicate an e-Commerce attack is imminent. It also provides these recommendations for retailers to follow to help maximize website availability during the holiday shopping season:

- Closely monitor social media sites and blogs. Hackers love to brag about their exploits and sometimes announce which industry or company they plan to target next. In addition, inflammatory or controversial messages posted on your corporate websites and blogs could motivate hacktivist groups to target your website – or you could even become the victim of a disgruntled employee or customer.
- Don't ignore an extortion or blackmail attempt, even if you don't plan on paying the ransom. Alert IT and your DDoS mitigation service provider and take all threats seriously.
- Learn how different types of DDoS threats can affect different elements of your network and implement a DDoS mitigation service that will protect all of them.
- Keep up with trends in DDoS attack signatures and toolkits. Prolexic has a wealth of information and threat reports at prolexic.com.

"The emergence of easy-to-use DDoS toolkits makes it simple for malicious actors to launch DDoS attacks – using computers or even mobile apps," said Stuart Scholly, president at Prolexic. "This makes it urgent that in Q4, all online retailers take the threat of DDoS attack seriously."

The infographic can be viewed and downloaded at www.prolexic.com/safeguardrevenues.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Infographic Explains the How and Why of Distributed Reflection Denial of Service (DrDoS) Attacks

HOLLYWOOD, FL – (November 18, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a new infographic that provides an overview of Distributed Reflection Denial of Service (DrDoS) attacks, an increasing cyber threat. The infographic can be viewed and downloaded at www.prolexic.com/reflection.

According to Prolexic's Q3 2013 Global DDoS Attack Report, the use of reflection attacks is increasing rapidly. Based on data gathered from attacks against Prolexic's global client base, reflection attacks increased 265 percent over Q3 2012 and 70 percent over Q2 2013. This can be explained by the increase in misconfigured servers worldwide and the ease with which perpetrators can now obtain lists of IP addresses and misconfigured servers from underground Internet communities. In addition, DrDoS attacks provide the benefits of obscuring the source of the attack (providing anonymity), while enabling the bandwidth of intermediary victims to be used, often unknowingly, to multiply the size of the attack (amplification).

"Reflection attacks need to be on everyone's radar," said Stuart Scholly, president of Prolexic. "Our goal in developing this infographic was to simplify this somewhat complex subject matter and raise awareness of reflection attacks so IT and security communities can take proactive action."

The infographic explains how DrDoS attacks impact both intermediaries (victims) and websites (targets), as well as why this attack type is gaining popularity. It also identifies six industries where DrDoS attacks have been most commonly used and offers recommendations that organizations can take to reduce their risk. Prolexic's latest infographic can be viewed and downloaded at www.prolexic.com/reflection.

The Prolexic Security Engineering and Response Team (PLXsert) has also published a series of white papers that analyze reflection and amplification DDoS attacks. The four types of DrDoS attacks covered are:

- DNS
- SNMP/NTP/CHARGEN
- SYN
- Gaming server attacks

The white paper series details real-world case studies of DrDoS attacks observed by PLXsert through the Prolexic global DDoS mitigation network and can be downloaded at www.prolexic.com/drdos.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Advises Against a Multi-Layered Strategy to Block DDoS Attacks

HOLLYWOOD, FL – (November 14, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today it has published a new executive series white paper that alerts businesses of the pitfalls of a multi-layered network security approach for blocking denial of service attacks. The paper can be downloaded from www.prolexic.com/block-ddos.

“Experience has shown that the more layers of security, appliances and providers involved in mitigation, the longer it takes to block a DDoS attack,” said Stuart Scholly, president of Prolexic. "There are too many possible weak links in a multi-layered approach that increase the risk of website downtime rather than reduce it. That is why Prolexic recommends a ‘single, strongest defense’ strategy to block DDoS attacks.”

The free Prolexic white paper, *Why a Multi-Layered Security Strategy is Not Ideal for DDoS Mitigation*, examines the common types of cyber security measures and the DDoS attack variants that can easily penetrate them. Prolexic states a strong case for switching from the industry norm to a single, strongest DDoS defense as the best way to achieve the fastest mitigation, block DDoS attacks, and minimize downtime.

The white paper will help executive-level and IT management gain a better understanding of:

- The broad impact of lengthy DDoS-driven site outages

- How complex DDoS variants can topple firewalls, routers, on-premise appliances, self-hosted DNS servers, and other traditional cyber security measures

- Why multiple layers of security devices and vendors can actually delay DDoS mitigation

The Prolexic white paper also includes a case study that provides a real-world example of a financial firm, whose multi-layered cyber security defense failed to block a complex DDoS attack, resulting in serious financial losses due to lengthy downtime. In contrast, a second case study illustrates the benefits of having a specialist DDoS mitigation service in place as a first responder to a DDoS attack.

The free white paper, *Why a Multi-Layered Security Strategy is Not Ideal for DDoS Mitigation,* can be downloaded for a limited time at www.prolexic.com/block-ddos.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases New Infographic Explaining DDoS Attack and Defense Strategies

HOLLYWOOD, FL – (November 6, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced it has released a new infographic that illustrates common DDoS attack and defense strategies.

"While DDoS is a technical subject, it cannot be ignored by any organization that conducts business online," said Stuart Scholly, president of Prolexic. "It's important that businesses discuss DDoS and plan proactively. We hope this infographic will help start that conversation."

<insert thumbnail of infographic>

The infographic shows the typical motivations behind DDoS attacks, how perpetrators select their target, identify weaknesses, and use tools to launch their attack. It also contrasts Prolexic's approach to DDoS defense with those of Internet Service Providers (ISPs), telcos, and Content Delivery Networks (CDNs).

According to Prolexic's latest Q3 2013 Global DDoS Attack Report, DDoS activity around the world remains high and shows no sign of declining. Q3 2013 set a record for the number of attacks directed against Prolexic's global client base. Compared to Q3 2012, the total number of attacks increased 58 percent. The total number of infrastructure attacks increased 48 percent, while the total number of application attacks (Layer 7) increased by 101 percent compared to one year ago.

Prolexic's DDoS Attacks and Defense infographic can be viewed and downloaded at www.prolexic.com/attackdefense.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Shares DDoS Infographic to Highlight Gaming Websites in Denial of Service Attacks

HOLLYWOOD, FL – (October 25, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today shared a DDoS infographic that highlights the problem of attackers leveraging vulnerable multi-player gaming servers in reflection and amplification (DrDoS) attacks. Gaming websites are often targeted by DDoS attackers or hijacked for use in DrDoS attacks against other businesses.

Each day more than a hundred million people play an online video game, but the gaming servers they use are often insecure and misconfigured, making the servers easy-to-use by criminals and hackers to launch powerful denial of service attacks, including DrDoS attacks.

For more details, the full infographic, *Target acquired: Gaming website,* is available at http://bit.ly/1blUFXD. To learn more about about the prominence of denial of service attacks involving online gaming communities and the repercussions of DrDoS attacks to online gaming infrastructures, read the white paper, *An Analysis of DrDoS and DDoS Attacks Involving the Multiplayer Video Gaming Community*.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

DDoS Perpetrators Changed Tactics in Q3 2013 to Amplify Attack Sizes and Hide Identities

Can now use smaller botnets to launch high-bandwidth attacks

HOLLYWOOD, FL – (October 23, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today reported that DDoS perpetrators changed tactics in Q3 2013 to boost attack sizes and hide their identities. This observation is one of many key findings found in the company's *Q3 2013 Global DDoS Attack Report*, which was published today, and can be downloaded from www.prolexic.com/attackreports.

"This quarter, the major concern is that reflection attacks are accelerating dramatically, increasing 265 percent over Q3 2012 and up 70 percent over Q2," said Stuart Scholly, president of Prolexic. "The bottom line is that DDoS attackers have found an easier, more efficient way to launch high bandwidth attacks with smaller botnets and that's concerning."

Attackers are flocking to so-called distributed reflection denial of service (DrDoS) attacks as they provide the benefit of obscuring the source of the attack (anonymity), while enabling the bandwidth of intermediary victims to be used, often unknowingly, to multiply the size of the attack (amplification). In DrDos attacks, there are always two victims, the intended target and the intermediary.

Prolexic's latest report reveals that the total number of attacks against its clients in Q3 2013 remained high and represented the highest total for one quarter. This occurrence illustrates a consistently heightened level of DDoS activity around the world over the last six months. Of note, more than 62 percent of Q3 DDoS attacks originated from China, far surpassing all other countries. Findings are based on data gathered from attacks launched during the quarter against Prolexic's global client base.

For the quarter, peak bandwidth averaged 3.06 Gbps and peak packets-per-second (pps) averaged 4.22 Mpps. The largest attack Prolexic mitigated during Q3 was directed at a European media company, peaking at 120 Gbps.

Summary highlights from Prolexic's *Q3 2013 Global DDoS Attack Report*

Compared to Q2 2013

- 1.58 percent increase in total DDOS attacks
- 6 percent decrease in application layer (Layer 7) attacks
- 4 percent increase in infrastructure (Layer 3 & 4) attacks
- 44 percent decrease in the average attack duration: 21.33 hours vs. 38 hours

Compared to Q3 2012

- 58 percent increase in total DDOS attacks
- 101 percent increase in application layer (Layer 7) attacks
- 48 percent increase in infrastructure (Layer 3 & 4) attacks
- 12.3 percent increase in the average attack duration: 21.33 hours vs. 19 hours

Analysis and emerging trends

Prolexic data for Q3 2013 shows a 70 percent increase in reflection attacks (DNS and CHARGEN) over the previous quarter and a 265 percent increase over the same quarter last year. This rise in DrDoS attacks should come as no surprise, as attack methods that inflict high damage with low effort will always be popular.

"DrDoS attacks don't require as many bots because the amplification factor is so large," explained Scholly. "Because less outbound bot traffic is needed, the botnet can be much smaller. This makes it easier for these botnets to fly under the radar unless you know what to look for."

Prolexic has closely monitored DrDoS attacks for the last 12 months and has correctly forecasted their increasing popularity, as discussed in a series of four white papers on this resurfacing attack methodology.

"Q3 data also shows that infrastructure attacks maintained their share of total attacks, but within this group there was a big jump in UDP attacks and a corresponding drop in SYN attacks," said Scholly. "Combined with the rise in reflection attacks, this quarter showed a significant shift in attack methodologies that all businesses should be aware of."

Prolexic's latest attack report includes a detailed analysis of the trend toward reflection attacks, *DrDoS reflection services within the underground marketplace*. The analysis examines DrDoS attack methods, tools and services – specifically CHARGEN attacks being integrated into the DDoS threatscape – and provides steps for remediating CHARGEN attacks.

A complimentary copy of Prolexic's *Q3 2013 Global DDoS Attack Report* is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q4 2013 report will be released early in the first quarter of 2014.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Protects OnCourse Systems for Education and its SaaS Applications against DDoS Attacks

HOLLYWOOD, FL – (October 10, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that OnCourse Systems for Education (https://oncoursesystems.com), a provider of software-as-a-service (SaaS) K-12 applications, has selected its PLXproxy DDoS mitigation service. OnCourse applications are used by schools and school districts in 40 U.S. states, and its website has tens of thousands of visitors daily.

OnCourse engaged Prolexic after three denial of service attacks earlier this year. UDP floods hit the company's website at 8 a.m. on weekdays just as the school day was getting underway for OnCourse's school district customers. Approximately four hours of downtime resulted from each attack, affecting the availability of attendance tracking, grading, student information, discipline tracking, and other SaaS applications.

After two DDoS mitigation service providers failed to prevent and stop these attacks, the company engaged Prolexic's emergency DDoS mitigation service. The cyber attackers abandoned their efforts as soon as they detected OnCourse was routing traffic through Prolexic's 1.5 Tbps cloud-based DDoS mitigation platform. OnCourse has not come under a DDoS attack since becoming a Prolexic client.

"OnCourse has learned from experience that there is no rhyme or reason to the motives of cyber attackers," said Stuart Scholly, president at Prolexic. "That is why DDoS protection and a well-rehearsed DDoS response plan are essential for every company that has an online presence, regardless of industry or size."

Prior to working with Prolexic, OnCourse had no visibility into the source of the malicious traffic and which attack vectors were being used. Other DDoS mitigation providers could not provide attack forensics, which OnCourse could have used to build a defense against future attacks. Now, as a Prolexic customer, OnCourse has access to deep network analytics and DDoS attack forensics through PLXportal. PLXportal is a secure online resource that gives Prolexic customers a real-time view of what is happening on their network and Prolexic's DDoS mitigation infrastructure before, during and after a denial of service attack.

"Like many companies, we thought that we would not be a target of a DDoS attack," said Mark Yelcick, chief technology officer and partner at OnCourse Systems for Education. "We have learned that firewalls and intrusion protection systems are not enough to be completely protected against DDoS. We simply cannot afford downtime brought about by a DDoS attack. That's why we chose Prolexic for DDoS protection."

To learn more, download the full OnCourse Systems for Education case study from www.prolexic.com/oncourse.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com and follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Wins Gold for Security Service Innovations at 2013 Golden Bridge Awards

PLXabm application-based monitoring solution for SSL is recognized

HOLLYWOOD, FL – (October 3, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it is the Gold Winner in the Security Service Innovations category at the 2013 Golden Bridge Awards for PLXabm SSL, Prolexic's application-based DDoS attack monitoring solution for Secure Sockets Layer (SSL) encrypted traffic.

PLXabm SSL adds a hardware security module (HSM) to Prolexic's PLXabm appliance, which resides at a customer site and provides 24/7 visibility into application layer (Layer 7) DDoS attacks. PLXabm solves the challenge of identifying and analyzing encrypted Layer 7 attacks while maintaining the security of the customer's SSL keys. As a result, Prolexic can identify and isolate attacking bots faster, allowing for faster mitigation of encrypted DDoS attacks.

The PLXabm SSL module is compliant with FIPS-140-2 Level 2 key management standards and provides a secure way to decrypt SSL traffic so that the PLXabm appliance can be used for SSL attack detection and analysis. The decryption of traffic is performed in hardware on the HSM, but the SSL keys are always under the customer's control.

"It's an honor to be named a Gold winner and to be recognized for Prolexic's innovation in security services," said Stuart Scholly, president at Prolexic. "An increasing number of enterprises have to comply with stringent privacy and security regulations, and PLXabm SSL makes that possible in the arena of DDoS monitoring."

More than 40 judges representing a broad spectrum of industry voices from around the world participated and their average scores determined who would receive the 2013 Golden Bridge Business and Innovation Awards. The winners were honored at a dinner and presentation on September 30, 2013, in San Francisco attended by the finalists, industry leaders and judges.

About the Golden Bridge Awards

Golden Bridge Awards are an annual industry and peers recognition program honoring Best Companies of all types and sizes. The Golden Bridge Business Awards honor and generate industry-wide recognition of the achievements and positive contributions of organizations and businesses worldwide in every major industry. Learn more at www.goldenbridgeawards.com.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Successfully Completes SOC 1 and SOC 2 Examinations

Demonstrates Controls Relevant to Security, Confidentiality, Financial Reporting and Data Security

HOLLYWOOD, FL – (October 1, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has successfully completed its Type 2 SOC 1 examination, commonly referred to as SSAE (Statement on Standards for Attestation Engagements) 16, and its Type 2 SOC 2 examination, formally known as a *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.* Prolexic also simultaneously completed the ISAE 3402 examination, which is the international equivalent of SSAE 16.

"Prolexic continues to assure customers of the integrity of our internal processes by submitting to these examinations," said Stuart Scholly, president at Prolexic. "By proving that Prolexic adheres to these stringent security standards, we make it easier for companies with strict compliance regulations to work with us and adopt our DDoS protection solutions."

SSAE 16 is a standard issued by the American Institute of Certified Public Accountants (AICPA). Prolexic successfully completed an SSAE 16 examination, formally known as a *Reporting on Controls at a Service Organization* (SOC 1). The examination was performed by BrightLine CPAs & Associates, Inc., an independent CPA firm, for the distributed denial of services attack mitigation services offered by Prolexic. This exam covered the review period of August 1, 2012, to July 31, 2013.

SOC 2 is also a standard issued by the American Institute of Certified Public Accountants (AICPA). Prolexic successfully completed a Type 2 SOC 2 examination, formally known as *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. Prolexic was examined under the selected SOC 2 principles of security and confidentiality. Meeting this standard shows Prolexic is protected against unauthorized access, both physical and logical, and shows that the company protects confidential information as committed or agreed. The Type 2 SOC 2 covered the review period of August 1, 2012, to July 31, 2013.

About SSAE 16

SSAE No. 16, *Reporting on Controls at a Service Organization* (AICPA, Professional Standards, AT sec. 801) is an attestation standard that establishes the requirements and guidance for reporting on controls at a service organization relevant to user entities' internal control over financial reporting. The controls addressed in SSAE No. 16 are those that a service organization implements to prevent, or detect and correct, errors or omissions in the information it provided to user entities.

SSAE No. 16 superseded the SAS 70 audit standard in mid-2011. It is the adopted version of the International Standards for Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, for use in the United States.

About SOC 2

SOC 2, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, is an attestation report on controls at a service organization relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed for user entities. Type 2 SOC 2 reports focus on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls. SOC 2 examinations may only be performed by a licensed CPA firm.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Enhances PLXportal with Expanded Real-Time Views of DDoS and Network Activity

HOLLYWOOD, FL – (September 26, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has introduced a number of enhancements to its customer gateway, PLXportal. These include an expanded user dashboard, additional real-time views of network activity, new views of global DDoS threat intelligence, and optimization for viewing on tablets, smartphones and other mobile devices.

PLXportal is a secure online resource that gives Prolexic customers a real-time view of what is happening on their network and Prolexic's DDoS mitigation network before, during, and after a denial of service attack. Prolexic customers can also access real-time and near real-time DDoS intelligence and alerts provided by the Prolexic Security Engineering and Response Team (PLXsert). There is also a robust set of account management tools, including a secure wizard to upload SSL encryption keys to Prolexic for encrypted Layer 7 DDoS attack mitigation.

"This latest iteration of PLXportal provides our customers with the broadest and deepest attack forensics and network data in the industry that is updated in real-time, which is unprecedented," said Stuart Scholly, president at Prolexic. "Because of this unique level of visibility, we can work more efficiently with our clients to detect and mitigate DDoS attacks faster."

PLXportal highlights

Using PXLportal, customers can quickly gain a big picture view of network activity and anomalies that may indicate DDoS, as well as drill down to view hundreds of metrics. This latest version provides a more holistic view of network health and access to a broader range of alert types from multiple monitoring points.

Prolexic customers can use PLXportal's new attack timeline analytics to improve their preparedness for future DDoS incidents. After an attack has been mitigated, Prolexic customers can analyze and view the individual events as they occurred to understand the scale of the DDoS attack and network impact. For example, data can be used to analyze attack vectors and identify network vulnerabilities.

Other highlights of PLXportal include:

Enhanced dashboard

- Watch all of the customer's traffic as it traverses Prolexic's network, in a single view

- Manage traffic information, alerts, tickets, and events in a comprehensive view with an intuitive interactive timeline space
- Filter information to their desired level of detail to best understand the composition and timing of traffic

Optimized views for mobile devices

- PLXportal can be accessed and viewed anywhere there is Internet access – on a tablet, smartphone, touch screen device or on any computer browser

New intelligence

- Access the latest DDoS threat information compiled by PLXsert
- View attack traffic distribution and attacker behavior globally from PLXpatrol, which is updated throughout the day, every day

New PLXabm analytics view

- Upload and deploy certificates and keys securely using the new SSL Manager
- Gain a more holistic view of application based monitoring with a new mapping display, advance filtering, and advanced searching

These enhancements build upon the existing features of PLXportal, which include:

- Views of real-time HTTP and HTTPS request patterns for live traffic
- Unified, timeline of changes associated with external sensors, monitoring, attacks and configurations
- Attack reports
- Security Operations Center (SOC) alerts
- Prolexic DDoS mitigation service configuration information
- Downloadable logs and stats
- Client-specific support information
- An online ticketing system for requests

“Seconds count when defending against DDoS attacks,” Scholly said. “That’s why Prolexic is committed to continually updating PLXportal with additional views and more granular DDoS threat data that is far beyond what other mitigation providers can offer.”

View a video and learn more at www.prolexic.com/plxportal.

About Prolexic

Prolexic Technologies is the world’s largest, most trusted Distributed Denial of Service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, and follow us on LinkedIn, Facebook, Google+ and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Selected by Arab National Bank for DDoS Mitigation After Outscoring Other Providers in Service Evaluation

HOLLYWOOD, FL – (September 25, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that Arab National Bank (ANB), a commercial bank serving more than 2 million customers across Saudi Arabia, has selected its 24/7 monitoring and mitigation services to protect the bank's online banking and e-trading websites.

ANB selected Prolexic after evaluating several local and global DDoS mitigation service providers and their capabilities. Prolexic scored highest in ANB's list of 18 technical and service requirements, which included:

- DDoS protection to cover all types of DDoS attacks and methods
- Activation either on-demand or always-on
- Low latency that will not significantly impact site performance
- No impact on legitimate business traffic when DDoS protection is on
- DDoS mitigation of both national and international traffic

"Arab National Bank is aware of the risk of DDoS in the financial services sector and has taken proactive action to minimize its impact," said Stuart Scholly, president at Prolexic. "More than 10 of the world's largest banks trust Prolexic for DDoS protection, and we are delighted to welcome Arab National Bank to our global financial services client base."

"Prolexic could give us 24/7 monitoring plus the bandwidth capacity and flexibility to route both national and international traffic through its global scrubbing centers," said Head of Information Security at Arab National Bank, Alrebdi Al Rebdi. "That, plus a time-to-mitigate SLA, gave us the confidence that Prolexic could protect ANB against DDoS."

Prolexic's PLXrouted service met ANB's criteria for providing maximum protection against the broadest range of DDoS attack types and sustained high-bandwidth attacks. PLXrouted is offered as a flexible, asymmetric, on-demand service and enables Prolexic customers to easily activate protection for an entire subnet by redirecting Internet traffic to the Prolexic network during a DDoS attack and routing off of the Prolexic network during non-attack periods. Prolexic's DDoS protection service for ANB also includes 24/7 monitoring by Prolexic's Security Operations Center (SOC). ANB also works with a local Prolexic global partner, Cyberia, which provides dedicated engineers to provide local support. ANB has not come under DDoS attack since PLXrouted was implemented.

"Financial services firms must educate themselves on the different types of DDoS attacks, because most people do not completely understand the huge impact they can have on our business," said ITG-Head of Telecoms at Arab National Bank, Jamil M. Barakat. "As we have learned at ANB, it is critically important to have a good and reliable DDoS mitigation solution in place."

To learn more, download the full ANB DDoS case study at www.prolexic.com/anb.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Shares Best Practices for Protecting e-Commerce Sites against Q4 DDoS Attacks

DDoS Threat Highest During Retailers' Critical Q4 Sales Period

HOLLYWOOD, FL – (September 19, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has released a number of best practices that firms operating e-Commerce websites can implement to reduce the impact of cyber attacks.

In a new Executive Series white paper, "*Safeguarding e-Commerce Revenues from DDoS Attacks in Q4,"* Prolexic advises online retailers to be on high alert for DDoS attacks in Q4. Extended site downtime and the resulting inability to make sales and process online orders during the holiday shopping period, including Black Friday and Cyber Monday, can significantly jeopardize Q4 revenues for e-tailers.

Prolexic expects DDoS attacks against e-Commerce sites to increase in size and intensity this fourth quarter, based on previous attack events noted in the company's "*Q4 2012 Quarterly Global DDoS Attack Report."* In Q4 last year, the most active quarter of the year, Prolexic mitigated attacks that reached more than 50 Gbps directed against clients in e-Commerce, financial services and SaaS markets. The average attack duration was 32.2 hours, a crippling duration in e-Commerce.

"Past experience shows that online retailers must take seriously the increased threat of DDoS and other cyber-attacks during the holiday shopping season," said Stuart Scholly, president of Prolexic. "Online shoppers have many options, and if they can't readily conduct business with you, they will quickly turn to competitors instead. This white paper offers insight about the current DDoS threat landscape and provides a clear blueprint for building a stronger DDoS defense, so you can avoid downtime and support sales."

This executive series white paper addresses the escalating cyber threats targeting e-Commerce sites and recommends best practices for protecting online retailers against loss of sales and revenue, damaged brand reputation, and reduced customer confidence due to DDoS. Prolexic also reveals key warning signs that a website could be targeted for a denial of service attack and concludes with best practice recommendations for making DDoS mitigation a part of a disaster recovery plan. The white paper is available to the public at www.prolexic.com/safeguarding.

The white paper also provides a link to PLXplanner, Prolexic's free, online DDoS protection and planning tool. PLXplanner helps e-Commerce sites understand their vulnerabilities for a denial of service attack, as well as provides recommendations on how to strengthen their DDoS defense. PLXplanner is available at www.prolexic.com/plxplanner.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Reveals the Tainted World of Multiplayer Video Games and Denial of Service Attacks

Gaming communities provide fertile ground for DrDoS attacks against financial services, fellow players

HOLLYWOOD, FL – (Sept. 10, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today detailed the rampant problem of denial of service attacks within and from online gaming communities. The DDoS attacks, which can pack a powerful punch by the use of reflection and amplification (DrDoS) techniques, have been used against other gamers, gaming platforms and even third party targets such as financial services and other non-gaming businesses.

The availability and accessibility of online gaming infrastructures and devices creates opportunities for malicious actors to launch DDoS attacks and steal login credentials. Denial of service attacks have a long tradition in the community, occur frequently and keep evolving.

“DDoS attacks fueled by rivalries, poor password security protocols and readily available DDoS tools are widespread and harm gaming and non-gaming targets alike,” said Stuart Scholly, president of Prolexic. “There are serious repercussions for every industry from denial of service attacks that feed off the explosive growth of online gaming infrastructures.”

A Prolexic customer in the financial industry was the target of a DrDoS attack that reached 5 Gbps and made use of misconfigured game servers as intermediary victims to reflect and amplify network traffic to the financial services target, in an effort to stop it with a DDoS attack.

As is common in DrDoS attacks, the malicious actors increased the power of their DDoS attack against the financial services firm with reflection and amplification techniques. Sending a small request to one gaming server produced an outsized response that was five times larger than the initial request. The attackers co-opted hundreds of gaming servers to produce the same outsized response at once, and repeatedly, against the targeted financial services firm.

The attack was stopped by Prolexic’s DDoS mitigation service.

“This attack targeted Call of Duty 2 gaming servers across the globe – in South Africa, Europe, Asia and the United States,” explained Scholly. “PLXsert has replicated the attack in our lab.”

In the white paper, the culminating piece in a series explaining DrDoS attacks, the Prolexic Security Engineering & Response Team (PLXsert) explains:

- Why DDoS attacks occur in online gaming communities
- The history of DrDoS attacks in online gaming
- DrDoS attack tools that use gaming servers – including Quake, Half Life, and Call of Duty – to attack non-gaming targets
- A case study of a DrDoS attack against a financial services firm
- The underground market for stressors, booters and other DDoS-as-a-Service tools that target online gaming communities

The white paper, the concluding piece in Prolexic's DrDoS series, is available free of charge at www.prolexic.com/gaming.

The laboratory-created proof-of-concept attack script will be available to the public on the official PLXsert GitHub page located at http://www.github.com/plxsert.

About the Prolexic Security Engineering & Response Team (PLXsert)
PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's DDoS mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's most recent Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic
Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com and follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Issues Warning: Growing Trend in Fraud, Identity Theft Being Camouflaged by DDoS Attacks

Threat advisory exposes DDoS attack signatures from the Drive Toolkit; issues alert to fraud departments

HOLLYWOOD, FL – (August 28, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today shared attack signatures and details that are helpful to detect and stop DDoS attacks from the Drive DDoS toolkit, an attack tool often used as a source of distraction while criminals break into customer accounts at finance firms and e-Commerce businesses.

DDoS attacks from the Drive DDoS toolkit and other variants of the Dirt Jumper toolkit can sidetrack IT security personnel while criminals attempt to transfer funds out of bank accounts, gather passwords for later use, or place unauthorized orders. Because attacks from this criminal DDoS toolkit are associated with identity theft, recognizing the Drive toolkit as the source of a DDoS attack can lead financial institutions, banking, insurance, investment firms, brokerages or e-Commerce firms to suspect and investigate possible fraudulent access of customer accounts that may have occurred during the attack.

“During the confusion of a DDoS attack, malicious actors can break into the financial and e-Commerce accounts of customers without being noticed,” warned Stuart Scholly, President at Prolexic. “IT departments are typically so focused on the damage caused by the DDoS attack that they don’t realize it may merely be a planned distraction while criminals loot customer accounts.”

New signatures, communication patterns

The Drive toolkit, which is being leaked in underground hacking forums, has been the source of multiple recent DDoS attacks observed by the Prolexic Security Engineering and Response Team (PLXsert). The tool is a newer variant of the Dirt Jumper family of DDoS toolkits, one of the most popular denial of service attack tools in use today.

“In recent weeks, Prolexic has detected, stopped and mitigated DDoS attacks launched against our clients from the Drive DDoS toolkit,” said Scholly. “Although these attacks are cousins to Dirt Jumper DDoS toolkit, they have new signatures and communication patterns. In all cases, Prolexic mitigated attacks from the new toolkit in minutes, as promised in our service level agreement.”

Attacks target Web applications

Six types of DDoS attacks are built into the Drive toolkit, allowing attackers to launch a variety DDoS attacks. The tool features GET floods, POST floods, POST2 floods, IP floods and IP2 floods directed at the application layer as well as UDP floods, which target network infrastructure. Encryption allows malicious actors to hide their identities.

"Companies often don't realize they are under attack from the Drive toolkit, because application attacks increase server utilization without excessive network traffic," Scholly added. "The information in the threat advisory can help detect these attacks quickly."

DDoS threat advisory

An analysis of the Drive threat, including screenshots, launch commands, sample payloads and identifying signatures to enable DDoS mitigation techniques, is available free of charge in Prolexic's *Drive DDoS Threat Advisory* at http://www.prolexic.com/drive-ddos.

Prolexic Threat Advisories

Designed to provide early warnings of new or modified DDoS attack signatures and scripts recently observed by PLXsert, threat advisories contains descriptions of the type of attack, attack signatures, and the network infrastructure or application that it targets. In addition, Prolexic's DDoS mitigation experts also offer insight into the nature of each type of attack and provide warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXsert also provides tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them. The latest threat advisories, including itsoknoproblembro and Pandora, are available to the public at www.prolexic.com/threatadvisories.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com and follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic's SSL Key Sharing Tools Keep Customers in Control

Enables short-term key certificates to fight encrypted DDoS attacks, Compliant with key management standards

HOLLYWOOD, FL – (August 27, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that its secure socket layer (SSL) key sharing tools allow customers to maintain control of their SSL keys at all times, while making it easier for Prolexic to detect and stop encrypted Layer 7 (application layer) DDoS attacks. The SSL key sharing tools are provided with the Prolexic Application-Based Monitoring (PLXabm) service and PLXproxy, Prolexic's on-demand, symmetric DDoS mitigation service.

"Malicious actors are employing more sophisticated attack techniques, and as a result we anticipate the frequency of encrypted Layer 7 DDoS attacks will rise," said Stuart Scholly, president at Prolexic. "It is especially challenging to stop DDoS attacks in encrypted flows, because they can only be examined using a customer's encryption key."

Monitoring encrypted traffic with PLXabm SSL Hardware Security Module

An encrypted Layer 7 DDoS attack is detected and analyzed by examining packet headers, which require a customer's unique SSL key to unlock. For quicker and easier DDoS analysis and detection, Prolexic developed the PLXabm SSL Hardware Security Module. Compliant with FIPS-140-2 Level 2 key management standards, the SSL Hardware Security Module facilitates decryption of SSL traffic bi-directionally and enables automated alerting when a DDoS attack is detected.

"This enhancement to PLXabm allows our engineers to identify and isolate the source IP address, which they can use to block encrypted Layer 7 attacks," said Scholly. "Best of all, this approach ensures that our customers can maintain control over their SSL keys at all times."

Stopping DDoS attacks in encrypted traffic with PLXproxy

Prolexic can mitigate encrypted DDoS attacks using its PLXproxy service once the customer's SSL keys and certificates are uploaded and deployed to Prolexic. Customers can elect to have these items stored securely for reuse or to provide temporary certificates and keys that are revoked after an encrypted DDoS attack is stopped. To aid in this process, PLXproxy SSL Manager, a secure and efficient way to upload SSL keys and certificates, can be accessed through the PLXportal, an online resource devoted to giving Prolexic customers greater visibility into their Prolexic DDoS mitigation services and activity.

For additional details, please visit the Prolexic DDoS Protection Services at http://www.prolexic.com/services-dos-and-ddos-protection.html to download data sheets on Prolexic's SSL capabilities, the PLXabm monitoring service and the PLXproxy mitigation service.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming, energy and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com and follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic DDoS Protection Service Stops Attackers from Bringing Down 1ink.com e-Commerce Sites

HOLLYWOOD, FL – (August 13, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that 1ink.com has selected Prolexic's DDoS mitigation service to protect its network of e-Commerce sites. 1ink.com is a leading online retailer of high-quality replacement inkjet and laser toner cartridges.

The 1ink.com network was hit with the first of three DDoS distributed denial of service attacks that grew in size and complexity. The first DDoS attack brought down www.101inks.com, one of the smaller 1ink.com e-Commerce sites, for more than a day. During that time, they routed traffic from 101inks.com to their other domains in an attempt to mitigate the attack.

To stop the DDoS attack, Roland Davoudikia, chief executive officer of 1ink.com, selected Prolexic from among several DDoS mitigation services he had researched. Prolexic mitigated the attack within 5 minutes, as outlined in Prolexic's industry-leading service level agreement (SLA).

"We concluded from our post-attack forensic analysis that it is likely the 1ink.com websites were mistakenly targeted," said Stuart Scholly, president of Prolexic. "This illustrates that even random events can have significant financial impact on a business if some level of DDoS mitigation is not in place."

Later in the year, the company's main e-Commerce site at www.1ink.com was hit with another attack – a combination SYN and DNS flood that peaked at 70 Gbps. As expected, this denial of service attack did not bring down the site, because Prolexic's PLXproxy DDoS protection service was already in place. Five days later, the DDoS attackers struck again, and once again Prolexic was able to quickly detect and mitigate the attack without any action from 1ink.com.

"Having Prolexic's DDoS mitigation service is like having insurance against DDoS attacks, and as a result, these last two attacks did not have any effect on our business," said Davoudikia. "There was the potential to lose hundreds of thousands of dollars in online sales each day, along with collateral damage to our partner relationships. Fortunately, none of that happened. I can't imagine running my business without DDoS attack protection from Prolexic."

To learn more, download the 1ink.com DDoS case study at www.prolexic.com/1ink.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com and follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Organizations Can Build a Stronger DDoS Defense Using Real-Time Data Analysis

Deploy a faster, better DDoS response with real-time analytics, mitigation appliances and experienced mitigation engineers

HOLLYWOOD, FL – (July 30, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today released recommendations on using real-time analytics as a powerful tool for identifying denial of service attacks and other cyber threats, risks and events.

Prolexic recommends that the information gleaned from real-time data analytics is the best foundation for a DDoS mitigation strategy that supports root-cause analysis of how a denial of service attack could affect an Internet-facing network. Potential targets are application logins, system performance (latency), network systems and mission-critical applications. Prolexic advises that DDoS mitigation providers and their customers can work more effectively by extracting intelligence from massive streams of data to determine the best response to the DDoS attack, resulting in faster mitigation and less risk of costly downtime.

"Today, every industry is deluged with data from multiple sources in different formats, and the business of cyber security and DDoS attack mitigation is no exception," said Stuart Scholly, president of Prolexic. "Prolexic has learned that these 'big data' streams are valuable for DDoS mitigation only if data analytics are used to gain real-time insight into the trends, behaviors and events that make up today's cyber-attack landscape. Most importantly, using real-time data analytics drives faster cyber threat identification and mitigation, and consequently helps Internet-facing organizations build a stronger cyber security strategy."

Prolexic also advises that even the best automated data analytics systems cannot replace the experience of skilled DDoS and cyber threat mitigation technicians, who analyze and extrapolate the data to make meaningful conclusions. In Prolexic's experience, the best data analytics strategy to support fast and effective DDoS mitigation is a combination of an automated data correlation and reasoning system, coupled with the human expertise of engineers and technicians with front-line success in fighting and defeating DDoS attackers.

The benefits of using real-time analytics tools for faster DDoS denial of service mitigation are discussed in detail in the white paper, "*Data Analytics and DDoS Mitigation: Lessons Learned*." The white paper explains:

- What Prolexic has learned about effectively managing data for DDoS mitigation
- How to make data relevant in real time to support faster DDoS mitigation

- How to leverage attack data analytics to provide meaningful snapshots that are easy to interpret by DDoS mitigation engineers and customers alike
- Why today's data analytics systems complement, rather than replace, the skills of experienced live mitigation engineers

The *"Data Analytics and DDoS Mitigation: Lessons Learned*" white paper can be downloaded from www.prolexic.com/ddosanalytics.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Technologies Secures US$30 Million Series C Financing Led by Trident Capital & Intel Capital

HOLLYWOOD, FL – (July 25, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, announced today it has closed a US$30 million Series C funding round led by new investors Trident Capital and Intel Capital. Prolexic's existing shareholders include Kennet Partners, Camden Partners and Medina Capital.

This latest round of financing comes at a time when Prolexic's year-over-year revenues have increased 65 percent, while remaining EBITDA positive.

Following the Series C investment, Trident Capital's Managing Director Gustavo Alberelli will join Prolexic's Board of Directors. "For the past two years, I have seen companies and government agencies around the world repeatedly select Prolexic for DDoS protection, cementing the firm's position as market leader," said Alberelli. "I'm excited to continue working with Prolexic management and providing Trident's IT security expertise to help Prolexic continue its rapid expansion."

The Series C financing comes in the aftermath of two of the largest DDoS attacks ever seen in the industry. So far in 2013, Prolexic has successfully mitigated the single largest attack in its 10-year history (167 Gigabits per second), as well as the world's most powerful attack campaign (144 million packets per second). To keep pace with bigger, stronger and more sophisticated attacks, Prolexic will use the new funding to expand its worldwide scrubbing center footprint, increasing the capacity of its cloud-based DDoS mitigation platform beyond 1 Tbps, and to develop new cloud-based security services. Prolexic currently operates four scrubbing centers located in London, Hong Kong, San Jose and Ashburn, Va.

"We are pleased to partner with seasoned security investors like Trident Capital and Intel Capital," said Scott Hammack, chief executive officer of Prolexic. "With this additional funding, we will be able to accelerate a number of strategic initiatives as we continue to expand our portfolio of cloud-based products and industry-leading DDoS protection services."

About Prolexic

Prolexic is the world’s largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow them on LinkedIn, Facebook , Google+ , YouTube , and @Prolexic on Twitter.

About Trident Capital

Founded in 1993, Trident Capital invests primarily in growth equity together with select investments in venture. Since its inception, Trident has raised nearly US$2 billion across seven funds and invested in more than 170 companies throughout the Software, Internet and Business Services sectors. Notable Trident investments in the IT Security market include: AirTight Networks, Alienvault, Arxan, HyTrust, Mocana, Neohapsis, Qualys (Nasdaq: QLYS), Solera Networks (acquired by Blue Coat), Sygate (acquired by Symantec), Tablus (acquired by EMC), Thor Technologies (acquired by Oracle), Tricipher (acquired by VMWare), and Voltage Security. Trident is headquartered in Palo Alto, California. For additional information, visit www.tridentcap.com.

About Intel Capital

Intel Capital, Intel's global investment and M&A organization, makes equity investments in innovative technology start-ups and companies worldwide. Intel Capital invests in a broad range of companies offering hardware, software, and services targeting enterprise, mobility, health, consumer Internet, digital media and semiconductor manufacturing. Since 1991, Intel Capital has invested more than US$10.9 billion in over 1,294 companies in 54 countries. In that timeframe, 202 portfolio companies have gone public on various exchanges around the world and 324 were acquired or participated in a merger. In 2012, Intel Capital invested US$352 million in 150 investments with approximately 57 percent of funds invested outside North America. For more information on Intel Capital and its differentiated advantages, visit www.intelcapital.com or follow @Intelcapital.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Average Packet-Per-Second and Attack Bandwidth Rates Rise 1,655 Percent and 925 Percent Respectively According to Prolexic's Latest DDoS Attack Report

HOLLYWOOD, FL – (July 17, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that the average packet-per-second (pps) rate reached 47.4 Mpps and the average bandwidth reached 49.24 Gbps based on data collected in Q2 2013 from DDoS attacks launched against its global client base. These metrics, representing increases of 1,655 percent and 925 percent respectively compared to Q2 2012, are just two of many findings contained in the company's ***Quarterly Global DDoS Attack Report***, which was published today.

"This quarter we logged increases for all major DDoS attack metrics, and some have been significant. DDoS attacks are getting bigger, stronger and longer," said Stuart Scholly, president at Prolexic. "We believe this growth is being fueled by the increasing prevalence of compromised Joomla and WordPress web servers in increasingly large botnets."

In Q1 2013, Prolexic recorded an average DDoS attack bandwidth of 48.25 Gbps, an all-time high since the company began issuing quarterly attack reports in Q3 2011. This second quarter, average bandwidth ticked even higher to 49.24 Gbps, representing a 2 percent increase over Q1 2013 and a 925 percent increase over Q2 2012. In addition, average packet-per-second volume reached 47.4 Mpps this quarter, a dramatic 46 percent increase over the 32.4 Mpps that was logged just last quarter. Compared to Q2 2012, the average packet-per-second rate has increased 1,655 percent.

After trending down in 2011 and part of 2012, average attack durations are increasing, rising from 17 hours in Q1 2012 and 34.5 hours in Q1 2013, to 38 hours this quarter.

"Attack durations are likely increasing because perpetrators are less concerned about detection and protecting their botnets," said Scholly. "The widespread availability of compromised web servers makes it much easier for malicious actors to replenish, grow and redeploy botnets. Traditionally, botnets have been built from compromised clients. This requires malware distribution via PCs and virus infections, and takes considerable time and effort. Consequently, attackers wanted to protect their client-based botnets and were more fearful of detection, so we saw shorter attack durations."

Summary highlights from Prolexic's *Q2 2013 Global DDoS Attack Report*

Compared to Q2 2012

- 33 percent increase in total number of DDoS attacks
- 23 percent increase in total number of infrastructure (Layer 3 & 4) attacks
- 79 percent increase in total number of application (Layer 7) attacks
- 123 percent increase in attack duration: 38 hours vs. 17 hours
- 925 percent increase in average bandwidth
- 1,655 percent increase in average packet-per-second (pps) rate

Compared to Q1 2013

- 20 percent increase in total number of DDoS attacks
- 17 percent increase in total number of infrastructure (Layer 3 & 4) attacks
- 28 percent increase in total number of application (Layer 7) attacks
- 10 percent increase in attack duration: 38 hours vs. 34.50 hours
- 2 percent increase in average bandwidth: 49.24 Gbps vs. 48.25 Gbps
- 46 percent increase in average packet-per-second (pps) rate
- China maintains its position as the main source country for DDoS attacks.

Analysis and emerging trends

As in previous quarters, attackers predominantly used infrastructure-directed attacks (Layer 3 and Layer 4), which accounted for 74.7 percent of all attacks, with application layer attacks making up the remainder. SYN floods were the attack type of choice, accounting for nearly one-third of all attacks mitigated by Prolexic's Security Operations Center (SOC). This is the highest volume for any single attack type since Prolexic began publishing its *Quarterly Global DDoS Attack Report*. GET, ICMP and UDP floods were also frequently directed against Prolexic clients over the three-month period.

Compared to the same quarter one year ago, the total number of DDoS attacks increased 33.8 percent. In addition, the total number of infrastructure attacks increased 23.2 percent while the total number of application attacks (Layer 7) increased by 79.4 percent compared to one year ago. While the split between the total number of infrastructure attacks and application layer attacks was similar between the two quarters, both attack types increased when the two quarters were compared. Average attack durations have increased significantly, rising from 17 hours in Q2 2012 to reach 38 hours this quarter, an increase of 124 percent.

Compared to Q1 2013, the total number of attacks increased by 20 percent. This reflects a consistently high level of denial of service attack activity around the globe over the last six months. The total numbers of both infrastructure and application attacks increased over

Q1 2013 (17.4 percent and 28.9 percent respectively). Average attack duration continued to tick upwards, rising from 34.5 hours last quarter to 38 hours in Q2 2013.

April was the most active month of the quarter for DDoS attacks, accounting for 39.7 percent of all attacks, followed by May (31.6 percent) and June (28.7 percent). This quarter, two weeks tied for the most active week of the quarter: April 8-14 and April 15-21. This high level of activity can be attributed to attacks against financial services clients and the ongoing use of the itsoknoproblembro toolkit.

Data for the Q2 2013 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Q2 2013 Global DDoS Attack Report is available as a free PDF download from www.prolexic.com/attackreports. The Q3 2013 report will be released early in the fourth quarter of 2013.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

How DDoS Attackers Turn Mitigation Devices Against You

Backscatter from mitigation devices can cause collateral damage in SYN reflection attacks

HOLLYWOOD, FL – (June 26, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today shared information on a popular cyber attack technique, SYN reflection attacks, which can leverage the defense mechanisms of DDoS mitigation devices to increase the strength of the attacks.

SYN reflection attacks are one of the more sophisticated DDoS attack methods and typically require some skill to execute. However, they have recently grown in popularity as they've become available on a DDoS-as-a-Service basis via the criminal underground.

"SYN reflection attacks have been around for a long time, but new attack apps make them extremely easy to launch. Even a novice can do it," said Stuart Scholly, President of Prolexic. "Malicious actors wrap web-based graphical user interfaces around sophisticated scripts and offer them as convenient DDoS-as-a-Service apps that you can launch from your phone."

SYN reflection attacks are used against targets that support TCP – a core communication protocol that enables computers to transmit data over the Internet, such as web pages and email.

However, before data is transmitted between machines, the computers must establish a connection in the form of a multi-step handshake. If a handshake cannot be completed successfully, the computers repeatedly attempt connections. SYN reflection attacks misdirect these communication handshakes to other machines until they are overwhelmed with a flood of communication requests.

"What most people don't realize is that mitigation equipment can contribute to the problem of SYN reflection attacks," Scholly explained. "The equipment is programmed to challenge these connection requests to ensure they are legitimate. The mitigation equipment will keep challenging the request from the spoofed IP address, thus creating backscatter toward the spoofed server.

"It's an unfortunate side effect of DDoS mitigation. Some backscatter is inevitable. However, it can be overcome using more sophisticated mitigation techniques once the attack is understood to be a SYN reflection attack," Scholly explained. "At Prolexic, we actively try to minimize backscatter. This is why it is so important to do packet analysis, and not just rely on equipment alone."

SYN reflection attacks, also known as spoofed SYN attacks, are discussed in detail in a new white paper from the Prolexic Security Engineering & Response Team (PLXsert).

The white paper explains:

- Why SYN reflection attacks expand upon the damage created by SYN floods
- How misuse of the TCP handshake is used by malicious actors to confuse and slow down servers
- How DDoS mitigation equipment can contribute to the problem
- How three types of SYN reflection techniques work
- How to identify SYN reflection attacks
- How cyber criminals offer SYN reflection attacks as DDoS-as-a-Service

The white paper is the third in the Distributed Reflection Denial of Servicer (DrDoS series), and is available free of charge at www.prolexic.com/drdos.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's DDoS mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's most recent Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

DDoS Attacks Against University Federal Credit Union End with Prolexic

Prolexic's mitigation services now protects Credit Union with US$1.6 Billion in Assets

HOLLYWOOD, FL – (June 18, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that University Federal Credit Union (UFCU) in Austin, Texas, has engaged Prolexic to provide always-on DDoS mitigation services through its PLXproxy solution. UFCU is the largest, locally-owned financial institution in Austin, Texas, with branches serving over 162,000 members throughout the Austin and Galveston areas. The online banking site of UFCU (www.ufcu.org) had been brought down by two DDoS attacks before the firm engaged Prolexic.

"Credit unions need to have DDoS protection, especially in light of the huge impact to financial institutions during the Operation Ababil DDoS attacks last fall," said Stuart Scholly, president at Prolexic. "Multiple attacks on UFCU and several other credit unions over the past few months is clear evidence that DDoS perpetrators are going after this financial sector with full force."

Multiple DDoS Attacks

On January 24 of this year, DDoS attackers targeted the firm's online banking URL and IP address and took down the website for 2 hours and 36 minutes. The attack peaked at 5.4 Gbps and lasted approximately two days before being mitigated by UFCU's in-house IT resources and the credit union's Internet Service Provider (ISP). During the site downtime, UFCU members could not access online banking, apply for auto loans or download documents, thereby totally disrupting the credit union's services.

UFCU experienced a second DDoS attack on February 25, during which the online banking site was down for 4 hours and 6 minutes. Traffic peaked at 10.1 Gbps in a more sophisticated, randomized attack. The attackers' strategy employed a toolkit to flood servers with repeated PDF requests and later switch to a new attack signature that targeted UFCU's external DNS over port 53. The attack was mitigated approximately two days later with assistance from UFCU's ISP.

Successful DDoS mitigation

After provisioning the PLXproxy DDoS mitigation service, Prolexic successfully mitigated a third DDoS attack against UFCU on March 7 of this year. The online banking site did not go down and neither UFCU's IT team nor credit union members realized that a DDoS attack had even taken place due to the effective DDoS mitigation techniques employed.

"The March 7 attack had zero impact on our site thanks to DDoS protection by Prolexic," said Glen Roberts, Infrastructure and Security Manager at UFCU. "The spike on the Prolexic Dashboard got up to just 575 Mbps, but our Internet pipe is only 50 Mbps, so that's well over 10 times what we're capable of handling. The Prolexic mitigation service kicked in quickly, so there wasn't even a blip on our radar. You could tell that Prolexic was scrubbing that traffic out. That was a good win for us and Prolexic."

Recommendations for DDoS preparedness

As the number of DDoS attacks against credit unions continues to rise, the National Credit Union Administration (NCUA) has responded by recommending three key DDoS preparation strategies for credit unions:

- "Performing risk assessments to identify risks associated with DDoS attacks.
- Ensuring incident response programs include a DDoS attack scenario during testing and address activities before, during, and after an attack.
- Performing ongoing third-party due diligence, in particular on Internet and web-hosting service providers, to identify risks and implement appropriate traffic management policies and controls"[1]

Prolexic helped UFCU fulfill these recommendations by working with Roberts to create a DDoS run book. UFCU's DDoS run book contains contact information for Prolexic, for the ISP, and for other credit unions that could possibly also be under DDoS attack. It also includes an architecture diagram of the UFCU network, as well as language to be used to communicate with credit union members when an attack occurs.

"Each company has its own incident response plan, but I think that every company should also have a DDoS-specific response plan, as well," said Roberts. "After UFCU's experience with DDoS attacks, I would encourage any credit union over US$500 million in assets to seriously consider purchasing DDoS mitigation services."

To learn more, the full UFCU case study can be downloaded from www.prolexic.com/ufcu.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other

[1] NCUA Risk Alert, February 2013, www.ncua.gov/Resources/Pages/RSK2013-01.aspx

at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

About UFCU

Exceeding US$1.6 billion in assets, UFCU is Austin's largest locally-owned financial institution and serves over 162,000 members in the Austin and Galveston areas. UFCU provides a variety of products, services and education programs to meet your needs through all phases of your life. To learn more about UFCU's products and services, including low rate auto loans, visit www.ufcu.org.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Outlines the Broad Impact of DDoS Attacks across the Enterprise

Distributed Denial of Service No Longer Just an IT Issue

HOLLYWOOD, FL – (June 11, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that organizations need to rethink their DDoS defense strategies to consider the broad impact that DDoS attacks can have throughout an organization.

"DDoS is typically thought of as only an IT issue, since attackers typically target and bring down Internet-facing network elements and applications," said Stuart Scholly, president at Prolexic. "Unfortunately, DDoS has become an enterprise-wide issue with adverse effects that go far beyond IT."

Prolexic advises adopting a DDoS protection strategy that spans teams and departments across the enterprise, not just the IT department. In addition, management must be aware of the many different types of DDoS attacks and how each type affects different elements and areas of a network.

Moreover, Prolexic warns that, if left unprepared and unprotected, the impacts of a DDoS attack go beyond website downtime and potential financial loss and can include:

- **Brand reputation and customer perception** – An organization's reputation for stability and technical expertise can suffer greatly from a DDoS attack, causing potential brand damage while granting a competitive advantage to rivals.

- **Email and call centers**– When network infrastructure and routers are targeted, DDoS attacks can bring down email and customer service call centers, especially if the call center is on a voice-over-IP (VoIP) network. In this case, a DDoS attack can cut off communication with customers, partners, vendors and even employees.

- **Stock price and investor confidence** – Some companies hit by DDoS attacks have seen stock prices temporarily fall and/or experience volatile fluctuations due to investor concerns.

- **Search engine rankings** – A lengthy outage may jeopardize a website's search engine ranking, since search engine organizations do not want to route users to sites that are down or performing slowly.

"Building a proactive defense against DDoS attacks is the best way to avoid the diverse damage that these incidents can cause," Scholly said. "Prolexic recommends working with a

DDoS mitigation provider to implement a simulated DDoS attack or dry run to confirm that an enterprise is prepared. This exercise will give management a clear idea of what needs to be addressed to ensure an effective response across the enterprise when a DDoS attack strikes."

Details about the effect of DDoS attacks on non-IT departments and best practices for developing a DDoS defense are available in Prolexic's new white paper, "*The Broad Impact of DDoS: It's More Than Just an IT Issue*," available for download for a limited time at www.prolexic.com/impact.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases Free DDoS Protection Planning Tool to Help Organizations Build Stronger Defenses

PLXplanner 2.0 available now at www.prolexic.com

HOLLYWOOD, FL – (June 4, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has released a role-based version of PLXplanner, the company's free, online DDoS protection planning tool. PLXplanner is a strategic risk assessment and planning tool to help IT and security professionals build a better defense against increasingly powerful and sophisticated DDoS attacks. Based on answers entered in a role-based quiz, PLXplanner delivers strategic recommendations for improving business, technology or operational strategies to fight DDoS attacks.

"Organizations need to realize that DDoS attacks are not just a technology problem," said Stuart Scholly, president at Prolexic. "There are several dimensions to building a strong defense against these attacks. PLXplanner helps organizations focus on areas that are typically overlooked when evaluating their DDoS vulnerabilities."

Last year, Prolexic introduced the industry's most detailed DDoS Downtime Calculator. Since then Prolexic has reworked and refocused the online tool to deliver more strategic value. Renamed PLXplanner, the tool now delivers specific DDoS defense guidance and best-practice recommendations rather than bottom line numbers.

The operations planner, for example, asks questions about security architecture, application testing, monitoring capabilities, web team availability and more.

If your company already has website availability monitoring in place, PLXplanner will recommend including synthetic transactions, such a login to a test account. Why? Because an attacker can target back-end databases via HTTP application attacks (such as a POST attack). In that case, the website may appear to be online even though users cannot log in.

"PLXplanner 2.0 is a much deeper, more valuable tool. Our detailed recommendations reflect the user's unique IT and networking environment, customized to their role and responsibilities. This makes it more relevant and valuable for users at every level of the organization," added Scholly.

PLXplanner is available at www.prolexic.com/plxplanner.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Stops Largest Ever DNS Reflection DDoS Attack

167 Gbps Attack Targets Real-Time Financial Exchange Platform

HOLLYWOOD, FL – (May 30, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has successfully mitigated the largest DNS reflection attack ever recorded, which peaked at 167 Gigabits per second (Gbps). The attack, the largest single DDoS attack Prolexic has mitigated in its 10-year history, was directed against a real-time financial exchange platform on May 27, 2013.

"This was a massive attack that made up in brute force what it lacked in sophistication," said Scott Hammack, chief executive officer at Prolexic. "Because of the proactive DDoS defense strategies Prolexic had put in place with this client, no malicious traffic reached its website and downtime was avoided. In fact, the company wasn't aware it was under attack."

The DDoS mitigation for this attack was distributed across Prolexic's four cloud-based scrubbing centers in Hong Kong, London, San Jose and Ashburn, Va. Prolexic's London-based scrubbing center mitigated the majority of the malicious traffic, which peaked at 90 Gbps.

The DNS Reflection Denial of Service (DrDoS) technique exploits security weaknesses in the Domain Name System (DNS) Internet protocol.

In this type of DNS reflection attack, an attacker makes many spoofed queries to many public DNS servers. The source IP address is forged to appear as the target of the attack. When a DNS server receives the forged request it replies, but the reply is directed to the forged source address. This is the reflection component. The target of the attack receives replies from all the DNS servers that are used. This type of attack makes it very difficult to identify the malicious sources. If the queries (which are small packets) generate larger responses, then the attack is said to have an amplifying characteristic.

Prolexic's digital forensics confirmed that 92 percent of the machines participating in the attack were open DNS resolvers, sourcing from port 53, which represented a malformed DNS response.

In March, Prolexic authored a white paper on DNS reflection attacks highlighting their increasing usage and illustrating how the DNS protocol can be exploited by cyber attackers. The white paper can be downloaded free of charge at www.prolexic.com/drdos. In addition, Prolexic's ***Q1 Global DDoS Attack Report*** featured an in-depth case study on the technique.

"It's only a matter of time, possibly by the end of this quarter, before the 200 Gbps marker is crossed," said Hammack. "To keep pace with increasing attack sizes, Prolexic is continuing to build out its 800 Gbps DDoS mitigation infrastructure and by the end of the year, we will have approximately 1.2 Tbps of bandwidth on tap."

Regardless of attack size, Prolexic recommends that all organizations proactively validate their DDoS mitigation service to minimize downtime. Best practices and guidance can be found in Prolexic's latest white paper, *"Planning for and Validating a DDoS Defense Strategy,"* which can be downloaded for a limited time from www.prolexic.com/planning.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, *Google+* , *YouTube* , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Gets Clickpoint! Media Back Online Quickly After Layer 4 SYN Flood DDoS Attack Campaign

HOLLYWOOD, FL – (May 21, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that Clickpoint! Media has chosen Prolexic as its DDoS mitigation services provider for multiple websites across its media services network. Clickpoint! offers a network of media services designed to help marketing and advertising organizations optimize their campaigns for greater return on investment, increased web traffic and heightened brand awareness.

Recently, Clickpoint! suffered a Layer 4 SYN flood that started out at 80 to 100 Mbps and quickly became a series of distributed denial of service attacks that increased to 800 Mbps. The company's websites experienced downtime of approximately four hours, twice a day, over the course of a week. During these downtime periods, Clickpoint! could not provide an important part of its media service and customer account access was limited. Clickpoint! engaged Prolexic for DDoS mitigation services after previous efforts failed to mitigate the series of attacks that were escalating in size and complexity.

"Online businesses like Clickpoint! that rely so heavily on the Internet for day-to-day business operations are especially susceptible to DDoS attacks," said Stuart Scholly, president at Prolexic. "Because attacks are continuing to increase in size and complexity, they are outgrowing the level of protection that hardware appliances, ISPs, telcos, and content delivery networks typically provide."

Prolexic's DDoS mitigation engineers in the Prolexic Security Operations Center (SOC) brought all Clickpoint! sites up within minutes after routing traffic through Prolexic's global scrubbing centers. Using a combination of advanced proprietary techniques, equipment, and live monitoring best practices, Prolexic's engineers were able to quickly develop and launch countermeasures to block the changing attack vectors. Prolexic also provided real-time attack metrics on the origin of the attacks – Turkey and Romania – as well as other metrics that Clickpoint! can use to build a stronger DDoS defense with Prolexic as the cornerstone.

"No one is safe from DDoS and other types of cyber attacks," said Roberto Siano, CEO and founder of Clickpoint! Media. "With Prolexic's protection against DDoS in place, Clickpoint! can give our marketing and advertising customers absolute confidence that the critical media services they rely on will always be available and accessible."

To learn more, the full Clickpoint! Media case study can be downloaded from www.prolexic.com/clickpoint.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

PLXabm DDoS Detection Solution Wins Multiple Awards From *Network Products Guide*

HOLLYWOOD, FL – (May 14, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that PLXabm won one gold and two bronze awards from the *Network Products Guide*, the industry's leading technology research and advisory guide.

Prolexic's application-based monitoring solution, PLXabm, is the first and only managed monitoring service that takes an in-depth analytical approach to combating application layer (Layer 7) DDoS attacks. By tracking 25 unique dimensions, PLXabm makes it possible to monitor and identify the sophisticated Layer 7 abuses and fraudulent activities that cause the greatest impact to online businesses.

Because PLXabm has both a service and hardware component, it was entered into and secured awards in multiple categories:

- **Gold Winner –** Best IT Services
- **Bronze Winner –** Security Hardware
- **Bronze Winner –** Security Services

Winners of 8th Annual 2013 Hot Companies and Best Products Awards were announced on May 7, 2013 in Las Vegas.

"We are pleased that the DDoS protection innovations developed at Prolexic are getting wider recognition," said Stuart Scholly, president and Prolexic. "With PLXabm, our technicians can identify and analyze malicious Layer 7 traffic – and its variants in randomized attacks – easier and faster than ever before. As such, PLXabm delivers a platform for a level of forensic analysis the DDoS mitigation industry has never seen before."

Prolexic's on-premise PLXabm appliance collects and sends data back to Prolexic's Security Operations Center (SOC) where alerts and forensic sets are created. Armed with this information, Prolexic's SOC can pinpoint the precise nature of an attack in minutes.

PLXabm is available as a subscription service as part of Prolexic's DDoS monitoring solution portfolio. For more information on PLXabm, please visit: http://www.prolexic.com/pdf/PLXabmdatasheet.pdf

About Network Products Guide Awards

As industry's leading technology research and advisory publication, Network Products Guide plays a vital role in keeping decision makers and end-users informed of the choices they can make in all areas of information technology. You will discover a wealth of information and tools in this guide including the best products and services, roadmaps, industry directions, technology advancements and independent product evaluations that facilitate in making the most pertinent technology decisions impacting business and personal goals. The guide follows conscientious research methodologies developed and enhanced by industry experts. To learn more, visit www.networkproductsguide.com.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:

Michael E. Donner

SVP, Chief Marketing Officer

Prolexic

media@prolexic.com

+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Issues Recommendations for Validating DDoS Defenses

HOLLYWOOD, FL – (May 14, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has issued a number of recommendations that organizations can use to validate their DDoS defenses, as well as protection services they receive from mitigation providers.

"Making sure a provider can actually deliver on the level of service it promises is a critical step that many organizations overlook," said Stuart Scholly, president at Prolexic. "Mitigation failure is such a common problem that the majority of Prolexic clients came to us after the DDoS protection they had in place did not work."

Prolexic recommends that organizations work closely with their DDoS mitigation provider(s) to complete a professional, planned provisioning and service validation. The only way to be sure that DDoS protection will be effective is through proactive validation against different types of attack scenarios.

Prolexic recommends the following best practices for DDoS mitigation service testing and validation:

- With the DDoS mitigation service active, verify that all applications are performing properly.
- Verify that all routing and DNS is working.
- In partnership with your mitigation service provider, generate a few gigabits of controlled traffic to validate the alerting, activation and mitigation features of the service.
- Test small levels of traffic without scrubbing and without any DDoS protection to validate that your on-premise monitoring systems are functioning correctly. This action will also help you identify the stress points on your network.
- Conduct baseline testing and calibrate systems to remediate any network vulnerabilities.
- Schedule validation tests on a regular basis (yearly or quarterly) with your DDoS mitigation service provider to validate that the service configuration is still working correctly – and eliminate the risk of network element failures due to DDoS. If network issues arise during testing, your service provider may need to make

modifications based on recent changes to your network, such as modified firewall rules, firmware updates and router reconfiguration.

“Based on the test results, Prolexic also recommends developing a mitigation playbook as part of an incident response plan,” said Scholly. “This helps ensure that everyone in the organization knows what to do and what to expect if an attack strikes.”

Additional DDoS service validation recommendations and guidance on how to develop a DDoS mitigation playbook can be found in Prolexic’s latest white paper, "*Planning for and Validating a DDoS Defense,"* which can be downloaded for a limited time from www.prolexic.com/planning.

About Prolexic

Prolexic is the world’s largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Tracks More Than 47 Million DDoS Attack Bots Worldwide; Public Portal Now Available at www.prolexic.com/plxpatrol

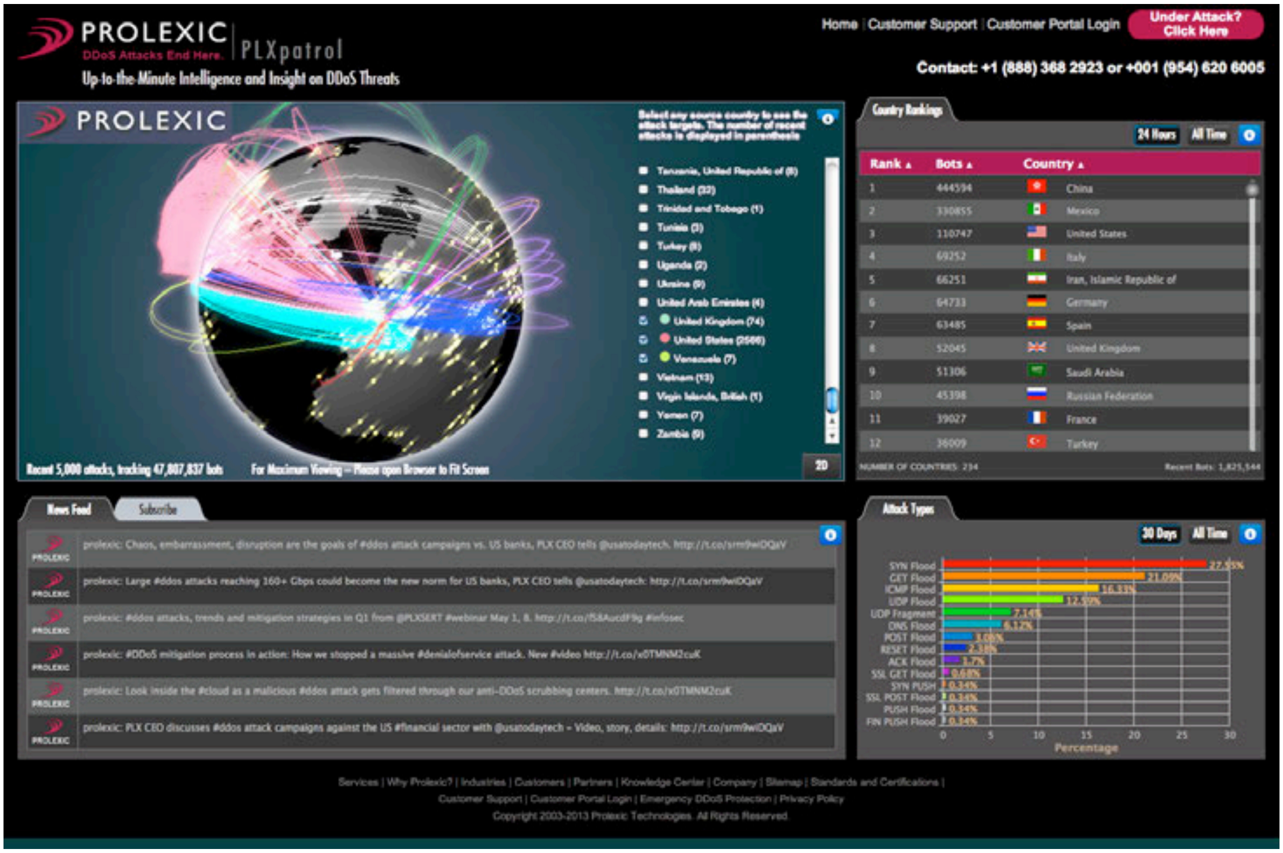
HOLLYWOOD, FL – (May 7, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it tracks more than 47 million bots in its global IP reputational database. Each time a bot is used in a DDoS attack against a Prolexic client, the bot's IP address and location are logged and tracked. Information on the number of bots, along with trend details on attack types and attack locations is now available in PLXpatrol, the company's free public DDoS attack portal, at www.prolexic.com/plxpatrol.

Since its launch in Q4 2012, PLXpatrol has been providing up-to-the-minute intelligence and insight on DDoS threats to the world's IT and security community. The information presented in PLXpatrol is sourced from Prolexic's analytical and IP reputational databases.

"Version 2.0 builds on the very successful launch of PLXpatrol and provides more views and more data," said Stuart Scholly, president at Prolexic. "With this free tool, users have the ability to drill down and get deeper insight on DDoS attacks, both historically and in near real-time."

The first release of PLXpatrol included an Attack Tracker, showing where DDoS attacks directed against Prolexic's clients were originating from and geographic locations of targets (anonymized). Additional views included Country Ranking (last 24 hours) and Country Ranking (All Time). Key additions in PLXpatrol 2.0 include:

- **Attack Tracker** (Enhancement) – This tool has been enhanced with an optional three-dimensional view of attacks sources and destinations, along with details on the number of recent attacks originating in each country



PROLEXIC DDoS Attacks End Here. | PLXpatrol

Up-to-the-Minute Intelligence and Insight on DDoS Threats

Home | Customer Support | Customer Portal Login | Under Attack? Click Here

Contact: +1 (888) 368 2923 or +001 (954) 620 6005

PROLEXIC

Select any source country to see the attack targets. The number of recent attacks is displayed in parenthesis

- ■ Tanzania, United Republic of (8)
- ■ Thailand (32)
- ■ Trinidad and Tobago (1)
- ■ Tunisia (3)
- ■ Turkey (8)
- ■ Uganda (2)
- ■ Ukraine (9)
- ■ United Arab Emirates (4)
- ☑ ● United Kingdom (74)
- ☑ ● United States (2566)
- ☑ ● Venezuela (7)
- ■ Vietnam (13)
- ■ Virgin Islands, British (1)
- ■ Yemen (7)
- ■ Zambia (9)

2D

Recent 5,000 attacks, tracking 47,807,837 bots   For Maximum Viewing – Please open Browser to Fit Screen

Country Rankings   24 Hours | All Time

Rank ▴	Bots ▴	Country ▴
1	444594	China
2	330855	Mexico
3	110747	United States
4	69252	Italy
5	66251	Iran, Islamic Republic of
6	64733	Germany
7	63485	Spain
8	52045	United Kingdom
9	51306	Saudi Arabia
10	45398	Russian Federation
11	39027	France
12	36009	Turkey

NUMBER OF COUNTRIES: 234   Recent Bots: 1,825,544

News Feed | Subscribe

prolexic: Chaos, embarrassment, disruption are the goals of #ddos attack campaigns vs. US banks, PLX CEO tells @usatodaytech. http://t.co/srm9wiDQaV

prolexic: Large #ddos attacks reaching 160+ Gbps could become the new norm for US banks, PLX CEO tells @usatodaytech: http://t.co/srm9wiDQaV

prolexic: #ddos attacks, trends and mitigation strategies in Q1 from @PLXSERT #webinar May 1, 8. http://t.co/f58AucdF9g #infosec

prolexic: #DDoS mitigation process in action: How we stopped a massive #denialofservice attack. New #video http://t.co/x0TMNM2cuK

prolexic: Look inside the #cloud as a malicious #ddos attack gets filtered through our anti-DDoS scrubbing centers. http://t.co/x0TMNM2cuK

prolexic: PLX CEO discusses #ddos attack campaigns against the US #financial sector with @usatodaytech - Video, story, details: http://t.co/srm9wiDQaV

Attack Types   30 Days | All Time

Services | Why Prolexic? | Industries | Customers | Partners | Knowledge Center | Company | Sitemap | Standards and Certifications |
Customer Support | Customer Portal Login | Emergency DDoS Protection | Privacy Policy
Copyright 2003-2013 Prolexic Technologies. All Rights Reserved.

- **Attack Types** (New Feature) – This new tool shows the most common attack vectors being used in DDoS attacks over the last 30 days and all-time (since Prolexic has been tracking attack types).

"Prolexic is sitting on a wealth of Big Data DDoS threat and Internet Protocol intelligence," said Scholly. "We are sharing this insight with the global IT and security community through PLXpatrol and will continue to build out the tool as the year progresses."

PLXpatrol 2.0 can be used for free at www.prolexic.com/plxpatrol.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia.

To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, *Google+* , *YouTube* , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Printers, Routers and Other Internet Devices Being Hijacked to Participate in DrDoS Cyber Attacks

New Prolexic white paper explains how to secure your devices and infrastructure from SNMP, NTP and CHARGEN attacks

HOLLYWOOD, FL – (April 30, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that Distributed Reflection and Amplification Denial of Service (DrDoS) attacks have grown increasingly popular with malicious actors as the number of vulnerable network appliances and servers has grown.

While DrDoS attack tactics have been used successfully for more than a decade, their popularity and effectiveness has increased during the past year. Specific DrDoS attacks target IP-based devices – printers, cameras, routers, hubs, sensors and other network devices – to take advantage of inherent vulnerabilities in standard network protocols, coopt the devices, and transform them into malicious bots.

"Protocol reflection attacks are a serious problem, but system administrators can help protect their organization and the Internet community by taking steps to avoid participating in these types of DrDoS attacks," said Stuart Scholly, Prolexic President. "Unfortunately, the protocols were written with functionality, not security, in mind. The Internet used to be a safer place than it is now."

DrDoS attacks using these protocols can be difficult to trace back to the malicious actor because they often involve spoofing, or faking, the origin of the attack.

In the new DrDoS white paper, the Prolexic Security Engineering & Response Team (PLXsert) explains how malicious actors leverage three common network protocols inherent in network servers and devices:

- Simple Network Management Protocol (SNMP), used to communicate with IP-based devices, such as routers
- Network Time Protocol (NTP), used to synchronize time and date information across the network
- Character Generation Protocol (CHARGEN), used to test and debug network connections

The white paper, second in the DrDoS series, explains the protocol vulnerabilities and how they are used in DDoS attacks. It also identifies actions system administrators can take to reduce, or mitigate, the vulnerability of their network devices and servers.

The SNMP, NTP, CHARGEN Reflection Attacks white paper by PLXsert is available free of charge at www.prolexic.com/drdos.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's DDoS mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's most recent Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases Video Visualization of Recent 160 Gbps, 120 Mpps DDoS Attack

Illustrates company's mitigation process against massive multi-vector attack

HOLLYWOOD, FL – (April 25, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has released a new video that documents and visualizes how it mitigated a sustained 160 Gbps, 120 million packet-per-second (pps) attack. The DDoS attack occurred earlier this month and was directed against one of Prolexic's enterprise clients.

"Prolexic's latest video provides a snapshot of an unusually large attack and shows how it was mitigated using our cloud-based DDoS protection infrastructure," said Scott Hammack, CEO of Prolexic. "It's not easy to understand what DDoS mitigation services entail. This video clearly illustrates what Prolexic does on a daily basis."

The three-minute, narrated video, entitled "Prolexic in Action," shows the many different points in the cloud-based infrastructure where Prolexic blocks malicious DDoS attack traffic. Viewers can see malicious traffic routed through Prolexic's scrubbing centers and sorted by attack type – infrastructure (Layer 3 and 4) or application (Layer 7) attacks. The video then shows how the two different attack types are mitigated with blocking signatures through automated mitigation gear and in real-time by Prolexic engineers at the company's 24/7 Security Operations Center. For each attack type, the video shows the destination IP addresses and ports that are targeted how that attack type was blocked.

"There's a lot of scaremongering at the moment and hyping of attack sizes," said Hammack. "Even though attack sizes are getting extremely large, as documented in this video and our recent ***Q1 2013 Global DDoS Attack Report***, Prolexic is able to mitigate them effectively. Organizations can remain confident that these attacks can be stopped with the right DDoS mitigation service provider."

Prolexic's new video can be viewed at www.prolexic.com/real-attack.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in

Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Average Attack Bandwidth up 718 percent; Average Packet-Per-Second Rate Reaches 32.4 Million According to Prolexic's Q1 2013 DDoS Report

Giant attacks overwhelming appliances, ISPs, carriers, content delivery networks

HOLLYWOOD, FL – (April 17, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that average attack bandwidth totaled 48.25 Gbps in Q1 2013, a 718 percent increase over last quarter, and the average packet-per-second rate reached 32.4 million. These startling metrics are just two of many contained in the company's ***Quarterly Global DDoS Attack Report***, which was published today.

"Average packet-per-second rate and average bit rate spiked in the first quarter and both are growing at a fast clip," said Stuart Scholly, president at Prolexic. "When you have average – not peak – rates in excess of 45 Gbps and 30 million packets-per-second, even the largest enterprises, carriers, and quite frankly most mitigation providers, are going to face significant challenges."

Early last year, a different type of DDoS attacker emerged: one with considerable botnet resources, but also an intimate understanding of how the Internet routing topology works. As a result, Prolexic detected a clear shift to high packet-per-second DDoS attacks specifically designed to overwhelm infrastructure elements such as routers. Failure of these devices often causes collateral damage, typically taking thousands of customer websites offline.

"It's a classic change up," said Scholly. "Nearly everyone has been focused on bandwidth and gigabits per second, but it's the packet rate that's causing the most damage and presenting the biggest challenge. These packet rates are above the thresholds of all but the most expensive routers and line cards and we are seeing networks buckle as a result."

Highlights from Prolexic's *Q1 2013 Global DDoS Attack Report*

Compared to Q4 2012

- Average attack bandwidth up 718 percent from 5.9 Gbps to 48.25 Gbps
- Average attack duration increases 7.14 percent from 32.2 hours to 34.5 hours
- Total number of infrastructure attacks rise 3.65 percent; total number of application attacks fall 3.85 percent
- 1.75 percent increase in total number of DDoS attacks

Compared to Q1 2012

- Average attack bandwidth up 691 percent from 6.1 Gbps to 48.25 Gbps

- 21 percent increase in average attack duration from 28.5 hours to 34.5 hours
- Total number of infrastructure attacks up 26.75 percent; total number of application attacks up 8 percent
- 21.75 percent rise in total number of attacks

Analysis and emerging trends

During Q1 2013, more than 10 percent of DDoS attacks against Prolexic's global client base averaged more than 60 Gbps. The largest attack mitigated in the quarter peaked at 130 Gbps, occurring in March against an enterprise customer. In response to these huge attacks, more carriers and ISPs are being forced to null route (black hole) traffic to protect their networks.

Attack volume also grew in Q1 2013 and reached the highest number of attacks Prolexic has logged for one quarter. However, the percentage increase over the previous quarter was nominal. Attack volume has been especially high during the last six months, reflecting a general trend of heightened global DDoS activity and risk of attack.

Like recent quarters, Layer 3 and Layer 4 infrastructure attacks were the favored attack type, accounting for 76.54 percent of total attacks during the quarter, with Layer 7 application layer attacks making up the remaining 23.46 percent. This approximate 3:1 split remains unchanged. This quarter, SYN (25.83 percent), GET (19.33 percent), UDP (16.32 percent) and ICMP (15.53 percent) floods were the attack types most often encountered during mitigation.

Average attack duration continued to rise, from 32.2 hours the previous quarter to 34.5 hours in Q1, an increase of 7.14 percent. March was the most active month for attacks, accounting for 44 percent of the quarter's attacks. The week of March 19 was the most active of the quarter. The last two weeks of the quarter were the most active and showed the largest percentage increase compared to Q1 2012 (306 and 154 percent respectively).

As is commonplace, the top 10 list of source countries responsible for launching the most DDoS attacks was fluid with the exception of China. Once again, China secured the top place in attack source country rankings, joined by the United States, Germany, and for the first time, Iran.

"Because Prolexic operates an 800 Gbps cloud-based, upstream network and typically intercepts traffic long before it hits carriers and saturates their networks, it is one of the few companies in the world that can handle this level of attack traffic," said Scholly. "Prolexic gained a significant number of new clients in Q1 as more and more providers that offer DDoS as a add on service failed to cope with these enormous attacks."

Data for the Q1 2013 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Q1 2013 Global DDoS Attack Report is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q2 2013 report will be released in the third quarter of 2013.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Betstar Chooses Prolexic DDoS Mitigation Services

Protects Online Betting Site from Revenue Loss During Australia's Biggest Horse Racing Event

HOLLYWOOD, FL – (April 9, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that Betstar (Betstar.com.au), a popular online betting site located in Australia, has engaged Prolexic to provide DDoS protection and mitigation services. Betstar offers Internet betting on Australian and international sports and racing.

Recently, cyber attackers launched a series of DDoS attacks against online betting companies at the height of the Australian horse racing season known as Spring Carnival. Spring Carnival is the busiest and most profitable time for online betting companies in Australia and any revenue losses due to a website outage would be financially disastrous.

At the beginning of Spring Carnival, Betstar experienced a 30-minute site outage due to a DDoS attack on one of its competitors with whom it shares infrastructure in a colocation data center. The high-volume Layer 3 DDoS attack peaked at 10 Gbps and crippled the data center, which led to an eight-hour site outage for Betstar's competitor, and brief downtime for Betstar due to collateral damage. Two other online betting companies came under DDoS attack during the same weekend. The continued threat of DDoS attacks against the online betting industry led Betstar to seek DDoS mitigation services from Prolexic.

"Betstar wisely has taken proactive action against DDoS attacks," said Stuart Scholly, president at Prolexic. "DDoS attackers are known to target specific industries and unleash their most potent attacks during peak revenue-generating periods."

With the racing season just getting underway, it was especially urgent that Betstar quickly deploy the Prolexic PLXproxy DDoS mitigation solution. Prolexic and Betstar worked over a weekend to ensure a fast deployment. Within three days from signed contract, the Prolexic solution was up and running, well in time to ensure 24/7 uptime for online Betstar customers betting on the Melbourne Cup, Australia's equivalent to the Kentucky Derby, and other Spring Carnival races.

"Since Betstar has been protected by Prolexic, our site has never gone down again even though DDoS attackers have targeted our industry many times," said Bryan Dunne, IT manager at Betstar. "Most of all, our company no longer risks losing revenue or potential customers due to DDoS during the most profitable time of the year. I would advise any online betting company to put DDoS protection in place, because our experience has shown that it's only a matter of time before you will be attacked."

To learn more, download the Betstar DDoS protection case study at www.prolexic.com/betstar.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Protects Americaneagle.com's Hosting and e-Commerce Network Against DDoS Attacks

HOLLYWOOD, FL – (March 26, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it recently mitigated a multi-vector Layer 4 and Layer 7 DDoS attack directed at a customer of website development and hosting provider Americaneagle.com (www.americaneagle.com).

In business since 1995, Americaneagle.com had experienced isolated DDoS attacks over the past four years and mitigated them in-house. Recently, it was hit by a large scale DDoS attack directed at a customer's website. After this intense distributed denial of service attack, Americaneagle.com experienced a surge of 15 DDoS distributed denial of service attacks over the next two months. Americaneagle.com engaged Prolexic for DoS and DDoS protection after researching several DDoS mitigation providers, and a global telecommunications and Internet services provider (ISP).

"We were really impressed when we talked with Prolexic's engineers," said Ryan McElrath, chief technology officer at Americaneagle.com." The others we talked to just did not have the experience and expertise that Prolexic has."

"Web hosting companies are in critical need of reliable DDoS mitigation services since a DDoS distributed denial of service attack that brings down one hosted site can potentially cause performance problems for other customer sites, or even render them inaccessible," said Stuart Scholly, president of Prolexic. "Now Americaneagle.com can give its customers the assurance of proven Prolexic protection against DDoS."

Since becoming a Prolexic client, Americaneagle.com has deployed the PLXrouted DDoS mitigation service and it has already been put to good use. Recently, Prolexic mitigated a DDoS attack on an Americaneagle.com hosted e-Commerce site that experienced a combination Layer 4 SYN flood and UDP flood that peaked at 4.80 Gbps (bits per second) and 4.55 Mpps (packets per second). Using the PLXrouted service, Americaneagle.com was able to avoid both customer downtime and financial loss, as well as damage to its reputation for reliable service.

"I couldn't be happier with Prolexic," McElrath says. "Their response times are great, whether we have an urgent or non-urgent request. Having Prolexic's protection against DDoS gives our customers and Americaneagle.com peace of mind."

To learn more, the full Americaneagle.com case study can be downloaded from www.prolexic.com/americaneagle.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases DNS Reflection Attack White Paper

Popular, effective distributed reflection denial of service (DrDoS) attacks disrupt the Internet domain name system to target their victims

HOLLYWOOD, FL – (March 19, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has released the first of several white papers about Distributed Reflection Denial of Service (DrDoS) attacks. DrDoS attacks, an attack method which has been used for more than a decade, have recently surged in popularity across a broad range of industries.

In this white paper, prepared by the Prolexic Security Engineering and Response Team (PLXsert) discusses and analyzes DNS Reflection attacks. The DNS Reflection DrDoS technique exploits security weaknesses in the Domain Name System (DNS) Internet protocol, an important Internet feature that allows the public to type in human-friendly domain names instead of numerical IP addresses to access websites.

In this type of attack, a cyberattacker leverages zombie computers in a botnet to send domain name requests to DNS servers in a way that causes DNS servers to send a flood of responses to a targeted domain. This kind of DrDoS attack can overwhelm and slow response times – or completely stop legitimate user access – and affects both the DNS servers and the targeted domain.

A DNS Reflection attack is relatively easy for cybercriminals to launch, and takes advantage of security loopholes in the DNS protocol, PLXsert warns. What's more, it is difficult to pinpoint the source of a reflected DDoS attack, offering anonymity to the attacker.

"DNS Reflection DrDoS attacks are an overlooked but dangerous DDoS attack method," said Stuart Scholly, Prolexic President. "Prolexic is releasing this white paper to help make DNS server administrators, IT administrators and business leaders aware of this potential security threat against their networks. In addition, the white paper can help victims understand the technical details of what took place, so they can more quickly mitigate these kinds of DDoS attacks in the future."

The DNS Reflection Attack white paper explains DNS and how an attacker exploits the protocol to cause an outage. The white paper is available free of charge at www.prolexic.com/drdos.

About the Prolexic Security Engineering & Response Team (PLXsert)
PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By

identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's DDoS mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q4 2012 Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic
Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in- the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Selected for DDoS Mitigation Services by Australia's Number One Job Search Website

HOLLYWOOD, FL – (March 12, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that Seek.com.au, Australia's leading employment website, has selected Prolexic to provide DDoS detection and DDoS protection services. With 21 million site visitors each month, the Australian owned and operated website provides access to information on 120,000 jobs, as well as current insights into local labor markets and research on employment trends.

Recently, Seek.com.au was hit by a Layer 7 (application layer) distributed denial of service attack that rendered the site's extensive job search data and services inaccessible. As an insurance policy against downtime caused by future attacks, SEEK chose Prolexic to provide DDoS mitigation services.

"Prolexic is a specialist in DDoS mitigation and that's all they do," said Andre Bertrand, security services manager at SEEK. "DDoS mitigation is only an add-on service with ISPs and other providers. It all comes down to how much experience the provider has in DDoS, which is a very specialized business. We wanted only the best protection and we feel that Prolexic is clearly the best DDoS mitigation provider in the industry."

"Being prepared is the best defense against DDoS attacks and SEEK has taken a proactive step by putting Prolexic on the front lines of its mitigation strategy," said Stu Scholly, President of Prolexic. "Prolexic advises all businesses to make cyberattack defense a part of their incident response plan to eliminate panic and ensure a calm and controlled response to a DDoS attack."

Since signing on as a Prolexic client, Prolexic has worked with SEEK to create a pre-rehearsed DDoS mitigation plan or playbook of defensive actions to be taken as soon as a DDoS attack is detected. As a result, SEEK now has a proven DDoS mitigation plan in place with Prolexic as its first line of defense. While SEEK has not needed to use Prolexic's DDoS mitigation service yet, management has taken advantage of other benefits of being a Prolexic customer. "We have found Prolexic to be very helpful in providing intelligence on DDoS and cyber attacks so that we can be proactive in our DDoS defense," Bertrand said.

"Prolexic's efforts in testing our mitigation strategy, keeping up-to-date with the playbook, and providing DDoS intelligence on a regular basis has been refreshing compared to other DDoS mitigation vendors," continued Bertrand.

To learn more, the full seek.com.au case study can be downloaded from www.prolexic.com/seek.

Learn more about DDoS mitigation testing and DDoS playbooks by downloading the free Prolexic white paper, *Plan vs. Panic: Making a DDoS Mitigation Playbook a Part of Your Incident Response Plan*, at www.prolexic.com.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Mitigates DDoS Attack Against U.S. Utility Company

Attackers now targeting network infrastructures that cause collateral damage

HOLLYWOOD, FL – (March 7, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it mitigated an attack against a U.S. metropolitan utility company earlier this month. The utility, which provides services to an estimated 420,000 electric, 305,000 water, and 230,000 sewer customers, has engaged Prolexic to provide DDoS protection services.

On February 17, 2013, the utility company's website, online payment system and automated pay-by-phone billing system were brought down for 48 hours by a combination Layer 4 DDoS attack. During that time, more than 155,000 customers could not pay bills online or by phone. In addition, employees could not receive external e-mails.

"Utilities is another vertical market that is likely to be victimized in the coming months as attackers look beyond daily targets like e-Commerce and financial services," says Stuart Scholly, president at Prolexic. "Attackers are targeting network infrastructures to cause collateral damage to other shared resources, so organizations must think about their different areas of vulnerability beyond website URLs."

The DDoS attack, which Prolexic identified as originating in the U.S., was highly sophisticated and particularly difficult for the utility company's IT department to detect and mitigate because the attack directly targeted the back-end IP addresses of the utility's Internet-facing network. On the second day of the attack, Prolexic was engaged by the utility to take emergency action to mitigate the distributed denial of service attack.

Prolexic's DDoS mitigation engineers quickly determined that the attackers were targeting backend IPs directly. They developed and launched a specially crafted routed DDoS defense that immediately began to reduce the strength of the hackers' sophisticated attack on the back-end IPs. Prolexic mitigation engineers continued to fight the distributed denial of service attack and quickly adjusted defense strategies as the attackers changed their attack signatures. The Layer 4 attack peaked at 3.3 Gbps and 5.7Mpps (packets-per-second).

"Once traffic was on-ramped to Prolexic, the DDoS attack was mitigated in a matter of minutes and all services were restored to our website and automated pay-by-phone system," said a representative of the utility company. "Prolexic quickly ended what could have been a devastating blow to our customer service and our reputation for reliable service."

“Prolexic considers every DDoS attack to be zero-day and we have designed our mitigation infrastructure so we can respond accordingly,” said Scholly. “As a result, clients can be confident that Prolexic’s proxy or routed solutions can provide 100 percent protection against all distributed denial of service attacks.”

The case study about this utility is available to the public, free of charge, at www.prolexic.com/utility-case-study.

About Prolexic

Prolexic is the world’s largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Provides Real-Time, Granular DDoS Attack Data for Deep Network Analysis

New functionality to be demonstrated at RSA, Booth #2539

HOLLYWOOD, FL – (February 25, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it will provide customers with real-time data and analysis of their network perimeter, empowering them with much of the same information it uses to prevent and mitigate DDoS attacks. As a result, Prolexic customers can watch and analyze DDoS attacks in real-time with drill-down detail into the attack mitigation industry's most granular data for deep network analysis.

An industry first, this includes views of real-time HTTP and HTTPS request patterns for live traffic, as well as a unified, timeline view of changes associated with their external sensors, monitoring, attacks and configurations. This detailed information is presented in a converged view in the Prolexic Portal so users do not have to navigate multiple screens to piece together key data.

"Prolexic customers want more than a high level summary of the top 10 DDoS attacks," said Stuart Scholly, president at Prolexic. "They want to be able to diagnose potential problems as they happen. That means important details can't be glossed over and then summarized 15 minutes (or several hours) later. While we do provide big picture views, the Prolexic Portal allows users to quickly drill down into hundreds of metrics for a clearer picture of what is happening *now*."

To support this data-rich real-time analysis, Prolexic invested heavily to upgrade its big data architecture to support its analytics platform. While most industry portals use batch processing and present aggregated data, Prolexic built a low-latency, high-resolution data architecture to provide customers with the industry's most granular data in real-time. This enables Prolexic customers and staff in the company's Security Operation Center to watch events – as they happen – and respond more quickly.

"Prolexic is the first DDoS mitigation provider to extend its portal experience down to this level," said Scholly. "Real-time analysis is the best way to understand how an attack evolves and counteract it, and this is what the Prolexic portal now provides to all of our customers."

The public can preview the Prolexic Portal in Booth 2539 at the RSA Conference, Feb. 25 – March 1 in San Francisco or by watching our Prolexic Portal video tour at www.prolexic.com/newportal.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube, and @Prolexic on Twitter.

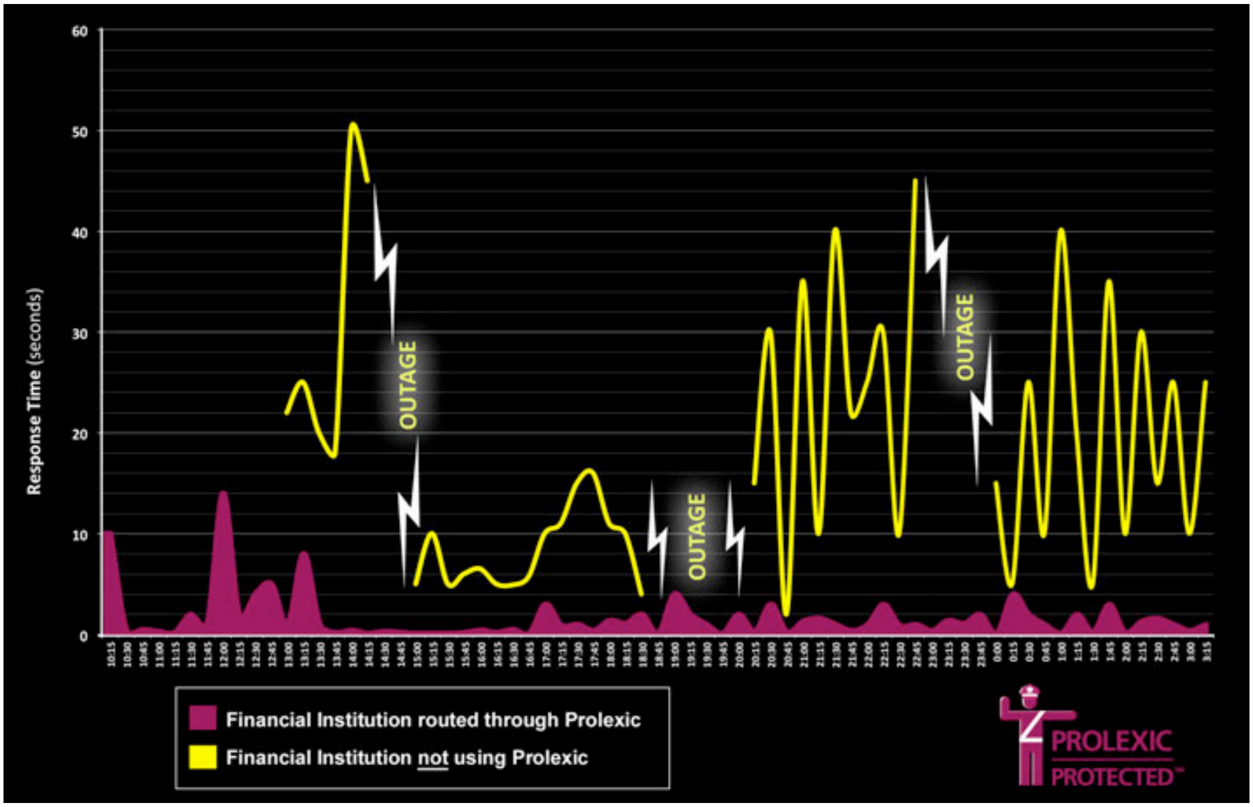
###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Website Latency Study Highlights Differences in Response Times during Recent DDoS Attacks against Two Banks

HOLLYWOOD, FL – (February 22, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today released results of a website performance case study that documented variations in load times during live DDoS attacks. The study tracked performance of two financial institutions; one website had average website load times of two seconds or less, while the other experienced multiple site outages and lengthy delays in server response times.

The headline-making attacks were publicly announced on underground hacker sites before they started. Based on that information, Prolexic was able to track the same DDoS attack against two financial services companies simultaneously. One firm used Prolexic's PLXrouted DDoS protection service while the other financial institution was engaged with another DDoS protection provider. Response time – how long a page takes to load on a website – was tracked for both firms using the Compuware Gomez Application Performance Monitor, from multiple worldwide locations.



Data shows that the user experience was far superior with Prolexic. The Prolexic client suffered zero outages and pages typically loaded in a tolerable two seconds, even though the financial services firm was under a significant DDoS attack. In contrast, the firm that did not use Prolexic suffered three separate outages and website users had to endure page-loading times as high as 50 seconds in some cases, making the site unusable.

“Minimizing the impact of an attack is job number one for DDoS mitigation providers,” said Stuart Scholly, president at Prolexic. “Even if your website is under a severe attack, Prolexic can help ensure the user experience is maintained at acceptable levels.”

The public can learn more about Prolexic’s performance under attack conditions in Booth 2539 at the RSA Conference, Feb. 25 – March 1 in San Francisco, or by viewing our website latency video at prolexic.com/latency.

About Prolexic

Prolexic is the world’s largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Launches New Public Service: PLXpatrol

Provides security community with instant global view of DDoS threats

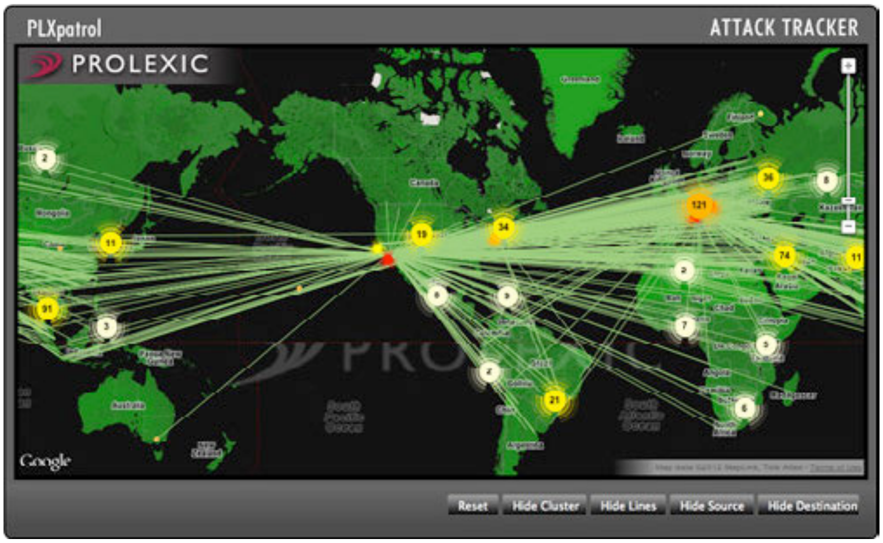
HOLLYWOOD, FL – (February 12, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has introduced PLXpatrol, a public service that the world's security community can leverage to gain an instant global snapshot of current denial of service (DoS) and DDoS threats and activity. The complimentary service is available at www.prolexic.com/plxpatrol and no registration is required.

In addition to mitigating the largest and most sophisticated attacks against its global client base, Prolexic typically mitigates more attacks than any other DDoS protection provider. As many of the company's clients are from the high-risk online gaming and financial services industries, Prolexic also faces emerging threats earlier than other providers, making it an ideal resource for unbiased DDoS threat intelligence.

"PLXpatrol is an invaluable service for the world's cyber security community," said Stuart Scholly, president of Prolexic. "Staying up-to-date and informed about threats is the best defense against DDoS attacks and PLXpatrol now makes that incredibly easy."

At launch, PLXpatrol offers three distinct data views:

- **Attack Tracker –** Continuously updated, this view shows where DDoS attacks directed against Prolexic's clients are originating from and geographic locations of targets (anonymized). Attack Tracker also displays the number of source and destination IP addresses involved in the attack.



- **Country Ranking (Last 24 hours)** – This ranking shows the countries that have originated the most attack traffic against Prolexic clients over the last 24 hours.

- **Country Ranking (All Time)** – This ranking shows the countries that have originated the most attack traffic against Prolexic clients since data collection began in 2009.

"Prolexic already publishes a widely respected Quarterly Global DDoS Attack Report, and while that format and deep analysis still has value, there's nothing like having instant access to data that is updated frequently," said Scholly. "Over the coming months we plan to roll out many more data views to make PLXpatrol the industry's number one destination for DDoS insight and intelligence."

The information presented in PLXpatrol is sourced from Prolexic's analytical and IP reputational databases. Prolexic makes this information, and more detailed views, available to its customers in near real-time through the Prolexic Portal.

Prolexic's new PLXpatrol service is available at www.prolexic.com/plxpatrol.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Media Advisory: February 7, 2013

The RSA Conference 2013 at Your Fingertips:

Mobile App sponsored by Prolexic is now available on iTunes and Google Play

Who: Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services.

What: **The new RSA Conference 2013 application allows attendees to manage their time and activities at the show on their mobile device.**

With the RSA Conference Mobile App, one can stay connected with all of their conference activities. View the event catalog, manage session schedules and engage with colleagues and peers while onsite using social and professional networking tools. Attendees will have access to dynamic agenda updates, venue maps, exhibitor listing and more!

Why: Prolexic understands that attendees need to get the most out of their time at the conference. Having the RSA Conference App on their mobile device means they will always know where they want to be – and they can adjust their schedule on the fly, right from the show floor.

Where: **Visit the iTunes store** (https://itunes.apple.com/us/app/rsa-conference-2013/id498594512?mt=8) **or the Google Play** (https://play.google.com/store/apps/details?id=com.activenetwork.mobile.rsaus12&feature=nav_result#?t=W251bGwsMSwxLDMsImNvbS5hY3RpdmVuZXR3b3JrLm1vYmlsZS5yc2F1czEyIl0.) **and download the "RSA Conference 2013" application – it's free.**

When: Available now

Questions: Michael Donner, SVP & CMO
+1 (954) 620 6017
media@prolexic.com

About Prolexic:
Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's twenty largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Mitigates DDoS Attack Campaigns Against Henyep's Financial Trading Sites

HOLLYWOOD, FL – (January 24, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has mitigated multiple SYN, GET and ICMP floods directed against a variety of trading websites operated by London-based Henyep Capital Markets, a leading international online trading and financial services company.

The initial DDoS attack caused performance issues on multiple Henyep trading websites for 24 hours. Company management did not respond to the DDoS attackers' demand for a ransom in exchange for ending the attack, and instead engaged Prolexic. The company's mitigation engineers restored access to all services on the sites within minutes after routing traffic through Prolexic's global scrubbing centers where malicious traffic was removed.

"Financial services companies like Henyep and their mission critical online services continue to be favorite targets of DDoS attackers," said Prolexic's President, Stuart Scholly. "It is vitally important to have DDoS mitigation services in place from a proven, experienced provider with the global resources and bandwidth capable of handling attacks well in excess of 50 Gpbs."

Prolexic DDoS mitigation engineers in the U.S. quickly identified the initial attack as a SYN flood followed by multiple GET floods. The attack campaign peaked at 35.30 Mbps (bits per second), 8.10 Kpps (packets per second), and 122.00 Kconn (connections per second) over two days. Prolexic mitigation engineers were monitoring the attacks and counteracting the perpetrator's changing attack vectors throughout the campaign. As a result, the attackers were unable to take down the Henyep site, nor disrupt services despite the length of the attack.

Recently, DDoS attackers tried to take down Henyep's trading operations again with a 30 Mbps ICMP flood and GET flood without success due to Prolexic DDoS protection. Throughout 2012, Henyep, like many other financial services companies, has continued to be the target of DDoS attackers, but Prolexic's DDoS mitigation services have prevented any downtime.

"The fact that Prolexic protects some of the biggest banks in the world gives us confidence in their DDoS mitigation expertise," said Henyep's director of business development and operations. "We can be confident in protecting our clients' trading activities and access to personal financial information with Prolexic. A high level of customer service is critical to our business and Prolexic DDoS protection helps us ensure 24/7 uptime."

To learn more, the full Henyep case study can be downloaded from www.prolexic.com/henyep.
According to data published last week in Prolexic's ***Q4 2012 Global DDoS Attack Report***, financial services, e-Commerce and software-as-a-service (SaaS) companies were targeted with high bandwidth DDoS attacks in excess of 50 Gbps in the fourth quarter. Over the three-month period, Prolexic logged more attacks than ever before against its global client base and predicts the scale and diversity of DDoS attacks will continue to increase. A complimentary copy of the report is available for download at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Large-Scale DDoS Attacks Grow Bigger and More Diversified According to Prolexic's Latest Report

Seven 50+ Gbps attacks mitigated against financial, SaaS and e-Commerce firms

HOLLYWOOD, FL – (January 17, 2013) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that the scale and diversity of attacks increased against its global client base in Q4 2012. This is one of a number of key findings contained in the company's Quarterly Global DDoS Attack Report, which was published today.

While Q4 media reports focused on large DDoS attacks primarily against U.S. financial services companies, Prolexic also mitigated 50+ Gbps DDoS attacks against clients in the e-Commerce and software as a service (SaaS) sectors. While the *itsoknoproblembro* (BroDoS) toolkit was used against financial services firms in Q4, data shows it was also used against businesses in other sectors. Digital forensics by the Prolexic Security Engineering & Response Team (PLXsert) also found that malware besides Brodos was used in Q4 to generate equally large bandwidth attacks.

"The fourth quarter was defined by the increasing scale and diversity of DDoS attacks," said Prolexic CEO, Scott Hammack. "While bandwidth attacks of 20 Gbps were the story last quarter, 50 Gbps is more relevant now."

Highlights from Prolexic's Q4 2012 Global DDoS Attack Report

Compared to Q3 2012

- 27.5 percent increase in total number of attacks
- 17 percent increase in total number of infrastructure attacks; 72 percent rise in total number of application attacks
- 67 percent increase in average attack duration to 32.2 hours from 19.2 hours
- 20 percent increase in average attack bandwidth from 4.9 to 5.9 Gbps
- China retains its position as the top source country for DDoS attacks

Compared to Q4 2011

- 19 percent increase in total number of DDoS attacks
- 15 percent rise in total number of infrastructure attacks; 30 percent rise in total number of application attacks
- 6 percent decline in average attack duration to 32.2 hours from 34
- 13 percent increase in average attack bandwidth from 5.2 Gbps to 5.9 Gbps

Analysis and emerging trends

During Q4 2012, Prolexic mitigated seven attacks over 50 Gbps directed against clients in the financial services, e-Commerce and SaaS verticals. "A case could be made that the size of attacks that are being reported in the financial services industry really just reflects the normal growth in DDoS," said Hammack. "We are seeing similarly sized attacks in other verticals, but they don't make headlines because companies in these industries are not required to report it in the same way."

In addition to increasing attack sizes, attack volume grew in Q4 2012 and reached the highest number of attacks Prolexic has logged for one quarter. Like the previous quarter, traditional Layer 3 and Layer 4 infrastructure attacks were the favored attack type, accounting for 75 percent of total attacks during the quarter, with application layer attacks making up the remaining 25 percent. This split has remained consistent throughout 2012. This quarter, SYN (24 percent), GET (20 percent), ICMP (18 percent) and UDP (15 percent) floods were the attack types most often encountered during mitigation.

Average attack duration increased 67 percent from 19.2 hours in Q3 2012 to 32.2 hours this quarter. November was the most active month for attacks, however, the total number of attacks for all three months of the quarter were consistent, showing a less than 10 percent difference from month to month. The week of Nov. 26 was the most active of the quarter, although only by a narrow margin.

As is commonplace, the top 10 list of source countries responsible for launching the most DDoS attacks was fluid. However, this quarter China secured the top place in attack source country rankings by a wide margin. Compared to last quarter, the United States dropped down in the rankings, while two European countries, France and Germany, rejoined the top 10 list.

"The take away for businesses from this Q4 report is to make sure that their DDoS mitigation provider can handle attacks in excess of 50 Gbps in a single location," said Hammack. "When attacks are this large, it's important that the provider can mitigate this volume of attack traffic in one place and distribute it effectively so it does not compromise intermediary transit providers and affect others."

Data for the Q4 2012 report has been gathered and analyzed by the PLXsert. The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert builds a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, PLXsert helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Quarterly Attack Report for Q4 2012 is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q1 2013 report will be released in the second quarter of 2013.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Selected by PayPro Global for DDoS Mitigation

HOLLYWOOD, FL – (January 9, 2013) – Prolexic, the global leader in distributed denial of service (DDoS) protection services, announced today that it is now providing DDoS detection and DDoS protection to PayPro Global, a leading Canadian software distribution service.

Headquartered in Toronto, PayPro Global hosts an e-Commerce infrastructure for software developers worldwide. Last November, the secure HTTPS payment transaction servers supporting www.payproglobal.com were taken offline for hours as a result of a Layer 7 distributed denial of service DDoS attack. During that time, PayPro Global's worldwide customer base of software developers could not generate revenue. This followed a previous DDoS attack launched against the site in the third quarter.

"The DDoS attacks against PayPro Global are proof that practically anyone can launch a DDoS attack these days," said Stuart Scholly, president at Prolexic. "As a Prolexic customer, PayPro Global is now fully protected against all types and sizes of distributed denial of service attacks, whether from an individual or a well-organized group of cybercriminals with significant botnet resources."

"After exploring and testing numerous options on the market we chose Prolexic as its DDoS protection system showed the best results in repelling cyber-attacks," said Matthew Silverman, CEO of PayPro Global. "We are confident that through the partnership with Prolexic, downtime will become ancient history for our company."

"We have been attacked several times since bringing Prolexic on board, but our site never went down," said Valeriu Braghis, marketing manager at PayPro Global. "Prolexic was successful against every DDoS attack. It is important for us to give our customers the confidence that they are no longer at risk of revenue loss due to a DDoS attack and Prolexic does that."

To learn more, the full PayPro Global case study can be downloaded from www.prolexic.com/PayPro.

About PayPro Global

Founded in 2006, PayPro Global, Inc. develops and hosts an e-commerce solution that allows anyone to easily sell software online. PayPro Global supports more than one hundred currencies, all major credit and debit cards, and a wide variety of payment options. The company also offers software developers state-of-the-art licensing, activation, and anti-piracy protection for their applications.

PayPro Global is headquartered in Toronto, Canada, with development center in Ramat Gan, Israel and regional offices in New York, USA, and London, UK.

Website: www.payproglobal.com
Twitter: @paypro_global

About Prolexic

Prolexic is the world's largest, most trusted distributed denial-of-service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases Threat Advisory to Detail Massive DDoS Threat from *itsoknoproblembro*

Multi-Tiered DDoS Toolkit Leveraged in Synchronized Attacks Against Banking, Hosting and Energy Industries

HOLLYWOOD, FL – (Jan. 3, 2013) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today released a suite of detection and mitigation rules, a log analysis tool and a comprehensive threat advisory on the *itsoknoproblembro* DDoS toolkit. Considered to pose a very effective, multi-level threat, *itsoknoproblembro* has been the favored weapon in headline-making DDoS attacks against the US banking industry.

Malicious hackers are using the toolkit to target known vulnerabilities in web content management systems, including Joomla and WordPress, to infect web servers with malicious PHP scripts. The toolkit then leverages a unique, two-tier command mode that can launch multiple high-bandwidth attack types simultaneously. Some of these attacks have peaked at 70 Gbps and more than 30 million pps, a magnitude of traffic that demonstrably overwhelms most network infrastructures.

“Our security experts have successfully mitigated this threat multiple times, in tense, real-time digital battles,” said Prolexic Chief Executive Officer Scott Hammack. “This toolkit, which was dangerous to begin with, has been evolving rapidly over the past year, and has been increasingly used in coordinated campaigns targeting specific industries. The December attacks against the banking industry represented the fourth documented campaign against finance companies; we’ve also documented smaller campaigns against the energy and hosting provider industries.

“Given the chatter in the hacker underground, we expect these *itsoknoproblembro* DDoS campaigns will continue to grow in frequency,” Hammack added. “We want to support the security community by sharing our knowledge, so we can help eradicate this threat and remove these malicious scripts from infected machines before they do even more damage.”

The Prolexic Security Engineering & Response Team (PLXsert) first issued a public warning about *itsoknoproblembro* in October. The toolkit was also profiled in Prolexic’s Q3 2012 Attack Report.

The threat advisory issued today profiles 11 different attack signatures and provides detailed SNORT rules for DDoS mitigation. The attack vectors include POST, GET, TCP and UDP floods, with and without proxies, including a so-called Kamikaze GET flood script that can repeatedly relaunch automated attacks.

Additionally, PLXsert published a set of detection rules to identify infected web servers (bRobots), along with a free log analysis tool that can be used to pinpoint which scripts were accessed, by what IP address and for what DDoS targets. Armed with this information, the infected servers can be sanitized, preventing them from being used in subsequent *itsoknoproblembro* campaigns.

"The nature of these threats requires the cooperation of everyone in the network protection community to work together," Hammack added. "Working with our fellow engineers and researchers, we will continue to provide free updates of this log analysis tool and encourage users to share their logs of compromised servers for continued analysis and refinement."

A complimentary copy of the full DDoS threat advisory, including mitigation rules and detection rules, as well as the log analysis tool, BroLog, are available for download at www.prolexic.com/itsok.

Additional information on the *itsoknoproblembro* attacks and other recent DDoS trends will be shared in the Prolexic Q4 2012 Global DDoS Attack Report later this month.

About PLXsert
PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q4 2012 Global DDoS Attack Report will be available in January at www.prolexic.com/attackreports.

About Prolexic
Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please

visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Recommends Combining Two Scoring Systems for More Accurate Analysis of DDoS Threat Levels

HOLLYWOOD, FL – (December 4, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it recommends organizations combine two commonly used risk scoring systems to obtain a more accurate gauge of DDoS threat levels.

The recommendation and a detailed how-to guide is featured in Prolexic's new white paper, "***Risk Rating Analysis of DDoS Attacks: How the integration of the MIDAS Scoring System with NIST CVSSv2 can improve DDoS risk assessment,***" that was published today.

The practice of assigning a risk rating to the intensity level of a DDoS attack can be obtained by adapting the Measure of Impact of DDoS Attacks (MIDAS) scoring system (developed by AT&T Research Labs) and blending those results with the National Institute of Standards and Technology Common Vulnerability Scoring System version 2 (NIST CVSSv2) calculator.

The base metric risk scoring system from the NIST CVSSv2 analysis framework focuses on three key aspects of information security: confidentiality, integrity and availability. When dealing with DDoS, the only metric that would be affected is availability. This limited metric is where the integration of the MIDAS system, along with risk rating modifier parameters of the CVSSv2 system, comes into use.

"Combining the threat classification of the MIDAS system with the NIST CVSSv2 scoring system enables businesses to immediately assess the risk of various types of DDoS attacks against specific network resources," said Neal Quinn, chief operating officer at Prolexic. "By using the MIDAS system to define ddos attack types, businesses are able to tailor the CVSS analysis toward a more accurate risk rating, providing an understanding of both the targets and the sizes of incoming attacks."

The new white paper, "***Risk Rating Analysis of DDoS Attacks: How the integration of the MIDAS Scoring System with NIST CVSSv2 can improve DDoS risk assessment,***" can be downloaded for a limited time from www.prolexic.com/ddos-risk-rating.

This white paper follows the recent introduction of Prolexic's DDoS Downtime Calculator, which is available at www.prolexic.com/downtime. By completing the short questionnaire, business can obtain an estimate of downtime in terms of hours and cost based on their specific information technology infrastructure.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Keeps Revenues Flowing for worldofwatches.com by Mitigating DDoS Attacks

HOLLYWOOD, FL – (Nov. 13, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has successfully mitigated two attacks against the popular e-commerce website www.worldofwatches.com.

The website is owned by Swiss Watch International (SWI), a Florida-based company that designs and manufactures timepieces. The company also distributes and owns watch lines including SWI, Edox, Giordano, Jacques Lemans, Magico, Swiss Legend, Triumph Motorcycles and Ventura. The website averages more than 33,000 unique visitors daily, and at peak times, it generates more than US$100,000 each day, so any extended period of downtime can significantly affect revenues.

Despite having a firewall in place, a 130 Mb bandwidth flood penetrated the network via a well-known gaming port and brought down worldofwatches.com for 12 hours. The next day the company called Prolexic about emergency provisioning and mitigating the attack.

“The person we spoke to at Prolexic said they could mitigate the attack within minutes of receiving our traffic, so we signed a contract,” said Darin Grey, chief technology officer at Swiss Watch International. “Prolexic gave us a virtual IP address to use, and when I pointed traffic to Prolexic they were able to mitigate the attack and sent us back clean traffic. We were back up and running within minutes as promised.”

When it comes to effective DDoS mitigation, Grey believes that relying on an external provider is the best strategy. “Some attacks overwhelm your bandwidth and some overwhelm your hardware,” explained Grey. “It is almost impossible for a company to block these large attacks without investing hundreds of thousands or even millions of dollars in extra network equipment. Plus networks like this take time to set up. That’s one reason we chose Prolexic.”

After the attack was over, SWI increased network capacity to avoid a similar scenario. However, one month later, the website was attacked again, this time with an attack that was three times larger than the first. Network bandwidth flooded and the site went down again, but this time only briefly. Working closely with the website hosting provider, Prolexic successfully stopped this much larger second attack using its cloud-based mitigation network.

Grey has sage advice for other e-commerce providers with revenue-generating websites.

“If you have a successful site and are concerned about outages and you don’t have experience in fighting DDoS attacks on a large, large scale, I would definitely recommend

Prolexic," he said. "As I've told other people, use it as an insurance plan. If you're not attacked now, you will eventually get attacked as DDoS increases every year. And as your site becomes more successful, you are more of a target."

With Prolexic's cloud-based mitigation network standing between worldofwatches.com and any incoming DDoS attacks, Grey is confident about long-term site availability. "I know we're doing as much as we can to prevent DDoS attacks, and I know I have someone else in my back pocket in case we ever get hit to help mitigate it."

To learn more about the DDoS attack launched against worldofwatches.com, download the full case study at www.prolexic.com/worldofwatches.

An extended outage caused by a DDoS attack can lead to financial loss, and adversely affect the reputation of your online business, customer relationships and Google search rankings. Learn the best practices that support fast DDoS mitigation in our new white paper, "Strategies for Surviving a Cyber Attack this Holiday Season." Or, to find how much DDoS attacks could affect your business, visit the DDoS Downtime Calculator at www.prolexic.com/downtime.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Parts Geek Turns to Prolexic for DDoS Denial of Service Protection Services after Other Solutions Failed

Prolexic mitigates DDoS attacks against popular auto parts e-Commerce site

HOLLYWOOD, FL – (November 6, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today it recently mitigated a number of high-volume Layer 3 DDoS attacks directed at Parts Geek® (www.partsgeek.com), a popular e-Commerce web site for purchasing discount auto parts and accessories.

The DDoS attack campaign lasted three days and brought down the site for eight hours on the first day, and several hours on two subsequent days. The DDoS attacks rendered the site inaccessible to 100,000 site visitors daily. Prolexic was engaged by partsgeek.com after the site's hosting provider and another DDoS mitigation service provider were unable to mitigate the DDoS attacks, which were escalating in size and strength during the three-day campaign.

"The distributed denial of service attacks appeared to be random, since no specific ransom demands or warnings were received by the site's management," said Stuart Scholly, president of Prolexic. "Partsgeek.com now has Prolexic DDoS protection against all types of distributed denial of service threats, so it can deliver business as usual to customers anytime they want to place orders, day or night."

One recent Saturday evening, DDoS attackers brought down partsgeek.com for eight hours with a high-volume Layer 3 DDoS attack ranging between 25 and 40 Gbps. Management contacted the site's hosting provider but they were unable to mitigate this size of attack. The distributed denial of service attacks continued through the next two evenings. The company's management contacted a DDoS mitigation service provider, but this provider also lacked the resources to mitigate the DDoS denial of service attacks, which were escalating in size and strength.

"We contacted Prolexic and their mitigation team was able to stop the DDoS attacks immediately after provisioning their service," said Brian Tinari, president of Parts Geek. "These distributed denial of service attacks were disrupting our business so it was critical that we find a DDoS mitigation solution that would protect us from future attacks and the potential revenue loss they would cause."

Prolexic quickly mitigated the DDoS attack on partsgeek.com using its PLXproxy DDoS mitigation service, which is the quickest way to provision Prolexic's mitigation protection against all types and sizes of DDoS attacks. Any disruption to a site or downtime is resolved in just minutes.

“I’ve been very happy with Prolexic’s response and their customer support,” Tinari adds. “Their mitigation team is very professional and quick, and they were able to do what our hosting provider and other DDoS mitigation providers could not. We have had no DDoS attacks since engaging Prolexic and that gives us and our customers peace of mind.”

To learn more about the DDoS attack launched against partsgeek.com, download the full case study at www.prolexic.com/partsgeek.

DDoS attacks affect businesses differently. To find how much DDoS attacks could affect your business, visit the DDoS Downtime Calculator at www.prolexic.com/downtime.

About Prolexic

Prolexic Technologies is the world’s largest, most trusted Distributed Denial of Service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, and follow us on LinkedIn, Facebook, Google+ and @Prolexic on Twitter

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Publishes Executive Series White Paper: *Strategies for Surviving a Cyber Attack this Holiday Season*

HOLLYWOOD, FL – (October 29, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has published a new white paper in its Executive Series. A complimentary copy of the white paper, *Strategies for Surviving a Cyber Attack this Holiday Season,* can be downloaded from prolexic.com/holidayddos for a limited time.

The fourth quarter is a critical sales period for online retailers. According to predictions by digital marketing intelligence firm comScore, consumers will spend more than US$2 billion on online purchases on Black Friday and Cyber Monday this year. E-Commerce businesses have the potential to make 25 percent to 40 percent of their annual sales and profits during the holiday sales season.

Unfortunately, DDoS attacks against e-Commerce sites typically increase during the holiday sales season. Data compiled by the Prolexic Security Engineering & Response Team (PLXsert) and released exclusively in the new white paper, shows that between Q4 2009 and Q4 2010 there was an 8 percent increase in the total number of DDoS attacks against Prolexic's global client base of e-Commerce companies. Between Q4 2010 and Q4 2011, the total number of attacks increased significantly, rising 153 percent.

Prolexic's white paper examines how an extended outage from a DDoS attack can not only lead to greater financial losses, but also adversely affect the reputation of an online business, its customer relationships and even its search engine rankings. The paper also recommends best practices that support fast, controlled DDoS mitigation to minimize the impact of attacks.

"Prolexic advises all businesses that depend on online sales for revenues in Q4 to hope for the best, but prepare for the worst," said Stuart Scholly, president of Prolexic. "This paper can help businesses be proactive and adopt strategies that minimize financial loss in the event a DDoS attack strikes this holiday season."

In addition, Prolexic recently released the Prolexic DDoS downtime cost calculator, an online tool for gauging the cost and risk of a DDoS attack in a custom report. The Prolexic calculator also provides best practice tips and DDoS protection advice. E-Retailers and other e-Commerce businesses can use the report to evaluate the effectiveness of their DDoS protection strategies and take proactive steps if necessary. The Prolexic calculator is available for use at no charge at www.prolexic.com.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ , YouTube , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Releases Online DDoS Downtime Calculator

Provides Accurate, Detailed DDoS Risk Assessment and Recommended Mitigation Strategies

HOLLYWOOD, FL – (October 22, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has released a DDoS downtime cost calculator, available online at www.prolexic.com.

The Prolexic DDoS downtime calculator takes into consideration the many DDoS attack variables that can affect revenue. Using the Prolexic calculator, businesses that depend on e-Commerce for sales revenue can obtain an accurate and detailed risk assessment and the resulting downtime costs associated with a DDoS attack. Users can also run a number of what-if scenarios by changing any number of variables.

The Prolexic calculator includes a detailed questionnaire divided into three sections: Technologies, Experience and Cost Savings. To help users complete the various fields of the calculator, Prolexic has provided relevant tips, clarifications and advice, which can be used to evaluate current DDoS distributed denial of service protection strategies for e-Commerce. To ensure privacy, no user data is recorded by Prolexic.

"Prolexic developed this calculator so businesses can evaluate their unique DDoS risk and downtime cost based on hard numbers, not guesswork," said Stuart Scholly, president at Prolexic. "We know from previous years that DDoS attacks ramp up during the critical holiday sales period, so this calculator will help businesses make more informed decisions about DDoS protection in the coming weeks."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, *Google+* , *YouTube* , and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Increasing Size of Individual DDoS Attacks Define Third Quarter, According to Prolexic's Report

20 Gbps is the new norm

HOLLYWOOD, FL – (October 17, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that the size of DDoS attacks increased significantly against its global client base in Q3 2012. This spike is one of a number of key findings contained in the company's **Quarterly Global DDoS Attack Report**, which was published today.

During Q3, Prolexic mitigated seven DDoS attacks of more than 20 Gigabits per second (Gbps) for different clients across multiple industries. A number of these denial of service attacks leveraged the PHP-based bot toolkit called *itsoknoproblembro* that has been used in some recent high-profile DDoS attacks.

"Last year, a DDoS attack in excess of 20 Gigabits per second was notable, but today it seems commonplace," said Stuart Scholly, president of Prolexic. "To put this in perspective, very few enterprises in the world have a network infrastructure with the capacity to withstand bandwidth floods of this size."

Other highlights from Prolexic's Q3 2012 Global DDoS Attack Report

Compared to Q2 2012

- 14 percent decline in total number of attacks
- 11 percent increase in average attack bandwidth
- Slight increase in average attack duration to 19 hours from 17 hours
- Packet per second volume increase of 33
- China joined by the United States as the top source countries for DDoS attacks

Compared to Q3 2011

- 88 percent increase in total number of DDoS attacks
- Significant decrease in average attack duration: 19 hours vs. 33 hours
- 230 percent increase in average attack bandwidth

Analysis and emerging trends

While the size of individual DDoS attack campaigns increased, the number of attacks against Prolexic's global client based declined 14 percent this quarter when compared to Q2 2012. However, Prolexic logged more DDoS attacks last quarter than ever before, so attack volume continues to be robust. This statistic is illustrated by an 88 percent increase in denial of service attack volume when compared to Q3 2011.

This quarter, average attack bandwidth totaled 4.9 Gbps, up 11 percent from 4.4 Gbps in the previous quarter. Average packet-per-second (pps) volume continued its upward trajectory, increasing 33 percent over the previous quarter, rising from 2.7 mpps to 3.6 mpps.

Like last quarter, traditional Layer 3 and Layer 4 infrastructure DDoS attacks were by far the favored attack type, accounting for four out of five attacks during the quarter with application Layer 7 DDoS attacks making up the remainder. Five different attack types were commonly used in attack campaigns this quarter, including SYN floods (23.53 percent), UDP floods (19.63 percent), ICMP floods (17.79 percent), GET floods (13.50 percent), and UDP fragment floods (9.00 percent).

Interestingly, Prolexic also observed some uncommon attack types during the three month period, including SYN PUSH, FIN PUSH, and RIP floods. "In the attacks Prolexic mitigated, RIP floods were utilized in a reflection attack," said Scholly. "RIP is a legacy routing protocol not typically used as a DDoS attack vector. The inclusion of unexpected protocols in attack campaigns highlights the continued evolution and threat of DDoS toolkits."

One year ago, Prolexic tracked nine different attack types. With the addition of SYN PUSH, FIN PUSH and RIP floods, among others, types of tracked attacks have doubled to 18. "What this illustrates is the continued desire of attackers to search for new ways to deliver payloads against targets and bypass standard mitigation techniques," said Scholly.

As in all previous Prolexic quarterly DDoS attack reports, China (35 percent) is the top source country for distributed denial of service attack traffic. The United States jumped to second place, rising from 8 percent last quarter to 27 percent this quarter. Two newly ranked countries in the Q3 2012 top 10 are the UK (3 percent) and Saudi Arabia (4 percent).

Data for the Q2 2012 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Quarterly Attack Report for Q3 2012 is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q4 2012 report will be released in the first quarter of 2013.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+ and YouTube, or follow @Prolexic on Twitter.

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Believes Multiple Groups and Tactics Behind Recent High Profile DDoS Attacks

HOLLYWOOD, FL – (October 11, 2011) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that it believes the recent spate of DDoS attacks should not be attributed to just one group/individual or toolkit, as has been widely assumed.

The bot toolkit discovered to be responsible for the majority of these attacks is a PHP-based suite known as *itsoknoproblembro*; the infected hosts are known as *brobots*. However, post forensic attack analysis of a number of infected hosts conducted by the Prolexic Security Engineering & Response Team (PLXsert) point to multiple malicious actors participating in the crippling DDoS attacks using individualized toolkits and tactics. The PLXsert team found:

- Techniques of exploitation and defacements varied. In some instances hosts were taken over and defaced. In others, files were dropped and scans were setup to identify additional targets. This leads PLXsert to believe that the initial infections were performed by multiple groups (or multiple individuals).

- Forensics showed that different toolkits were used to maintain or gain access to infected hosts.

- A blend of attack scripts and different techniques during each observed campaign points to the possibility of multiple, well-organized groups.

- PLXsert was able to gain visibility into some machines and was able to prove persistence of infection going back to May 2012. The difficulty of cleanup is directly related to the number of different toolkits used and the high number of back doors installed. This supports PLXsert's hypothesis that multiple groups/individuals used different tactics.

"A blend of attack scripts and different techniques used in each campaign is another pointer to the likelihood that multiple, well-organized groups or individuals were behind these attacks," said Stuart Scholly, president at Prolexic. "As we approach the critical online holiday shopping period, there is no doubt that attackers have armed themselves with advanced toolkits capable of generating amplified and sophisticated DDoS floods."

Prolexic will issue its Q3 2012 Global DDoS Attack Report in mid-October. The report will include a detailed case study on the *itsoknoproblembro* toolkit as well as data from the recent high profile DDoS attacks. A complimentary copy of the report will be available for download at www.prolexic.com/attackreports.

About Prolexic

Prolexic Technologies is the world's largest, most trusted Distributed Denial of Service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, and follow us on LinkedIn, Facebook, Google+ and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Publishes New Executive Series White Paper: *"DDoS Denial of Service Protection and the Cloud"*

HOLLYWOOD, FL – (October 10, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has published a new white paper in its Executive Series entitled, "*DDoS Denial of Service Protection and the Cloud."*

While the advantages of the cloud in terms of time and cost savings are hard to resist, security in the cloud remains in question. One startling fact is that elementary security controls and features that have been used for decades to protect secure enterprise applications against DDoS attacks and other cyber threats are just starting to be introduced to cloud-based applications. Unprotected cloud-based applications and services are easy marks for DDoS denial of service attacks as well as other hacking activity.

So how can businesses still take advantage of the cloud and stay protected against DDoS denial of service attacks? And with DDoS mitigation services being delivered in the cloud, how can you be sure that your DDoS mitigation service provider can protect itself and you, their customer? To shed light on these critical questions, Prolexic has developed a new white paper about DDoS protection and network protection entitled, "*DDoS Denial of Service Protection and the Cloud."*

The paper explores how businesses can protect their cloud-based infrastructures and applications against a DDoS denial of service attack by using a cloud-based DDoS mitigation service. It will also offer guidance in how to evaluate cloud-based DDoS mitigation providers in terms of the strength and sophistication of their best practices around cloud security.

"Cloud security, especially against distributed denial of service attacks, is improving, but is sadly lacking for many providers of cloud-based services," said Prolexic President Stuart Scholly. "As the preeminent provider of cloud-based DDoS protection services, we wanted to share our knowledge and experience with the broader IT and security community to help them bolster their defenses against the increasing risk of Dos and DDoS attacks."

A complimentary copy of the new "*DDoS Denial of Service Protection and the Cloud* " white paper can be downloaded for a limited time from www.prolexic.com/clouddefense

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Completes SSAE 16 Examination for Distributed Denial of Service (DDoS) Attack Mitigation Services

Demonstrates Compliance with Financial Reporting and Data Security Standards

HOLLYWOOD, FL – (October 8, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has completed its SSAE 16 Type 2 SOC 1 examination. The SSAE (Statements on Standards for Attestation Engagements) 16, which replaces the SAS 70, is an internationally recognized third-party assurance audit designed for service organizations and establishes service organization reporting standards. Prolexic also simultaneously completed the ISAE 3402 examination, which is the equivalent to examination in the European Union (EU).

“Completing these examinations assures enterprises that Prolexic has adopted relevant controls that are well designed and operating properly,” said Stuart Scholly, president at Prolexic. "Global companies that must comply with these standards can now avoid the time and expense of auditing Prolexic prior to working with us.”

SSAE 16 is a standard issued by the American Institute of Certified Public Accountants (AICPA). Prolexic successfully completed an SSAE 16 examination, formerly known as a *Report on Controls of a Service Organization (SOC 1)*. The examination was performed by BrightLine CPAs & Associates, Inc., an independent CPA firm, on the scope of distributed denial of services attack mitigation services offered by Prolexic. This was a Type 2 SOC 1 examination that covered the review period of August 1, 2011 to July 31, 2012.

Prolexic is also the first DoS and DDoS mitigation provider to secure PCI DSS (Payment Card Industry Data Security Standard) level 1 certification. While PCI DSS certification is not required because Prolexic does not store or process any credit card data, certification makes it much easier for a compliant organization to engage Prolexic for DDoS protection services. Critically, certification speeds deployment of remediation for compliant organizations during encrypted Layer 7 (application layer) DDoS attacks.

About SSAE 16

SSAE No. 16, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*, AT sec. 801) is an attestation standard that establishes the requirements and guidance for reporting on controls at a service organization relevant to user entities’ internal control over financial reporting. The controls addressed in SSAE No. 16 are those that a service organization implements to prevent, or detect and correct, errors or omissions in the information it provides to user entities.

SSAE No. 16 superseded the SAS 70 audit standard in mid-2011. It is the adopted version of the International Standards for Assurance Engagements (ISAE) No. 3402, *Assurance Reports on Controls at a Service Organization*, for use in the United States.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Selected by Auction Site BidCactus.com for DDoS Denial of Service Mitigation

HOLLYWOOD, FL – (October 3, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it recently mitigated high-volume Layer 3 DDoS attacks directed at BidCactus.com, a popular online auction site. Due to the success of the emergency provisioning, BidCactus has signed a contract with Prolexic for ongoing DDoS detection and DDoS protection.

The DDoS attacks spanned two days and rendered BidCactus.com inaccessible to millions of global bidders for six hours. The site's hosting company recommended Prolexic for DDoS mitigation services after its efforts failed to stop the denial of service attacks. BidCactus.com management received a ransom demand from the denial of service attackers for several thousand Euros in exchange for stopping the DDoS attacks, but management refused to pay.

"Although any company with an online presence is vulnerable to a DDoS attack, e-Commerce companies are favorite targets for attackers who threaten with extortion," said Stuart Scholly, president at Prolexic. "BidCactus.com is typical of most online companies who will not give in to attackers' ransom demands. Now, with DDoS protection from Prolexic in place, the auction site will no longer have to worry about dealing with cyber criminals."

A small attack started in the early evening and lasted for approximately two hours before subsiding. The site experienced a stronger and more lethal DDoS attack the following morning around 10 a.m. The denial of service DDoS attack overwhelmed the site's firewall capabilities. When the site's hosting provider exhausted its resources to try to stop the attack, the provider nullrouted or blackholed BidCactus.com in order to protect other hosted sites. This resulted in a six-hour outage during which BidCactus.com was unable to conduct business.

"It's difficult to put a dollar value on an outage, but it was definitely significant in terms of our reputation," said Jeffrey Dvornek, director of technology at BidCactus.com. "Prolexic responded to our initial request for help with great speed and our site was back online almost immediately. And after Prolexic took over, the DDoS attackers never returned."

Prolexic quickly mitigated the DDoS attack on BidCactus.com using its PLXproxy DDoS mitigation service. This is the quickest way to provision Prolexic's mitigation and protection against all types and sizes of DDoS attacks. Any disruption to the site or downtime is typically resolved in just minutes.

"My advice to other online businesses would be to secure DDoS protection," said Dvornek. "The cost of denying service to a site is shockingly low. Everyone can be a target and anyone can be a potential DDoS attacker."

The infrastructure (Layer 3) attack on BidCactus.com reflects the trend toward "back to basics" DoS and DDoS attacks being favored by DDoS attackers, according to the findings of the *Q2 2012 Prolexic Global DDoS Attack Report*. A complimentary copy of the report is available for download at www.prolexic.com/attackreports.

To learn more about the DDoS attack launched against BidCactus.com, download the full case study at www.prolexic.com/bidcactus.

About Prolexic

Prolexic Technologies is the world's largest, most trusted Distributed Denial of Service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, and follow us on LinkedIn, Facebook, Google+ and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

End of Quarter DDoS Attacks Reach New Level of Size and Sophistication

Sustained Floods Peak at 70 Gbps and more than 30 million pps

HOLLYWOOD, FL – October 1, 2012 – Prolexic Technologies, the global leader in distributed denial of service (DDoS) protection services, today warned of an escalating threat from unusually large and highly sophisticated DDoS attacks.

The DDoS attacks have been launched in the last week using the so-called *itsoknoproblembro* DDoS toolkit. The malicious actor(s) behind the attacks have used this potent tool in conjunction with sophisticated attack methods that clearly demonstrate knowledge of common DDoS mitigation methods. The attack signatures are extremely complex and Prolexic has recorded sustained floods peaking at 70 Gbps and more than 30 million pps against some of its customers. Most mitigation providers would struggle to combat DDoS attacks with these characteristics.

“What we are experiencing is a dramatic uptick in the size and sophistication of DDoS attacks to a level not previously observed,” said Prolexic Chief Executive Officer Scott Hammack. “Only a handful of companies around the world could survive a hit of 70 Gbps in conjunction with the complex blend of attack vectors we have witnessed.”

The *itsoknoproblembro* toolkit includes multiple infrastructure and application-layer attack vectors, such as SYN floods, that can simultaneously attack multiple destination ports and targets, as well as ICMP, UDP and SSL encrypted attack types. A common characteristic of the attacks is a large UDP flood targeting DNS infrastructures. Uniquely, the attacking botnet contains many legitimate (non-spoofed) IP addresses, enabling the attack to bypass most anti-spoofing mechanisms.

“The size and sophistication of this threat has created a high-alert within various industries and with good reason,” said Hammack. “I’m proud to say we’ve successfully mitigated multiple *itsoknoproblembro* campaigns throughout the year, even when attack vectors have continuously modulated during the course of the assault.”

The Prolexic Security Engineering & Response Team (PLXsert) has been monitoring the *itsoknoproblembro* suite and issued an internal threat advisory to Prolexic customers earlier this month. A case study with more details about the toolkit will be included in Prolexic’s quarterly attack report, which will be published in mid-October, along with a public threat advisory that includes fingerprinted attack signatures for recommended detection and mitigation strategies. The latest threat advisories are available to the public at www.prolexic.com/threatadvisories.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q3 2012 Global DDoS Attack Report will be available shortly at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Publishes New Technical Series White Paper: *"Firewalls - Limitations When Applied to DDoS Protection"*

HOLLYWOOD, FL – (September 25, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has published a new white paper in its Technical Series entitled, "*Firewalls - Limitations When Applied to DDoS Protection.*"

While firewalls serve many purposes, this new white paper focuses on the role of a firewall during a denial of service DDoS attack. The paper discusses ways in which IT organizations can use a firewall effectively as well as the risks involved, whether the firewall represents the only DDoS protection or is part of a broader DDoS defense. If an organization uses a firewall as part of its DDoS mitigation strategy, this paper provides information to help make more informed decisions around firewall selection and management. The paper also includes a firewall management for DDoS protection assessment guide.

"In a Distributed Denial of Service situation, a firewall can provide limited blocking of malicious traffic for network protection," said Stuart Scholly, president at Prolexic. "However, IT organizations should realize that firewalls are playing an increasingly limited role in DDoS protection and this paper brings this fact to light."

A complimentary copy of the new "*Firewalls - Limitations When Applied to DDoS Protection*" white paper can be downloaded for a limited time from www.prolexic.com/firewalls

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Mitigates DDoS Attacks Against Leading European Provider of Prepaid Virtual Visa Cards

HOLLYWOOD, FL – (September 12, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it recently mitigated a high volume Layer 4 DDoS attack on EntroPay (www.entropay.com), a virtual credit card web site owned and operated by Ixaris Systems.

At www.entropay.com, anyone can open and fund an account to obtain a virtual prepaid Visa card that is accepted by millions of merchants worldwide. As the first and now most successful virtual prepaid card introduced in Europe, EntroPay provides consumers with a safe, flexible and instantaneous way of making and receiving online payments.

As awareness and popularity of the web site increased, it became a target for DDoS denial of service attacks. Although no user data was ever compromised, the DDoS attacks brought down the EntroPay site, sometimes for a considerable length of time. In response, the company increased network protection with a hardware mitigation appliance from its Internet Service Provider. However, this solution failed when EntroPay was hit with an attack that had traffic volume exceeding the appliance's limit of 100Mbps.

EntroPay then decided to engage Prolexic for DDoS detection and DDoS protection. Ixaris now uses Prolexic's PLXrouted service to provide DDoS protection for the EntroPay wen site. With this service, DDoS attacks are detected by monitoring on-premise equipment. In the event of an attack, the traffic-routing service is activated using Border Gateway Protocol (BGP) to on-ramp network traffic to Prolexic's 500 Gbps cloud-based denial of service DDoS mitigation infrastructure.

Recently, the EntroPay web site has been hit by a wide range of attack types – SYN Flood, ICMP Flood, UDP Flood – in various durations including a Layer 4 DDoS attack peaking at 700 Mbps. EntroPay has also experienced attacks characterized by high CPU usage on its routers and several UDP drops on the router's Access Control Lists (ACLs). In each case, Prolexic technicians were able to defeat the attacks in minutes. With the assistance of PLXsert (Prolexic's Security Engineering and Response Team), post-attack forensic information helped Ixaris identify where the attacks originated.

“The first half of 2012 has seen an increase in the number and size of DDoS attacks on financial industry web sites,” said Stuart Scholly, president of Prolexic. "The recent attacks against EntroPay.com is no surprise in light of the escalating activity against the financial industry.”

"As a Level 1 PCI compliant financial services provider, the security of our service is of the utmost importance so any attack is something we take very seriously," said Tim Murfet, chief information officer at Ixaris Systems. "Once our traffic is routed through Prolexic's network, we're immediately back in business."

With DDoS attacks against financial web sites on the rise, Murfet recommends that DDoS protection be treated like a disaster recovery plan that should be regularly tested to ensure that everyone in IT knows how to respond during an attack.

"It's important to have good communication with your DDoS mitigation provider even in non-attack situations and to test the service regularly so you'll know it will work when you need it," Murfet advised. "For a financial services company like ours that requires 100 percent uptime, we need the peace of mind that Prolexic mitigation services provide."

To learn more, the full EntroPay.com case study can be downloaded from www.prolexic.com/entropay. More information on Prolexic's mitigation activities and the attacks directed at its global client base, including EntroPay, is published in Prolexic's *Q2 2012 Quarterly Global DDoS Mitigation Report*. A complimentary copy can be downloaded from www.prolexic.com/attackreports.

About EntroPay

EntroPay is one of the most cost-effective, easy and rapid means for businesses and consumers to remit funds around the world through less-restricted access to global payment networks (Visa, Mastercard, SWIFT). It is a highly recognized payment platform among online companies and has a strong track record of converting customers when offered as a payment alternative. EntroPay has operated since 2003 by Ixaris Systems, which is authorized by the UK Financial Services Authority under the Payment Service Regulations 2009 for the provision of payment services, with FSA registration number 540990. For more information, visit www.entropay.com.

About Prolexic

Prolexic Technologies is the world's largest, most trusted Distributed Denial of Service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, and follow us on LinkedIn, Facebook, Google+ and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Launches New Online DoS and DDoS Attack Glossary

PLXsert Defines Hacker Jargon to Aid Businesses and Media

HOLLYWOOD, FL – August 30, 2012 – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has added an extensive glossary of DoS and DDoS terms to its online Knowledge Center, explaining the tools and methods hackers use to target organizations.

The Glossary of Terms defines more than 60 common acronyms and technical terms used to describe DDoS attacks. Such attacks increased 10 percent in Q2 2012, according to the Prolexic Security Engineering & Response Team (PLXsert). Armed with this new resource, at-risk businesses can now decipher industry jargon to better understand the nature of a potential denial of service threat.

"When faced with a DDoS attack, confusion can quickly set in, especially when an organization's key IT personnel are unavailable," said Stuart Scholly, Prolexic's president. "Decision makers typically aren't familiar with these terms, but have to act fast. This glossary provides one more tool to help them promptly assess the situation and take appropriate action to mitigate any damage."

Media outlets will also benefit from access to the glossary. Whether covering amplification attacks or UDP protocols, reporters can easily research complex technical aspects of cybercrime and inform the general public with greater accuracy.

"Malicious hackers already know this stuff," said Scholly. "They know the difference between a Layer 4 and a Layer 7 attack. When businesses and media can speak their language, too, it becomes more difficult to catch a potential target off guard."

Prolexic will update the Glossary of Terms frequently to keep pace with emerging threats and trends. The Glossary is available to the public free of charge at www.prolexic.com/ddos-glossary and does not require registration.

About Prolexic

Prolexic Technologies is the world's largest, most trusted Distributed Denial of Service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit prolexic.com, and follow us on LinkedIn, Facebook, Google+ and @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Exposes Critical Vulnerabilities in Popular Dirt Jumper DDoS Toolkit Family

PLXsert Offers Free Vulnerability Disclosure Report

HOLLYWOOD, FL – August 14, 2012 – Prolexic Technologies, the global leader in distributed denial of service (DDoS) protection services, today released a vulnerability disclosure report on the Dirt Jumper DDoS Toolkit family, exposing weaknesses in the command and control (C&C) architecture that could neutralize would-be attackers. The Dirt Jumper family of toolkits is considered one of the most popular attack tools on the market today.

"DDoS attackers take pride in finding and exploiting weaknesses in the architecture and code of their targets. With this vulnerability report, we've turned the tables and exposed crucial weaknesses in their own tools," said Scott Hammack, chief executive officer at Prolexic.

Armed with the identity of the C&C server or infected host, and open source penetration-testing tools, it is possible to gain access to the C&C database backend and, more importantly, the server-side configuration files.

"With this information, it is possible to access the C&C server and stop the attack," Hammack said. "Part of our mission is to clean up the Internet. It is our duty to share this vulnerability with the security community at large."

In conjunction with the Dirt Jumper vulnerability disclosure report, the Prolexic Security Engineering & Response Team (PLXsert) has also issued a public threat advisory on the newest member of the Dirt Jumper family, Pandora. Both documents are available to the public, free of charge, at www.prolexic.com/threatadvisories.

Believed to be authored by the same individual responsible for the other Dirt Jumper family of toolkits, it includes five DDoS attack methods, designated Attack Types 0 through 4. These include HTTP Min, HTTP Download, HTTP Combo, Socket Connect and Max Flood. The HTTP Combo offers a one-two punch that targets the application and infrastructure layer simultaneously, while the Max Flood attack initiates a flood that contains a 1-million-byte payload within the POST request.

One advertisement for the toolkit claims that 10 infected bot workstations can take down an unhardened or poorly protected site, while a thousand bots supposedly slowed response times for Russia's most popular search engine.

Prolexic already successfully mitigated a Pandora attack, which targeted KrebsOnSecurity.com on July 27, using the Max Flood attack method. It was the first documented use of the toolkit by PLXsert, and site owner Brian Krebs blogged about it last week.

“The first DDoS campaigns consisted of several hundred systems repeatedly requesting image-heavy pages on my site,” Krebs wrote. His site went down, and the traffic hurled at it was beginning to cause problems for other sites. On the recommendation of his hosting provider, Krebs turned to Prolexic for help and was able to fight off the attack.

Although effective, the code of the Pandora DDoS toolkit contains typographical errors, Prolexic analysts noted. Infected computers (bots) beacon to the user’s command and control (C&C) panel with broken GET requests that identify the availability of the bots. In addition, a GET request in the Socket Connect attack is sent as an ‘ET’ request, which is invalid HTTP request. Some web servers such as Apache, however, will interpret the ET request as a GET request and will respond with a valid OK response. Other web servers, such as nginx, will return a Bad Request error message.

“The DDoS problem is not going away and it’s only going to get worse,” Krebs says. “As illustrated by the denial of service attacks on my site using the Pandora toolkit, it’s never been easier to build your own DDoS bot army.”

An analysis of the Pandora threat, including recommended mitigation techniques, is available free of charge at www.prolexic.com/threatadvisories.

To learn more about the attack on KrebsOnSecurity.com, the full case study can be downloaded from www.prolexic.com/Krebs.

Prolexic Threat Advisories

Designed to provide early warnings of new or modified DDoS attack signatures and scripts, recently observed by PLXsert, each threat advisory contains a detailed description of the type of attack, a list of attack signatures, and the specific network infrastructure or application that it targets. In addition, Prolexic’s DDoS mitigation experts also offer insight into the nature of each type of attack, as well as provide specific warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXsert also provides threat remediation tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them. The latest threat advisories, including HOIC and Dirt Jumper, are available to the public at www.prolexic.com/threatadvisories.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q2 2012 Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic DDoS Protection Services Selected by Financial Services Technology Firm Global eSolutions, Hong Kong

HOLLYWOOD, FL – (August 7, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that its DDoS detection and DDoS protection services have been selected by Global eSolutions (Hong Kong) Limited, a provider of trading technology that enables fast trade execution via personal computer and mobile devices.

One Global eSolutions client is an online foreign exchange (Forex) and Contracts for Difference (CFD) trading firm headquartered in the U.K. This firm is a fully regulated brokerage in London's dynamic financial district and leverages the innovative trading technology provided by Global eSolutions. Recently, its Forex trading web site was a target of a DDoS attack after management did not respond to a ransom demand from cybercriminals.

Initially Layer 3 and Layer 4 volumetric floods interrupted web site availability for approximately four hours. A second, more damaging application layer (Layer 7) attack occurred three weeks later, rendering the trading platform almost inaccessible to online traders.

Prolexic has charted an upward trend in Layer 7 attacks against its global client base in its *Quarterly Global DDoS Attack Reports*. Data shows Layer 7 attacks increasing from 17% in Q3 2011 to 21% in Q4 2011 and reaching 27% in Q1 2012. Interestingly, Prolexic's most recent attack report for Q2 2012 shows Layer 7 attacks declining to 19% as attackers returned to more common DDoS data floods. A complimentary copy of the Q2 2012 Report can be downloaded at www.prolexic.com/attackreports.

Global eSolutions IT technicians detected the DDoS attack when they noticed that the sessions and memory status of the firewall were abnormally high and bandwidth was fully consumed. They found that there were over 80,000 different IPs accessing the network. First, Global eSolutions IT experts tried to block some of the IPs that looked suspicious. When that didn't work, the firm requested that its two ISPs in Asia black hole the traffic to its site. This action made it impossible for most legitimate traders and users to access the Forex trading platform and other applications, damaging the company's reputation and customer trust.

"Global eSolutions got caught up in the wave of DDoS attacks that flooded the online financial services industry in the early months of 2012," said Stuart Scholly, Prolexic's president. "The large ransom received by one of the firm's clients indicates that cybercrime against financial companies is only getting more serious and prevalent."

Today, Global eSolutions has Prolexic's PLXrouted service in place to provide DDoS protection against attacks on its Forex trading platform and other components of its Internet facing infrastructure. In event of a DDoS attack, all site traffic will be routed to Prolexic's cloud-based mitigation platform where malicious traffic will be removed. Clean traffic can then be routed back to the site.

"Prolexic has the strongest defense against DDoS so we can give our customers the confidence that our Forex trading platform is secure and available," said Ramon Chan, systems architect at Global eSolutions. "I would advise other online trading services companies to be proactive and have a DDoS mitigation service in place."

To learn more, the full Global eSolutions case study can be downloaded from www.prolexic.com/pr_globalesolutions.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in- the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Publishes New Technical Series White Paper: *12 Questions to Ask a DDoS Mitigation Provider*

HOLLYWOOD, FL – (July 25, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has published a new white paper in its Technical Series entitled "*12 Questions to Ask a DDoS Mitigation Provider*."

The paper presents 12 key questions that decision makers should ask a DDoS mitigation service provider, whether a pure-play provider, ISP or Content Delivery Network (CDN), before engaging their services. It also offers guidance to help evaluate a vendor's response to each question and what to expect in terms of DDoS detection and DDoS protection services.

"With so many providers entering the marketplace, there's a lot of confusion about DDoS detection and DDoS protection services," said Prolexic President, Stuart Scholly. "One way to determine which providers can really deliver what they promise is to ask some tough, technical questions. This paper should be an invaluable resource for decision makers as they evaluate current or prospective providers and the DDoS protection services they offer."

Choosing a DDoS protection provider is one of the most important business decisions for an online company today – one that can have serious financial ramifications if not made properly. Prolexic developed the 12 key questions in its white paper based on its own customers' inquiries and nearly a decade of experience providing DDoS detection and DDoS protection to some of the world's leading brands.

A complimentary copy of the new "*12 Questions to Ask a DDoS Mitigation Provider*" white paper can be downloaded from www.prolexic.com/12technicalquestions

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in- the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Application Layer (Layer 7) DDoS Attacks Decline According to Prolexic's Q2 2012 Report

HOLLYWOOD, FL – (July 17, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that the number of application layer (Layer 7) attacks against its global client base declined in Q2 2012. This is one of a number of key findings contained in the company's Quarterly Global DDoS Attack Report, which was released today.

Even though the total number of DDoS denial of service attacks increased 10% this quarter, the Prolexic Security Engineering & Response Team (PLXsert) logged an 8% decline in application layer DDoS attacks, which accounted for 19% of all attacks. Infrastructure attacks (Layer 3 and 4) against bandwidth capacity and routing infrastructures totaled 81%.

"Q2 data showed a return to traditional infrastructure attacks and is likely a reflection of changing tools for launching DDoS attacks," said Stuart Scholly, president of Prolexic. "With Layer 7 attacks, the risk of detection and eventual take down by law enforcement increases because these attacks disclose the IP address of the attacking botnet and this may be another reason for their decline this quarter."

GET Floods, the most popular Layer 7 attack type, continued to decline in popularity. In Q2 2011, GET Flood attacks accounted for 22% of all DDoS attack campaigns mitigated by Prolexic. In Q2 2012, GET Flood attacks account for just 14%.

PLXsert also identified a rise in popularity for certain types of infrastructure-directed DDoS attacks: ICMP, SYN, and UDP floods. In Q2 2011, these attack types accounted for 55% of attacks mitigated by Prolexic. In Q1 2012, they accounted for 59% and this quarter, the total percentage has increased to 67%.

Other highlights from the Q2 2012 Global DDoS Attack Report

Compared to Q1 2012

- 10% increase in total number of attacks
- 8% rise in Layer 3 and 4 infrastructure attacks
- Average attack duration declines to 17 hours from 28.5
- China retains its position as the main source country for DDoS attacks

Compared to Q2 2011

- 50% increase in total number of DDoS attacks
- 11% increase in infrastructure (Layer 3 & 4) attacks
- Shorter average attack duration: 17 hours vs. 26 hours
- 63% higher packet-per-second (pps) volume

Analysis and emerging trends

This quarter, DDoS attacks against Prolexic's global client base were evenly spread across all vertical industries - financial services, e-Commerce, SaaS, payment processing, travel/hospitality, and gaming. "No industry was spared this quarter, illustrating that denial of service is a global, mainstream problem that all online organizations must face," said Scholly.

In Q2 2012, average attack duration for Prolexic clients continued to decline, dropping to 17 hours from 28.5 hours the previous quarter. "Once DDoS attackers realize they are up against Prolexic's cloud-based DDoS mitigation infrastructure, they typically move on and choose easier targets where they can have much greater impact," explained Scholly.

Despite a low number of DDoS attacks in April and May, Q2 2012 was active overall, with the total number of denial of service attacks increasing by 10% compared to Q1 2012. This quarter, June was by far the most active month, accounting for 47% of the quarter's total number of DDoS attacks. The week of June 3-10 was the most active when PLXsert logged 14% of the entire quarter's total number of DDoS denial of service attacks. Interestingly, this period of high activity coincided with the beginning of the UEFA Euro 2012 soccer tournament.

As in previous attack reports, China (33%) is the top source country for distributed denial of service attack traffic and this quarter it is joined at the top of the list by Thailand (23%) and the United States (8%).

"While Layer 7 attacks show a slight decline overall, organizations cannot afford to be complacent because you never know when one will strike" warned Scholly. "If your Internet-facing infrastructure is critical to business operations, you'll need a DDoS mitigation service that can block volumetric infrastructure attacks, but also all application layer attacks, including HTTPS, GET and POST Floods."

Data for the Q2 2012 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Quarterly Attack Report for Q2 2012 report is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q3 2012 report will be released in the fourth quarter of 2012.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Leading UAE Bank Mashreq Partners with Prolexic to Implement DDoS Protection Services

HOLLYWOOD, FL – (JUNE 20, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that Mashreq, one of the leading financial institutions in the United Arab Emirates (UAE), will be supported by Prolexic's DDoS detection and DDoS protection services in the event that attacks are directed against its web site.

Since 1967, Mashreq has provided banking and financial services to millions of customers and businesses. With a growing retail presence in the region, including Egypt, Qatar, Kuwait and Bahrain as well as representative offices worldwide, awareness of the bank has increased along with the likelihood of DDoS attacks.

Mashreq has relied on the DDoS detection and DDoS protection services of its own security infrastructure, however, with DDoS attacks against financial institutions becoming larger and more intense, the bank took a proactive step to add more robust DDoS protection. Now, as a Prolexic client, when attacks become too large or complex to handle internally, it can draw upon Prolexic's industry-leading 500 Gbps cloud-based mitigation platform and technicians based at the company's Security Operations Center.

"Hosting providers, even with large networks and dedicated internal resources, are no match for today's complex application layer or high packet-per-second attacks", said Neal Quinn, chief operating officer at Prolexic. "Having additional DDoS defenses in place is critical for protecting hosted sites in the banking and financial services sector in light of the recent surge of attacks on this industry."

DDoS Attacks on Financial Services Sector Increases in Q1 2012

According to the *Prolexic Global Attack Report Q1 2012* compiled by the Prolexic Security and Engineering Response Team (PLXsert), financial services sites were hard hit by DDoS attacks in Q1 2012. During Q4 2011, over 168 trillion bits of data and 14 billion packets of malicious traffic were identified as targeting financial services clients. In Q1 2012, 5.7 quadrillion bits of data and 1.1 trillion malicious packets were identified and successfully mitigated, representing a 3,000% increase in malicious packet traffic over Q4 2011.

"Prolexic has observed that DDoS attackers are taking a more direct strategy and focusing on specific targets such as financial services," Quinn said. "Mashreq's adoption of Prolexic's DDoS protection services illustrates how financial services firms can be proactive against online threats."

Recent DDoS attacks on banks in the UAE illustrate the urgency for online financial services firms and their hosting providers to be well prepared with DDoS defenses. Recently, both domestic and global sites of UAE banks were hit with an application layer (Layer 7) attack of 10 Mbps for approximately 10 days, resulting in intermittent site performance issues.

David Horton, Head of Strategy at Mashreq, said, "Given the recent increase in DDoS attacks against banks locally and globally, Mashreq engaged Prolexic as a protective measure for attacks that our internal resources may not be equipped to handle. Recently recognized as 'The Best Regional Retail Bank", Mashreq has market leading online and mobile banking solutions for its customers, so protecting these services against disruption is of paramount importance to us. The age old advice certainly applies here – prepare for the worst and hope for the best."

A complimentary copy of the *Prolexic Global Attack Report Q1 2012* can be downloaded from www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in- the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

HULK DoS Tool More Hype than Threat

PLXsert Shares Simple Defense Strategies to Neutralize Attackers

HOLLYWOOD, FL – (June 1, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a threat advisory on the *HTTP Unbearable Load King* (HULK) denial of service (DoS) script. The script was developed by a network security researcher and shared publicly on his blog. Because of his role, the tool attracted widespread attention – and generated panic – throughout the digital security industry.

Though it was intended as an educational proof-of-concept, it exposed common weaknesses that could be exploited by malicious actors to bring down servers that have not been optimally configured for performance and DDoS resistance.

"What makes HULK dangerous is the fact that a single malicious actor with a single computer could feasibly take down a small, unhardened web server in minutes. We've tested the tool internally and it is functional," said Neal Quinn, chief operating officer at Prolexic.

"Fortunately, this is not a very complex DoS tool," he added. "We were quickly able to dissect its approach and stop it dead in its tracks. It is fairly simple to stop HULK attacks and neutralize this vulnerability with the proper configuration settings and rules."

HULK, released May 17, uses randomized header and parameter values to generate a threaded GET flood attack; the randomized requests make it more difficult to distinguish attack threads from legitimate traffic, particularly for automated mitigation solutions. HULK takes advantage of out-of-the-box web server configuration vulnerabilities and spawns 500 threads that collectively stream random GET requests at its website target upon launch, bypassing caching engines to exhaust server resources.

The Prolexic Security Engineering & Response Team (PLXsert) immediately instituted rules to defend against and mitigate HULK attacks and issued a detailed threat advisory to Prolexic customers last week. As a public service, full details of the HULK threat, including recommended mitigation techniques and SNORT rules, are available at www.prolexic.com/threatadvisories.

"There is a lot at stake for businesses online - whether it's a matter of money, reputation, regulatory compliance or business continuity. No one wants to be down for a second, let alone hours or days," Quinn noted. "Consequently, any threat can cause panic. While many DDoS threats are very real and severe, in the case of HULK, panic is not necessary. PLXsert is happy to share our practical, effective mitigation method that can be implemented on any WAF or content switch, and transform the HULK back into Dr. Banner."

Prolexic Threat Advisories

Designed to provide early warnings of new or modified DDoS attack signatures and scripts, recently observed by PLXsert, each threat advisory contains a detailed description of the type of attack, a list of attack signatures, and the specific network infrastructure or application that it targets. In addition, Prolexic's DDoS mitigation experts also offer insight into the nature of each type of attack, as well as provide specific warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXsert also provides threat remediation tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them. The latest threat advisories, including HOIC and Dirt Jumper, are available to the public at www.prolexic.com/threatadvisories.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q1 2012 Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Defends Dominican Republic Central Electoral Board Against DDoS Attacks

HOLLYWOOD, FL – (May 29, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that it has mitigated a number of attacks directed at the web site of Junta Central Electoral (JCE), the central electoral board of the Dominican Republic during a recent general election.

A DDoS attack uses multiple sources, often from compromised desktop systems (also known as a botnet), to flood a target system with legitimate looking requests. The target system is overwhelmed causing infrastructure failure and the inability to service normal users.

In the weeks before the general election, which took place on May 20, 2012, JCE realized its web site (http://www.jce.gob.do/) could be a potential target for a DDoS attack. As a preemptive measure, it secured DDoS detection and DDoS protection services from Prolexic on May 8, 2012.

As expected, on the day of the general election (May 20), Prolexic's Security Operations Center engineers detected a high amount of traffic targeting one of the JCE's virtual IPs. Within minutes, Prolexic security engineers created DDoS mitigation filters to block the attack. The attacker then launched a Layer 7 (application layer) attack, which was also blocked.

"Politically motivated DDoS attacks are increasingly common and are often timed to coincide with high profile events such as elections or executed in response to specific government actions," said Stuart Scholly, president at Prolexic. "The key to minimizing disruption is being proactive and putting DDoS protection in place ahead of time."

Despite significant attempts to bring down JCE's web site, good communication between Prolexic's security engineers and Daniel Joseph from JCE defeated these attacks.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Mitigates Politically Motivated Layer 7 DDoS Attack Against Client of VirtualRoad.org

HOLLYWOOD, FL – (May 16, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it mitigated an application layer (Layer 7) attack on behalf of VirtualRoad.org (www.virtualroad.org). This web hosting company based in Scandinavia provides a safe web presence for global, independent news media and human rights organizations that are denied freedom of expression in their home countries.

Unlike more common bandwidth floods aimed at the network (Layer 3) or transportation (Layer 4) layers, application layer (Layer 7) attacks can be structured to overload specific elements of an application server infrastructure. Even simple attacks – for example those targeting login pages with random user IDs and passwords, or repetitive random "searches" on dynamic web sites – can critically overload CPUs and databases.

In March 2012, one of VirtualRoad.org's independent news media clients in Asia came under a complex Layer 7 GET flood attack. VirtualRoad.org's DDoS mitigation team routed the client's traffic to Prolexic's 500 Gbps cloud-based mitigation platform.

Prolexic's Security Operations Center (SOC) quickly determined the type of attack and discovered that it was launched through a large multi-hop proxy network in order to mask the attackers' source IP address. In minutes, Prolexic mitigated an attack that could have brought the site down for many days or weeks.

"Launching DDoS attacks for politically and ideologically motivated purposes is not new, but is increasing in frequency," said Neal Quinn, chief operating officer at Prolexic. "This illustrates the ubiquity of DDoS and that targets are no longer limited to high profile commercial web sites."

VirtualRoad.org offers DDoS mitigation services as a core part of its standard and customized packages of web hosting services. As part of an agreement with Prolexic, VirtualRoad.org can leverage resources at Prolexic's SOC to mitigate large and complex attacks that are beyond the capacity and capabilities of its own network and technicians.

"The collaboration between VirtualRoad.org and Prolexic works extremely well because we can leverage Prolexic's proven experience in protecting large enterprises against DDoS attacks to give our social justice clients more peace of mind," said Thomas Hughes, director, Media Frontiers, the parent company of VirtualRoad.org. "Our partnership with Prolexic is now a crucial element of our mitigation services, and thanks to Prolexic's proven expertise, our clients can continue their freedom of expression without disruption, even in an increasingly hostile web environment."

To learn more, read the full case study at www.prolexic.com/virtualroad.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in- the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Mitigates Layer 7 GET Flood DDoS Attacks Against Enterprise Payment Processing Platform

HOLLYWOOD, FL – (May 8, 2012) – Prolexic, the global leader in Distributed Denial of Service (DDoS) protection services, announced today that it has mitigated several DDoS attacks against a URL used by online merchants for payment processing.

The payment processing platform is owned by IPG Holdings Limited, an independent, privately-owned technology company that specializes in the development, maintenance, and support of enterprise payment gateways delivered through Software-as-a-Service (SaaS). IPG hosts payment forms for some large direct merchants and payment service providers and these front-facing forms have been vulnerable to DDoS attacks.

“DDoS attackers are constantly finding new ways to modify bots to infiltrate online businesses and wreak havoc by disrupting the processing of customer transactions,” said Neal Quinn, chief operating officer at Prolexic. “IPG is another example of the increasing sophistication of DDoS attacks, which reinforces the need for DDoS protection for all e-Commerce providers.”

In the case of IPG, the attackers’ bots picked up the IPG payment processing URL and included it in an attack on multiple merchant sites. At first, IPG mitigated these attacks by blackholing the IP address of the payment form, which had come under attack. However, this meant that a merchant's ability to process payments ceased immediately, causing serious disruptions in revenue flow and financial losses for their suppliers.

Using more than 20 proprietary and commercial mitigation tools, Prolexic technicians quickly identified two attacks on the payment platform URL. The first was an 8-hour GET Flood, which peaked at 350 Mbps and 380,000 packets-per-second (pps). As that attack was mitigated, the attackers ramped up their efforts, launching a multi-vector attack consisting of a GET Flood, UDP Fragment, and RESET Flood which peaked at 200 Mbps, 50,000 pps and 4.5 million connections per second. This attack lasted for over 3 days before the attackers gave up after every attack signature change was immediately thwarted in real-time by Prolexic’s technicians.

Today, IPG collaborates with Prolexic to offer merchants a DDoS-protected payment form URL, which IPG manages on behalf of the merchant as part of its service offering. This protection has been put in place for all IPG merchants/customers who have come under DDoS attack to date.

"As part of our DDoS protection strategy, IPG is proactively offering the form-based service offering and referring larger merchants to the Prolexic service to protect their front end sites as well," says Alan Conder, chief executive officer at IPG. "With DDoS threats becoming more sophisticated, I would suggest to other online businesses to have a pre-planned strategy in place so they have pre-meditated steps they can take to deal with an attack if or when it arises."

To learn more, read the full case study at www.prolexic.com/ipg.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in- the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook and Google+ or follow @Prolexic on Twitter.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Issues Global Warning about Recent DDoS Blackmail Attempts Targeting Online Gambling Sites

HOLLYWOOD, FL – (April 30, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today reported a troubling trend in DDoS attacks targeted at online gambling sites, with multiple attacks accompanied by extortion letters.

During the past month, more than two dozen online gambling companies have come under attack and been targeted using similar attack methods. In recent days, multiple businesses in the online gambling sector have received extortion emails, demanding payments of up to US$50,000 to prevent new waves of DDoS attacks. The blackmail attempts have included escalation clauses, warning of increased size or frequency – as well as time-related price increases to stop them.

"The online gambling industry should be on high alert," said Neal Quinn, chief operating officer at Prolexic. "This appears to be a coordinated global threat. This is a focused level of effort accompanied by blackmail tactics, targeting a single industry in a compressed timeframe."

All the extortion attempts have mentioned DDoS capabilities associated with the Dirt Jumper DDoS toolkit, which the Prolexic Security Engineering and Response Team (PLXsert) first reported in a December threat advisory. The latest version of Dirt Jumper, v5, includes specific anti-DDoS functionality, designed to thwart protection services such as those offered by Prolexic.

"We've already identified and mitigated Dirt Jumper v5 attacks and instituted globalized rules to protect our customers. Our defenses have been fortified and our clients have been prepared," Quinn said.

"Business in all industries should be vigilant against Dirt Jumper 5," Quinn added. "Our experience shows that new DDoS threats frequently come to market in the online gambling industry before spreading to other targets."

PLXsert offers a custom scanning tool called Dirt Dozer (dirtdozer.py) that enables security research teams and engineers to validate if any suspected HTTP command and control servers utilize any strains of the malware. Prolexic's Dirt Dozer scanner is available free of charge and can be downloaded from www.prolexic.com/threatadvisories.

In the coming weeks, PLXsert will issue a public threat advisory on Dirt Jumper v5, including a detailed breakdown of attack signatures by attack type, as well as information on remediation and recommended mitigation strategies.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q1 2012 Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Threat Advisory: Booter Shell Scripts Turn DDoS Attacks into Child's Play

New Hacking Tactic Hijacks Web Servers, Enables DDoS as a Service

HOLLYWOOD, FL – (April 25, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a threat advisory on the use of booter shells, which allow hackers to readily launch DDoS attacks without the need for vast networks of infected zombie computers. As a public service, full details of the booter shell threat are available at www.prolexic.com/threatadvisories.

"Increased use of techniques such as booter shells is creating an exponential increase in the dangers posed by DDoS attacks," said Neal Quinn, chief operating officer at Prolexic. "For hackers, DDoS attacks have never been easier to launch, while for their victims, the power and complexity of attacks is at an all-time high. The threat of a DDoS attack has never been more likely or its potential impact more severe. We've entered the age of DDoS-as-a-Service."

The increased use of dynamic web content technologies, and the rapid deployment of insecure web applications, has created new vulnerabilities – and opportunities for hackers to use infected web servers (instead of client machines) to conduct DDoS attacks.

Traditional DDoS attacks make use of workstations infected with malware, typically infected through spam campaigns, worms or browser-based exploits. With these traditional tactics, hackers needed multitudes of infected machines, to mount successful DDoS attacks.

DDoS booter scripts, however, are simple standalone files that execute GET/POST floods when accessed via HTTP. With booter shells, DDoS attacks can be launched more readily and can cause more damage, with far fewer machines. Web servers typically have 1,000+ times the capacity of a workstation, providing hackers with a much higher yield of malicious traffic with the addition of each infected web server.

Furthermore, the skill level required to take over a web server and convert it into a DDoS zombie has been significantly reduced. A DDoS booter shell script can be easily deployed by anyone who purchases hosted server resources or makes use of simple web application vulnerabilities such as RFI, LFI, SQLi and WebDAV exploits.

The power, availability and ease-of-use of booter shell scripts has lowered the barrier to entry for launching a DDoS attack, putting attacks within reach of even novice hackers. Many booter shell scripts, tools and lists of infected hosts are freely available in the hacker underground, or can be available for a nominal fee.

"The design and deployment of DDoS attack tools have been greatly simplified. At the same time the power of attacks has increased because server capacity and bandwidth is being utilized instead of workstation bandwidth," Quinn said. "Businesses have to be prepared for DDoS attacks of a nature they may never have seen before."

The best way to prevent infection is with continuous testing of proprietary web applications, as well as repeated testing of known vulnerabilities in commercial applications, either in-house, or through a third-party service, such as Prolexic.

Prolexic Threat Advisories

Designed to provide early warnings of new or modified DDoS attack signatures and scripts, recently observed by PLXsert, each threat advisory contains a detailed description of the type of attack, a list of attack signatures, and the specific network infrastructure or application that it targets. In addition, Prolexic's DDoS mitigation experts also offer insight into the nature of each type of attack, as well as provide specific warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXsert also provides threat remediation tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them. The latest threat advisories, including HOIC and Dirt Jumper, are available to the public at www.prolexic.com/threatadvisories.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q1 2012 Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Financial Services Firms Hit by DDoS Attacks According to Prolexic's Q1 2012 Report

Malicious packet volume increases 3,000% quarter over quarter

HOLLYWOOD, FL – (April 11, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that financial services firms were in the cross hairs of attackers during Q1 2012. This is one of a number of key findings contained in the company's **Quarterly Global DDoS Attack Report**, which was released today.

The Prolexic Security Engineering & Response Team (PLXsert) team logged an almost threefold increase in the number of attacks against its financial services clients during Q1 compared to Q4 2011, as well as a 3,000% increase in malicious packet traffic. The company also mitigated more attack traffic this quarter than it did in all of 2011.

"This quarter was characterized by extremely high volumes of malicious traffic directed at our financial services clients," said Neal Quinn, Prolexic's vice president of Operations. "We expect other verticals beyond financial services, gaming and gambling to be on the receiving end of these massive attack volumes as the year progresses."

During Q4 2011, over 168 trillion bits of data and 14 billion packets of malicious traffic were identified as targeting financial services clients. This quarter, 5.7 quadrillion bits of data and 1.1 trillion malicious packets were identified and successfully mitigated, representing a 3,000% increase in malicious packet traffic over Q4 2011.

Other report highlights

Compared to Q1 2011

- 25% increase in total number of DDoS attacks
- 25% increase in Layer 7 (application layer) attacks
- Shorter attack duration: 28.5 hours vs. 65 hours
- Decline in UDP Floods and increase in GET Floods

Compared to Q4 2011

- Total number of attacks was virtually unchanged
- 6% rise in Layer 7 attacks
- Average attack duration declined to 28.5 hours from 34 hours
- China remains the top source country for attacks but the U.S. and Russia both move up in the rankings

Key trends to watch

In Q1 2012, average attack durations continued to edge down, dropping from 34 hours in Q4 to 28.5 hours this quarter. Of note, average attack bandwidth increased to 6.1 Gbps, up from 5.2 Gbps in the previous quarter. Taken together, these two metrics confirm previous trend predictions of shorter attack durations, but with higher traffic volumes. This conclusion can be drawn when comparing data from Q1 2012 and Q4 2011 as well as Q1 2012 and Q1 2011.

Infrastructure layer attacks targeting Layer 3 and Layer 4 continue to be the choice of attackers, however, this quarter showed a 6% increase in DDoS attacks targeting the application layer (Layer 7). PLXsert believes that there will be a gradual shift to Layer 7 attacks over the long term. Regarding attack types over the last 12 months, UDP Floods have declined in popularity with SYN Floods emerging as the "go to" attack type.

"The expertise of Prolexic's Security Operations Center staff and the unrivaled capacity of our cloud-based mitigation platform minimized the impact of these large attacks against their targets," said Quinn.

Data for the Q1 2012 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Quarterly Attack Report for Q1 2012 report is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q2 2012 report will be released in the third quarter of 2012.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Recommends Developing Mitigation "Playbook" to Reduce Impact of DDoS Attacks

HOLLYWOOD, FL – (March 28, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, is recommending that all online businesses should develop a mitigation playbook to minimize the disruption and confusion that typically occurs at the outset of a DDoS attack. This is a best practice that Prolexic implements with all clients.

In simple terms, a playbook is a rehearsed and tested plan that outlines in detail who in an organization needs to be involved in the event of a DDoS attack, their roles and responsibilities, as well as a detailed communications strategy.

"DDoS attacks are deliberate, targeted events – happening on a daily basis – that demand a preparedness plan much like homeowners preparing for hurricane season," said Neal Quinn, Prolexic's vice president of Operations. "When the hurricane inevitably hits, they don't panic because they knew what to expect and what steps to take to protect their investment."

To maintain business continuity, Prolexic encourages online businesses to make DDoS mitigation part of their enterprise incident response practices. During the first quarter of 2012, more than six of Prolexic's top global financial services clients received significant DDoS attacks. Because they had worked with Prolexic to develop and test a mitigation playbook in advance, the usual panic that can grip an organization during a DDoS attack was avoided. In addition, Prolexic was able to deploy its mitigation services faster and more efficiently.

Building a proven playbook

Prolexic recommends that companies work with their DDoS mitigation service provider to create a simulated DDoS attack or dry run that makes no actual changes to the network. This will help management see the best way to manage both internal and external communications when confronted with a DDoS attack. The incident response team then works through the DDoS attack without doing an actual live test, much like a military training drill in which no live ammunition is used.

Depending on the size and complexity of the organization, this type of dress rehearsal exercise can be completed in a little more than an hour, or slightly longer if the company's incident response plan has additional requirements. Executive management will understand how long it takes to put the mitigation plan into action. Following this exercise, optimizations may be developed to ensure a rapid, repeatable and predictable action plan.

Optimizing communications during attack events

To streamline communications and ensure a fast, controlled response to DDoS attacks, Prolexic recommends that organizations focus on three critical areas of communications:

- **Managing communications** – DDoS attacks have an impact not just on IT, but on all users of the company's services, including non-technical departments. It should be clear who is to be called and what to do when issues arise during a DDoS attack. Prolexic advises incident response teams to have a single point of contact for relaying information and sending short Twitter-like updates internally across the organization. These notes should be confidential and help people understand what is going on during the attack so that they don't panic and create an additional internal crisis.

- **Identifying key contact persons –** The main goal of the playbook is to eliminate organization-wide panic that can delay the mitigation response when a DDoS attack occurs, so it is vitally important that the right people be notified of the attack immediately. By completing a simulation exercise, everyone in the triage team will understand what their role is in the DDoS mitigation process, what changes they need to make to the network, and how they can continue to maintain business as usual even when some resources are unavailable.

- **Organizing information for easy, fast accessibility** – Something as simple as keeping all names and phone numbers of key contacts in a single place can save valuable time. This facet of the DDoS mitigation process is all about containment and order – how to turn a DDoS attack from a major disaster into an incident that is routine when handled according to the well-rehearsed playbook.

As part of the playbook, Prolexic recommends outlining procedures and policies for setting up teleconference bridges. Typically, these would include:

- **A Mitigation Bridge –** primarily for engineers to coordinate and monitor mitigation efforts

- **A Troubleshooting Bridge –** primarily for engineers and application owners to investigate any problems arising during the on-ramping

- **A Security Emergency Response Team (SERT) Bridge –** primarily for security and forensics participants

"When everyone in an organization – not just IT staff– understands what it is really like to be under a DDoS attack before one actually occurs, they will be able to face the actual event with more confidence, control and calm," said Quinn. "As a result, the DDoS mitigation process will go more smoothly for a faster return to business as usual. That is why Prolexic advises all of our customers to prepare themselves for the real thing with a simulated DDoS incident and to incorporate DDoS into their incident response plan."

For more information on building a DDoS mitigation playbook, go to www.prolexic.com/playbook to download the free Prolexic white paper, *Plan vs. Panic: Making a DDoS Mitigation "Playbook" a Part of Your Incident Response Plan.*

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Issues Threat Advisory Outlining DDoS Protection Strategies for High Orbit Ion Cannon

Latest Stealth Attack Tool Targets Hundreds of URLs Simultaneously

HOLLYWOOD, FL – (February 23, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today released a threat advisory for the High Orbit Ion Cannon (HOIC), an increasingly popular attack tool that can target up to 256 web addresses simultaneously. As a public service, full details of the HOIC threat, including recommended protection strategies, are available at www.prolexic.com/threatadvisories.

"A DDoS attack can come from anywhere, anytime. It can be an act of revenge for a real or perceived slight, a political statement or completely random. No business is immune to becoming a target," said Paul Sop, chief technology officer at Prolexic.

"As the world's most advanced experts in DDoS protection and mitigation, we feel it is our duty to arm the public with the tools and information they need to protect themselves from emerging DDoS attack tools such as HOIC," he said.

The Prolexic Security Engineering and Response Team (PLXsert) continuously reviews and analyzes DDoS attack patterns and emerging trends to develop the intelligence and tools to prevent and combat DDoS attacks. HOIC DDoS protection strategies have already been put in place for Prolexic's customers. In addition, as part of its public mission, PLXsert issues quarterly attack reports, as well as periodic threat advisories.

Considered the next generation replacement for the Low Orbit Ion Cannon (LOIC) flood attack tool, HOIC also includes support for booster files – customizable scripts that randomize attack signatures and make attacks more difficult to differentiate from legitimate traffic.

"On its own, the HOIC tool is limited. It still requires a coordinated group attack to bring a site down," said Neal Quinn, VP of Operations at Prolexic. "But with the booster scripts – which are already circulating widely among hacker circles – a group attack gains the advantage of stealth. It becomes much more difficult to identify and mitigate, prolonging the outage caused by the attack."

The DDoS underground has been urging participants to abandon the LOIC tool in favor of HOIC, making it likely that HOIC-based attacks will become increasingly common.

"The ability to hit up to multiple targets simultaneously (instead of just one with LOIC), and the use of randomization to evade detection, makes HOIC a threat to any business with a presence online," Quinn said. "Businesses should take steps now to protect themselves, either by following our recommendations or subscribing to a DDoS protection service."

Prolexic Threat Advisories

Designed to provide early warnings of new or modified DDoS attack signatures and scripts recently observed by PLXsert, each threat advisory contains a detailed description of the type of attack, a list of attack signatures, and the specific network infrastructure or application that it targets. In addition, Prolexic's DDoS mitigation experts also offer insight into the nature of each attack type and provide specific warnings about how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXsert also provides threat remediation tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them. The latest threat advisories, including HOIC and Dirt Jumper, are available to the public at www.prolexic.com/threatadvisories.

About the Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q411 Global DDoS Attack Report is available at www.prolexic.com/attackreports.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's 20 largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Unveils New DDoS Mitigation Service at the 2012 RSA Conference

HOLLYWOOD, FL — (February 21, 2012) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced that it will introduce PLXconnect, a new Routed Mitigation Service, at the 2012 RSA Conference (Moscone Center, San Francisco, CA) on February 27, 2012.

PLXconnect provides a new way to activate Prolexic's industry-leading DDoS mitigation solutions. With a direct physical connection from a client's network to Prolexic's scrubbing centers via a private cloud, PLXconnect provides Prolexic clients with a high bandwidth option and predictable latency through an industry leading Service Level Agreement (SLA).

"PLXconnect is ideal for organizations that desire a high bandwidth solution for on-demand mitigation that is easier to set up and manage," said Neal Quinn, vice president of operations at Prolexic. "Deploying the PLXconnect service is as simple as deploying a normal Internet connection and greatly simplifies activation for customers with large, complex networks."

Because PLXconnect leverages a private cloud, it eliminates the complex network changes that are required when using an Internet-based routing solution like Generic Route Encapsulation (GRE). As a result, PLXconnect will be welcomed by businesses that operate a complex Internet edge deployment using many protocols and site to site VPNs or have complex application interactions.

"Prolexic has also extended our industry leading Service Level Agreement and we're offering a latency and packet loss SLA for PLXconnect," Quinn said. "That's not possible with GRE over the public Internet and it demonstrates Prolexic's firm commitment to meeting the demands of our customers."

Prolexic is exhibiting in booth 2735 at the 2012 RSA Conference.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's twenty largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Secures US$8 Million Series B Funding Led by Camden Partners

HOLLYWOOD, FL – (February 8, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that it has closed an US$8 million Series B investment led by Camden Partners, a Baltimore-based private equity firm. The additional funding will be used to support staff, network and service augmentation.

"Prolexic grew more than 55% last quarter, and our growth rate should continue increasing throughout 2012," said Scott Hammack, Chief Executive Officer of Prolexic. "This Series B investment, while not necessary because Prolexic was profitable last year, will enable us to accelerate our growth and bring forward a number of strategic initiatives that will further solidify our global leadership position."

According to a recent Gartner report, "DDoS mitigation services should be a standard part of business continuity/disaster recovery planning and be included in all Internet service procurements when the business depends on the availability of Internet connectivity. Any Internet-enabled application that requires guaranteed levels of availability should employ DDoS protection to meet those requirements."[1]

Jason Tagler, Principal at Camden Partners, said Prolexic fits the firm's strategy of partnering with fast growing companies in specific markets. "Prolexic is the clear leader for DDoS mitigation and with the increasing frequency of attacks globally, demand for the company's services remains strong. We look forward to helping the company fulfill its tremendous potential," said Tagler. Effective immediately, Jason Tagler will join Prolexic's Board of Directors as Camden Partners' representative.

Details of Prolexic's mitigation activities and insights into the latest tactics, types, targets and origins of global DDoS attacks are provided in quarterly reports published by the company. A complimentary copy of Prolexic's Q411 global report issued yesterday can be downloaded from www.prolexic.com/attackreports.

In 2011, Prolexic completed two financings led by Kennet Partners totaling US$15.9 million. "Prolexic has a proven management team, sustained revenue growth and a growing market opportunity. We are obviously very excited to continue supporting the company's global expansion," said Gustavo Alberelli, Director at Kennet Partners and a member of Prolexic's Board of Directors. "Camden Partners' network of relationships and overall experience will be invaluable as Prolexic launches new Cloud security services and embarks on its next stage of growth in 2012."

[1] Gartner, "Hype Cycle for Infrastructure Protection, 2011", 8/10/11

About Camden Partners

Founded in 1995, Camden Partners is one of the largest growth equity and investment management funds in the United States with more than US$700 million under management. Camden focuses on the technology-enabled business services, healthcare and education sectors. For more information, please visit www.camdenpartners.com

About Kennet Partners

Kennet is a leading international growth equity firm that invests in companies in North America and Europe. Kennet supports entrepreneurial technology businesses with expansion capital to accelerate growth and build exceptional shareholder value. Kennet is an experienced investor with approximately US$600 million in funds under management. www.kennet.com

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Records Dramatic Rise in Packet-Per-Second Volume in Q411 Global DDoS Attack Report

HOLLYWOOD, FL – (February 7, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that data collected during Q411 global attacks against its clients indicates a significant rise in packet-per-second (PPS) volume. Full details and statistics of the company's quarterly DDoS mitigation activities are available in a complimentary quarterly report that can be downloaded from www.prolexic.com/attackreports.

"Based on fourth quarter statistics, Prolexic predicts that 2012 will feature DDoS attacks that will be shorter in duration, but much more devastating in terms of packet-per-second volume," said Paul Sop, chief technology officer at Prolexic. "Think of it this way. In the past, attackers had a rifle. In 2012, they have a machine gun with a laser site." Prolexic predicted this increase in PPS volume in its previous attack report and noted that attackers were changing their strategy.

Report highlights

Compared to Q410:

- Prolexic mitigated 45% more DDoS attacks
- Prolexic mitigated 7 times more attack traffic
- PPS volume increased 18-fold
- Average attack duration was down to 34 hours from 43 hours

Other highlights:

- Prolexic mitigated more than twice as many attacks in Q411 compared to Q311
- In Q411, approximately 22% of attacks were ICMP floods, 20% were UDP Floods, 20% were SYN Floods and 16% were GET Floods
- November was the month with the greatest number of total attacks, but the highest volume of attacks occurred during the period of December 3-10, which is a peak buying and shipping period before the holidays
- Clients in the e-Commerce sector received a disproportionately high percentage of Layer 7 (application layer) attacks and much longer average attack durations
- The top three countries from which attacks originated were Japan, China, and Germany with Japan-based IP addresses accounting for 35% of attacks
- Average attack bandwidth was 5.2 Gbps compared to 2.1 Gbps in Q311, an increase of 148%
- Average attack bandwidth was 2.6 Gbps in 2011 compared to 1.1 Gbps in 2010, an increase of 136% year over year

Key trends to watch

Prolexic believes Q411 data is indicative of several key trends that will shape the DDoS mitigation landscape in the coming year.

“We have seen a trend toward shorter overall attack duration, but with unprecedented high packet-per-second volume and lethal attack signatures,” said Sop. “This is a devastating cocktail that can quickly bring down even well protected sites and their mitigation providers. We are starting to see packet-per-second attack volumes that are simply off the charts.”

The findings in Prolexic’s Q411 Attack Report also indicate a somewhat surprising surge of DDoS attacks originating from Japan, a geographic location rarely in the top ten source countries and usually not known for large concentrations of botnets. Prolexic speculates that this activity may stem from temporarily lax security practices when many global vendors set up impromptu communication networks after the tragedy in Japan.

The fourth quarter also saw a rise in Layer 7 (application layer) attacks against e-Commerce companies, which is not surprising since online retailers and ancillary service providers such as shippers are prime attack targets during the fourth quarter holiday shopping season. Indeed, data from Q4 showed that the highest number of attacks occurred during the week of December 3-10. Average attack duration was also significantly higher for attacks directed at e-Commerce businesses.

“The Internet is becoming a more dangerous place for online companies that do not have a high level of DDoS protection,” Sop said. “With regard to DDoS attacks, we expect 2012 to be one of the most challenging years for all online businesses. As such, it’s critical to continually evaluate the vulnerabilities of your network and the capabilities of your mitigation provider to ensure they are keeping pace with this ever increasing threat.”

Sop suggests that companies start becoming more proactive in their defenses by leveraging better traffic monitoring and analysis tools that provide greater Layer 3 and 4 DDoS alert accuracy and faster identification and analysis of Layer 7 attacks. The faster attacks can be recognized, the faster they can be mitigated, which minimizes site downtime and lost revenue.

As the size and frequency of DDoS attacks continue to rise, Prolexic is keeping pace. In Q411 the company opened a new scrubbing center in Ashburn, VA and significantly increased the size of its global attack mitigation network. Demand for Prolexic’s services is increasing rapidly and the company recorded a 45% growth in revenues for 2011.

Data for the Q411 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Quarterly Attack Report for Q411 is available as a free PDF download from www.prolexic.com/attackreports. Prolexic's Q112 report will be released in the second quarter of 2012.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Launches “Protected by Prolexic” Program

Protected by Prolexic Logo on Customers’ Web Sites
Indicates Gold Standard Defense Against DDoS Attacks

HOLLYWOOD, FL – (February 2, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that it has launched a new customer program called “Protected by Prolexic.” Prolexic will offer incentives to new and existing customers who sign up to display the Protected by Prolexic logo on their web sites.

“By joining the Protected by Prolexic program, businesses will be sending a strong, clear message to customers, competitors, and even cyber attackers that they are taking the threat of DDoS attacks seriously enough to secure the services of the gold standard in DDoS mitigation,” said Paul Sop, chief technology officer at Prolexic. “When they see this logo, online customers will have added peace of mind that a DDoS attack will not bring down sites they rely on for shopping, membership services, entertainment, and other online activities.”

The Protected by Prolexic logo is a registered trademark that belongs exclusively to Prolexic. To prevent unauthorized duplication and misuse of the logo, Prolexic will provide each customer a unique HTML code that hyperlinks to a numbered logo hosted by Prolexic.

“The Prolexic name is known all over the world as the leader in DDoS mitigation and many of the businesses we serve already use our recognized reputation as a selling point to their customers,” Sop said. “Displaying the Protected by Prolexic logo will give these businesses an instant competitive advantage through association with the ‘gold standard’ for DDoS mitigation.”

“We have been proactive and added premium DDoS attack protection from Prolexic and that has increased the value of our web hosting service,” said Lisa Retief, Vice President of Engineering at Yola (www.yola.com), a global web site builder and hosting service serving small businesses. “Prolexic’s protection provides peace of mind to Yola and our customers from around the world.”

Certain terms and conditions surrounding the use of the Protected by Prolexic logo apply. Businesses that are interested in participating in the Protected by Prolexic program can learn more by logging on to www.prolexic.com/protected or by contacting protected@prolexic.com

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Enhances Portal to Provide Customers With More Insight into DDoS Threats and Mitigation

HOLLYWOOD, FL – (January 19, 2012) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced it has launched an enhanced Prolexic Portal, an online resource that provides customers with greater visibility and insight into Prolexic's monitoring and cloud-based mitigation services.

"The Prolexic Portal opens the door to a robust view of reports, graphs, alerts, and statistics that give our customers more insight into DDoS threats on their network and how we mitigate them," said Paul Sop, chief technology officer at Prolexic. "Most importantly, the Portal helps us work with our clients in a closer and more coordinated manner."

A key highlight of the Prolexic Portal is the Flow Based Attack Monitor that provides subscribers to the optional service with a "customer view" of traffic that passes through their routers. Updated every five minutes, the Flow Based Attack Monitor includes access to all DDoS alerts and traffic profiles.

In addition, Prolexic customers can view Network Flow Based Alerts for all DDoS events detected on traffic traversing the customer's network. Clients can also view bandwidth graphs, which illustrate the volume of clean bandwidth that traverses their network. This is updated in five-minute intervals and the bandwidth volume can be viewed in time-selectable intervals. Reports, including Prolexic DDoS mitigation reports, customer site traffic profiles, alerts, and DDoS attack statistics can also be accessed through the Portal.

The Prolexic Portal also gives customers a robust set of account management tools to help them save time and gain greater efficiency. Additionally, all Prolexic customers have access to an in-depth document library within the Portal that contains standard service documents such as current provisioning documents, service descriptions and web optimization guides. Customers can also obtain fast and secure access to Prolexic's 24/7, 365-day support team consisting of the world's most highly trained DDoS mitigation technicians based at the company's Security Operations Center.

"The Prolexic Portal is another important way that we can help our customers minimize the disruption and financial impact of DDoS attacks, while illustrating the value that Prolexic provides," Sop said. "This latest enhancement and new features are customer-driven and so far, feedback has been very positive."

Key Features

Password protected and only accessible to Prolexic customers, the Portal features a full complement of monitoring statistics, reports, and alerts, including:

- **Flow Based Attack Monitor** – Available to customers who subscribe to Prolexic's Flow Based Monitoring service.

- **Reports** – Quick access to traffic profiles, alerts and DDoS attack statistics.

- **Bandwidth graphs** – Illustrates the volume of clean bandwidth that traverses the customer's network.

- **Network Flow Based Alerts** – Tied to action items and customer contact within a time-to-notify service level agreement.

- **Proxy statistics –** Provides easy access to statistics related to proxy traffic that traverses through the customer's network, including unique visitors, cache properties and URL and host requests.

- **HTTP statistics –** Proxy customers can access statistical information related to inbound requests for all traffic passing through the customers network.

- **Attack statistics –** All Prolexic customers have access to post-mortem attack event statistics, which are summarized by attack size, duration, and type.

- **Ticket Listing** – All Prolexic customers can easily create and view service tickets.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Revenues Increase 45 Percent in 2011

Significant investments in staffing, R&D and network capacity to accommodate growth

HOLLYWOOD, FL — (January 12, 2012) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced that it achieved profitability and a year of record growth in 2011. Since completing a US$13.9 million financing in March led by Kennet Partners, a leading technology growth equity investor, and putting in place a new executive management team, the company significantly increased its staffing, R&D investment and network capacity to better service its clients worldwide.

"I am delighted to report a compound annual growth rate of 45 percent for 2011," said Scott Hammack, chief executive officer at Prolexic. "To maintain service delivery excellence, we have doubled the number of Prolexic employees since the beginning of the year and increased attack bandwidth capacity to over 400 Gbps."

In December, Prolexic opened a new scrubbing center in Ashburn, Va. to counter the increasing volume of DDoS attacks. In addition, Prolexic also doubled network capacity at its other scrubbing centers located in San Jose, London and Hong Kong. Prolexic already had the world's largest attack mitigation network and this latest enhancement elevates capacity far beyond any other DDoS mitigation provider.

In addition to investing heavily in its attack mitigation network, Prolexic also devoted significant resources to research and development in 2011. "DDoS mitigation is a very dynamic business that requires continuous innovation to stay ahead of malicious attackers," said Hammack. "To maintain our leadership position and protect our clients against emerging DDoS threats, Prolexic will significantly broaden its solutions portfolio in 2012."

During the year, Prolexic also doubled its customer base. The company added organizations in the public sector as well as many Fortune 2000 business enterprises to its roster. Currently, six of the world's 10 largest banks are Prolexic customers along with many leading companies in other "at-risk" industries including, e-Commerce, SaaS, travel/hospitality, healthcare, and online gaming/gambling.

"Prolexic is ideally positioned to protect organizations from the increasing number and severity of DDoS attacks and we expect this to translate into continued growth in 2012," said Hammack. "We enter the New Year with strong momentum and high expectations."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Issues Dirt Jumper Threat Advisory and Releases Free Security Scanner

HOLLYWOOD, FL — (December 29, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced it has issued a threat advisory for Dirt Jumper, a high-risk DDoS toolkit that can be used to launch application layer attacks on web sites. Prolexic has also developed a security-scanning tool that can be used to detect Dirt Jumper command and control servers. The threat advisory and scanner can be downloaded free of charge from www.prolexic.com/threatadvisories.

Dirt Jumper is a prepackaged toolkit that has evolved from the Russkill strain of malware. It is now widely available on various underground websites and retails for as little as US$150. Dirt Jumper can be spread via spam, exploit kits, fake downloads and can be pushed out to machines already infected with other forms of malware.

"The Dirt Jumper DDoS toolkit is currently one of the most aggressive malware strains used by DDoS attackers globally," said Neal Quinn, vice president of operations at Prolexic. "Increasingly, we are seeing this tool used against clients worldwide and it is likely to become more widespread and effective as distribution spreads."

After analyzing the Dirt Jumper v3 DDoS Toolkit, the Prolexic Security Engineering and Response Team (PLXSERT) categorized it as a high-risk threat. The Prolexic team identified the newest variant, known as Dirt Jumper September and uncovered that it had updated functionalities as well as an enhanced control panel, which makes it simple for attackers to use. Prolexic's Dirt Jumper Threat Advisory provides an analysis of the payload and also gives a detailed breakdown of attack signatures by attack type, as well as information on remediation and recommended mitigation strategies.

PLXSERT has also written a custom-scanning tool called Dirt Dozer (dirtdozer.py) that enables security research teams and engineers to validate if any suspected HTTP command and control servers utilize any strains of the malware. As a public service to business enterprises and organizations worldwide, Prolexic's Dirt Dozer scanner is being made available free of charge and can be downloaded from www.prolexic.com/threatadvisories.

Prolexic Threat Advisories

Prolexic recently launched a service that provides its subscribers with regular Threat Advisories. Compiled by the Prolexic Security Engineering and Response Team (PLXSERT), on-going advisories will help subscribers stay informed and vigilant so they can make better, proactive decisions.

Designed to provide early warnings of new or modified DDoS attack signatures and scripts recently observed by PLXSERT, each Threat Advisory contains a detailed description of the type of attack, a list of attack signatures, and the specific network infrastructure or application that it targets. In addition, Prolexic's DDoS mitigation experts also offer insight into the nature of each type of attack, as well as provide specific warnings as to how the attack will affect businesses and enterprises of different sizes and infrastructures. PLXSERT also provides threat remediation tips to help subscribers not only recognize the new attack signatures, but also proactively defend against them.

"The more our subscribers understand about DDoS attacks, the more they will be able to make informed decisions about DDoS protection and mitigation strategies," said Paul Sop, chief technology officer at Prolexic. "As the industry's premium provider, Prolexic is ideally positioned to provide this unique level of insight and intelligence to our customers."

New Threat Advisories will be distributed to subscribers via email and will also be posted on the Prolexic Portal, a password protected, subscriber-only resource.

About the Prolexic Security Engineering & Response Team (PLXSERT)

PLXSERT monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXSERT is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXSERT team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer, Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

DDoS Attack on Noticias24.com is Abandoned After Traffic is Provisioned Through Prolexic

HOLLYWOOD, FL – (December 15, 2011) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that the company was engaged by Noticias24.com, a popular international news outlet in Venezuela, to provide protection against Distributed Denial of Service (DDoS) attacks.

Noticias24 is the most popular online news web site in Venezuela and ranks as the fifth most visited Spanish-language news web site in the world, with 15 million visits and 58 million page views per month.

Recently, the Noticias24 web site was subjected to a 10-hour DDoS attack launched by extortionists from Russia. In the two months prior to the attack, the attackers had demanded a ransom from Noticias24. When management did not respond, the attackers launched an exceptionally large Layer 7 DDoS attack of 30 Gbps. Noticias24 had contracted for DDoS mitigation services through its hosting provider, but the hosting provider could not mitigate this magnitude of attack and Prolexic was brought in.

After determining that it was a Layer 7 attack, Prolexic's DDoS mitigation technicians assisted Noticias24 in changing its DNS name servers to route all site traffic to servers in Prolexic's global scrubbing centers – thus stopping any malicious traffic from reaching Noticias24.com. Once the site traffic was flowing through Prolexic's cloud-based scrubbing centers, it took about an hour to route the DNS changes to Prolexic. In this case, the attackers abandoned the attack as soon as they saw that Noticias24's traffic was being routed through Prolexic.

"Hosting companies and ISPs simply do not have the bandwidth, advanced tools, experience, and live attack monitoring expertise that Prolexic has so it should be no surprise that they are overwhelmed by attacks of this nature," said Paul Sop, chief technology officer at Prolexic. "This case also clearly illustrates how attackers sometimes abandon their campaigns when they realize Prolexic's mitigation network, which is by far the largest in the world, stands between them and success."

"The fact that we have Prolexic in front of us caused that attacker to turn away," said Ana Diaz, co-founder and president of Noticias24. "Now, Noticias24 is no longer an easy target for DDoS attack, especially the Layer 7 attacks that can really damage a business. My advice to other news sites and online companies would be to be prepared for Layer 7 attacks of the magnitude we experienced and call a professional firm like Prolexic to defend your site."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Selected by Web Hosting Provider Yola to Protect More Than 6 Million Customer Sites

HOLLYWOOD, FL – (December 7, 2011) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that Yola (www.yola.com), is using its DDoS mitigation service to protect its corporate web site and servers where the sites of more than six million web hosting customers reside.

As a business that is 100 percent dependent on the Internet and providing uninterrupted availability for its customers' web sites, protection from DDoS attacks was critical for Yola. According to Vice President of Engineering Lisa Retief, Yola looked for a best-in-class partner that could maintain service uptime and mitigate all types of DDoS attacks, no matter how large or complex. After reviewing many options, Yola selected Prolexic.

"Prolexic's premium service ensures that any potential malicious traffic will be prevented from getting through to us and our customers," said Retief. "We are also able to tell our customers that they are getting premium DDoS attack protection which differentiates and increases the value of our web hosting service."

As noted in Prolexic's **Q3 2011 Global Attack Report**, the potency of DDoS attacks continues to increase, causing site unavailability and in some cases financial loss. While hosting providers, ISPs and Content Delivery Networks offer DDoS mitigation as a lower cost, "add on" option, these basic services are often overwhelmed by large, complex attacks. Because web site availability was critical to Yola and its 6 million customers, it selected Prolexic, the industry's premier service provider.

Since choosing to partner with Prolexic, Prolexic's Security Operations Center (SOC) has mitigated a number of DDOS attacks against Yola that have had peak traffic levels reaching 6.2 Gbps. "We are happy to be able to offer this service to Yola's users and to further demonstrate our commitment to providing world-class website building and hosting services," said Trevor Harries-Jones, president at Yola.

Prolexic protects Yola and its six million customer web sites with DDoS mitigation services that combine proprietary analysis and mitigation tools, plus the expertise of 24/7 real-time monitoring by Prolexic technicians based in the company's Security Operations Center (SOC).

About Yola

Yola is at the forefront of the Web 2.0 movement, offering a free website creation tool that empowers small businesses, non-profits, and everyday users to easily create professional quality websites. Yola's intuitive drag-and-drop technology enables users to easily incorporate a variety of widgets including YouTube videos, Google Gadgets, PayPal shopping cart widgets, and many more without needing to leave Yola or to see any html code. Privately-held Yola, backed by Reinet Fund, is the recipient of numerous industry accolades including Business Week's 50 Best Tech Start-ups, The Industry Standard 100, and Fast Company's Fast 50 Reader Favorites. The company is headquartered in San Francisco, CA. For additional information, please visit www.yola.com.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Contact:
Dave Saxton
VP Marketing and Business Development
Yola
marketing@yola.com
+1 (415) 227 0250

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Opens New Scrubbing Center in Ashburn, Virginia to Counter Increasing DDoS Attacks

Sets new standard in the DDoS mitigation industry for attack handling capacity

HOLLYWOOD, FL – (December 5, 2011) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced the opening of a new Internet traffic-scrubbing center in Ashburn, Va. This latest addition to Prolexic's global network raises the bar for DDoS mitigation capacity and is a direct response to the increasing size and frequency of DDoS attacks as noted in Prolexic's recent Q3 2011 Global Attack Report which can be accessed at www.prolexic.com/attackreports.

"This one scrubbing center is now able handle twice as much volume as the largest DDoS attack recorded this year," said Neal Quinn, vice president of Operations at Prolexic. "We've taken this step based on our own projections that show DDoS attacks increasing in frequency, size and complexity."

When a DDoS attack on a customer's web site begins, Prolexic re-routes all incoming site traffic through its cloud-based scrubbing centers before returning clean traffic back to the client's network. As a result, Prolexic technicians can quickly mitigate a DDoS attack and bring the customer's web site back online in minutes.

Located in Ashburn, Va., Prolexic's newest scrubbing center is ideally positioned to help government agencies based in Washington, D.C. that host their web sites locally. Locating a scrubbing center close to where a web site is hosted can be beneficial when fighting the largest DDoS attacks. With the increase in global social unrest and "hacktivism", Prolexic expects these attacks against government agencies to increase.

In Prolexic's recently published Q3 2011 Global Attack Report, the company noted that attackers are now beginning to directly target DDoS mitigation appliances, which are vulnerable to high packet-per-second rates. "With this significant increase in mitigation capacity, Prolexic is taking a bold, proactive step in order to protect its customers as the size and speed of DDoS attacks continue to increase," said Quinn. "It's critical to always stay ahead of the curve."

Prolexic's own figures, compiled by its Security Engineering and Response Team, show that malicious traffic has averaged 2.39 Gbps so far this year. "These numbers are significant and show no sign of declining," said Quinn.

A singular focus on DDoS mitigation

Prolexic is one of the few companies dedicating 100 percent of its investment toward DDoS mitigation. Many other providers offer DDoS mitigation as an add on service and often, multiple service lines share the same network infrastructure. This can be problematic during a massive DDoS attack. For example, a DNS provider or hosting services company may try to maintain network performance for other customers by routing the attacked company's web traffic to a "black hole." While this protects the provider's core business lines and customers, the attacked company's web site will likely be inaccessible until the attack is mitigated, which could take days. As a pure play, cloud-based DDoS mitigation provider, Prolexic does not have these conflicts of interest.

"DDoS mitigation is our only business and no other company is investing as heavily in fighting back against the escalating threat of these cyber attacks," said Quinn. "Prolexic already has an industry leading mitigation network and these latest enhancements cement our position as the gold standard for DDoS mitigation."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Mitigates World's Largest Packet Per Second DDoS Attack in 2011

69 Million PPS Attack Illustrates Emerging Trend Toward Targeting DDoS Mitigation Appliances

HOLLYWOOD, FL – (November 21, 2011) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that the company mitigated the largest DDoS attack event in 2011 in terms of packets-per-second (PPS) volume. The attack target was a large Asian customer and its DNS service provider and it occurred between November 5 and November 12, 2011. Prolexic cautions organizations with an online presence that this magnitude of attack is confirmation of the trend toward DDoS attacks of escalating size and complexity as documented in Prolexic's Q3 2011 attack mitigation report which can be accessed at http://www.prolexic.com/attackreports.

According to Paul Sop, chief technology officer at Prolexic, the volume of the multi-event, randomized attack reached an unprecedented peak level of 69 million packets per second, bandwidth of 45 Gbps of traffic per second, and 15,000 connections per second. These are attack rates that no standalone automated DDoS mitigation appliance or service from an ISP or major carrier would be able to successfully mitigate. Attackers used six different attack signatures during the event, including a combination of bandwidth-driven Layer 3 and targeted Layer 7 attacks aimed at the organization's critical application layer. Prolexic mitigated a total of four separate DDoS attacks over the course of the event, which lasted 7 days and 20 hours.

"This attack was three times larger in packets per second volume than the biggest attack Prolexic has mitigated previously, which also occurred in 2011" said Sop. "Frankly, we are not surprised since we have seen an almost four-fold increase in packet volume since Q3 2010. This increase reflects an emerging strategy in which attackers directly target a company's DDoS mitigation appliances, which are commonly vulnerable to such attacks, as they cannot handle such high PPS rates. Prolexic is staying one step ahead of this trend through additional investments in DDoS mitigation infrastructure in the regions where we've seen the greatest increase of botnet activity and thus the greatest influx of extremely large attacks."

Using Prolexic's proprietary mitigation tools and live monitoring strategy, Prolexic technicians quickly identified a randomized attack consisting of the largest volume of GET, SYN, ICMP, UDP and DNS floods launched in a single attack campaign this year. They also identified that the attack was coming from botnets in multiple worldwide locations with China being the primary location of the highest recorded botnet traffic. In addition, unlike typical DDoS attacks that are coordinated from one geographic source, this attack was much more sophisticated because it was coordinated globally. Despite the unprecedented volume and complexity of the attack, time-to-mitigation in each DDoS attack was within minutes of the time traffic began flowing through the Prolexic scrubbing centers.

An early warning for the 2011 holiday online shopping season

Sop warns that this steady escalation in attack size and complexity will be especially threatening to e-Commerce businesses during the 2011 holiday season. He also cautions that other industries such as hospitality, gaming, and shipping services, should also be on high alert for DDoS attacks in Q4 2011 as botnet activity continues to ramp up in the Asia Pacific region. Sop advises that having attack prevention measures in place from a DDoS mitigation specialist is the best defense against attacks of escalating size and complexity during the online holiday shopping season and beyond.

"Prolexic succeeded in mitigating what was the largest DDoS attack this year in part because we could provide 24/7 real-time monitoring and immediate response to changing attack signatures," said Sop. "Prolexic specializes in mitigating high bandwidth attacks, so we had already invested in the technology and training to be ready for this exceptional attack. And we're ready to mitigate even larger attacks in the future."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

> NEWS

PROLEXIC
DDoS Attacks End Here.

Prolexic Charts Changing Nature of DDoS Attacks In New Quarterly Attack Report

HOLLYWOOD, FL – (November 17, 2011) – Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that data collected during Q3 2011 indicates a change in tactics by attackers. Full details and statistics of the company's quarterly DDoS mitigation activities are available as a complimentary download at www.prolexic.com/attackreports.

"Prolexic technicians are on the front lines fighting DDoS attacks every day, therefore, we're able to gather valuable data on the tactics, types, origins, and targets of these attacks," said Paul Sop, chief technology officer at Prolexic. "As a service to our customers and the global business community, Prolexic will publish a report each quarter to provide greater insight into current DDoS trends and threats."

Highlights of the Q3 2011 Prolexic Attack Report include:

- Prolexic mitigated 66% more attack traffic this quarter compared to Q3 2010.
- The volume of packets-per-second (PPS) has almost quadrupled compared to Q3 2010, illustrating a significant increase in the size and diversity of attacks over the past 12 months.
- Of all attacks mitigated by Prolexic, approximately 24% were SYN floods, 22% were ICMP floods, and 19% were UDP floods, indicating a change in attack tactics.
- Network layer (Layer 3) attacks were the most common, making up 83% of total attacks with application layer attacks (Layer 7) accounting for the remaining 17%.
- Average attack duration was 1.4 days and the average speed of traffic mitigated was 1.5 Gbps.
- The highest volume of attacks occurred during the period of August 19-25 and August was the month with the highest number of attacks overall.
- The top three countries from which attacks originated were China, India, and Turkey with China-based IP addresses accounting for 55% of attacks.
- Online gambling was the most heavily targeted industry with an average traffic speed of 1.3 Gbps and average attack duration of 1.2 days

Key trends to watch

According to Sop, the Q3 2011 data is indicative of several key trends that online companies should take seriously, especially as the busy holiday shopping season approaches.

“First and foremost, I think the nature of DDoS attacks are changing,” Sop said. “Attackers know most businesses have some level of DDoS protection and they are now starting to directly target DDoS mitigation equipment, most of which do not have the capacity to process the high packet per second attacks that are being used.”

The findings in the Q3 2011 Prolexic Attack Report also indicate a steady rise in certain attack types, especially high packet per second (PPS) SYN and ICMP floods. “High PPS SYN floods, in particular, target DDoS mitigation appliances by exhausting their processing capabilities with millions of small packets per second, which are commonly vulnerable to such attacks. For example, popular 10 Gbps appliances often exhibit peak handling rates of less than 5 million packets per second. The prevalence of high packet per second SYN floods indicates a change in strategy where attacks are less sophisticated, but more deadly,” said Sop.

According to Sop, online retailers and e-Commerce businesses are at the greatest risk of attack in the final quarter of the year, even if they have DDoS mitigation in place. “The simple truth is that automated mitigation tools and providers who offer only basic mitigation capabilities are likely to struggle against these kinds of attacks because they do not have an infrastructure in place with sufficient packet per second processing capacity,” he said.

This quarter also saw a significant number of attacks against the online gambling industry, which is often the first to be targeted with new variants. “We can expect some of these newer variants to show up in attacks against other businesses in other sectors over the coming months,” warned Sop.

Data for the Q3 2011 report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXSERT). The group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXSERT is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXSERT team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

A complimentary copy of the Prolexic Quarterly Attack Report for Q3 2011 is available as a free PDF download from www.prolexic.com/attackreports. Prolexic’s fourth quarter report will be released in January, 2012.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:

Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Introduces New Service to Provide DDoS Attack Forensics and Analysis

Creates new Security Engineering and Response Team (PLXSERT)

HOLLYWOOD, FL — (November 17, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced that it has created a data forensics and analysis group that will provide detailed pre- and post-attack data to clients as a subscription service. The new group and service is called Prolexic Security Engineering and Response Team (PLXSERT).

Formed in February 2011 as an internal research group, PLXSERT has been providing data forensics to select clients based on its insight into global DDoS threats and activities, as well as specific client attacks. Feedback from clients has been so positive that the service is now being made available on a subscription basis to all Prolexic clients.

"We are on the front lines counteracting more DDoS attacks daily than any other company and this provides a very rich data source to mine," said Neal Quinn, vice president of Operations at Prolexic. "Our hope is that the data and insight PLXSERT is providing can help organizations make more informed decisions and be proactive in defending against DDoS attacks."

PLXSERT is currently providing DDoS threat information in two forms. Threat Advisories are being issued to clients on an ad hoc basis, proving insight into specific threats, including steps clients can take to defend against them. PLXSERT is also compiling data on a quarterly basis and will issue attack reports that provide insight into Prolexic's mitigation activities for the most recent three-month period, including the volume of attacks, the most common attack types, and countries where attacks are originating. The first attack report for Q3 2011 can be downloaded from www.prolexic.com/attackreports.

The PLXSERT service can provide value to customers both before and after attacks. With intelligence gleaned from monitoring threats around world it is possible to identify botnet characteristics without having received any DDoS traffic. As a result, organizations can be alert and prepared ahead of time before an attack begins. Similarly, deep post-attack analysis can provide best practices to help minimize the impact of future attacks.

"PLXSERT lays the foundation for a more intelligent approach to DDoS monitoring and more successful mitigation," said Quinn. "What has helped us internally win against DDoS attackers is now being made available to our customers."

About the Prolexic Security Engineering & Response Team (PLXSERT)

PLXSERT monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXSERT is able to build a global view of DDoS attacks, which is shared with customers. By identifying the sources and associated attributes of individual attacks, the PLXSERT team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Michael E. Donner
SVP, Chief Marketing Officer
Prolexic
media@prolexic.com
+1 (954) 620 6017

Prolexic Predicts Increasing DDoS Attack Durations Against e-Commerce Companies During Holiday Season

Company launches marketing campaign to help e-Commerce companies prepare

HOLLYWOOD, FL — (October 31, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced it expects attack durations to increase during the upcoming holiday season, especially against companies with an e-Commerce presence.

"Last year we saw attack durations spike in the last three weeks of the year," said Neal Quinn, Vice President of Operations at Prolexic. "Our data shows that the two highest average attack duration figures for the entire year – six days and almost eight days – were recorded during the last two weeks of the year. Typically, we see average attack duration of one to three days so with longer attacks you can expect more downtime and more financial impact."

e-Commerce companies are particularly susceptible to DDoS attacks during the fourth quarter holiday season as attackers like to cause the most chaos and make the largest possible financial impact. For many businesses, a significant percentage of yearly revenues are made in the fourth quarter and a serious DDoS attack can be financially devastating.

To raise awareness of the increased potential for attack, Prolexic has launched a marketing campaign that suggests retailers put DDoS protection in place or re-evaluate the protection they already have, as it may not be sufficient to stop increasingly large and complex attacks.

"Many e-Commerce firms obtain DDoS protection from their ISP, hosting provider or content delivery network," said Michael E. Donner, Senior Vice President, Chief Marketing Officer at Prolexic. "What many companies fail to realize is that against the more complex Layer 7 and SSL attacks that target web applications, these mitigation services consistently fail to work. The campaign raises awareness of this little known fact."

The campaign is supported by a number of marketing assets that are available for download. In addition to two new white papers, "*'Tis the Season – for DDoS Attacks*" and "*The Executive's Guide to DDoS*", a case study on SpaFinder.com, a global online resource for spa and wellness services and products, are also available. Despite having DDoS mitigation services in place from its hosting company, the SpaFinder.com site was taken offline by a Layer 7 DDoS attack this summer before Prolexic stepped in to mitigate the attack. Assets can be downloaded from www.prolexic.com/ecommerce

The campaign features print advertisements, banner ads on web pages and in newsletters, as well as email promotions. To reach e-Commerce providers, Prolexic has selected four of the leading e-Commerce print and online publications including *Electronic Retailer, Internet Retailer, RIS News* and *Stores Media*.

Prolexic's fourth quarter campaign is part of a major rebranding effort currently underway that also includes a redesigned corporate web site at www.prolexic.com and a new corporate brochure.

"Prolexic represents the gold standard for DDoS monitoring and mitigation," said Donner. "It's important for businesses to realize that not all providers are the same so we hope to highlight this differentiation through our on-going branding and marketing efforts."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

Contact:
Prolexic Media Relations
media@prolexic.com
+1 (954) 620 6017

Prolexic Quickly Mitigates Series of Randomized DDoS Attacks Against Spafinder.com

HOLLYWOOD, FL — (September 22, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that it recently mitigated a series of randomized combination Layer 4 and Layer 7 DDoS attacks against Spafinder.com, a global online resource for spa and wellness services and products.

The attack, which spanned two days in August 2011, made Spafinder.com completely inaccessible to the nearly 30,000 customers who visit the site daily to view wellness articles or find wellness and spa providers where they can redeem gift certificates or points earned. In addition, customer service agents at the company's 24/7 call center were unable to access the site to provide answers and assistance with customer inquiries.

Accessibility to Spafinder.com was restored within minutes of site traffic being routed to Prolexic's globally distributed scrubbing centers.

"We never really expected to be the target of a DDoS attack," said Pete Ellis, chairman and chief executive officer, Spafinder. "However, we had a DDoS mitigation solution in place from a hosting company just in case. Unfortunately, that solution couldn't stop the attack. I was referred to Prolexic and they had our site back up that evening and fully operational by early the next morning."

Prolexic's technicians used the company's proprietary DDoS mitigation tools to quickly identify the type of attack and the IP addresses of the top ten sources, which included Kazakhstan, Belarus, Peru, and the United Arab Emirates. Security Operations Center staff monitored attack signatures and other characteristics in real time and developed countermeasures to block moves by the attackers.

"As we deployed our mitigation tools and real-time monitoring, the attack would trickle down to being almost non-existent, and then another wave of attacks with a different type of signature would start," said Neal Quinn, vice president of operations at Prolexic. "The attack actually spanned over two days after we began mitigation because the attackers changed the signature every time they realized we were successfully blocking the attack. Finally, they gave up after they realized that Prolexic could identify and block whatever they tried."

Spafinder.com has not experienced another DDoS attack since Prolexic has begun providing mitigation services, which is a common after attackers see that a web site is protected by Prolexic.

"With fourth quarter holiday sales season approaching, Spafinder is gearing up for heavy site traffic that will generate a large percentage of our yearly revenues," Ellis said. "A DDoS attack would be devastating during that time, but we are well protected against all threats with Prolexic. With the proliferation of DDoS attacks on all types of companies becoming more serious, I would recommend the Prolexic mitigation solution to any company that has any type of e-Commerce platform."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Five of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Prolexic Media Relations
media@prolexic.com
+1 (954) 620 6017

Prolexic Predicts Rise in Cyber Attacks as a Result of Latest Global Social Unrest

HOLLYWOOD, FL — (August 24, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced that it expects cyber attacks against companies and governments to increase in the near-term as a result of recent global social unrest.

According to Prolexic's Chief Executive Officer Scott Hammack, hacktivism – using computers and computer networks as a means of protest to promote political ends – is likely to increase in both the short and long-term. "Countries like Greece, Spain, Portugal, Israel and most recently the U.K. have all experienced demonstrations or social unrest and we expect this activism will soon spill over into the digital realm," said Hammack. "The same mentality and discontent that motivates someone to take to the streets is easily transferred to cyber attacks against governments and major corporations."

For the last eight years, Prolexic has monitored Internet attack traffic from its Security Operations Center on behalf of its clients. Prolexic has tracked a rise in attack traffic over the last few weeks, and as a result, the Company has increased its own internal threat barometer from "elevated" to "high".

Hammack believes it is only a matter of time before the number of DDoS attacks against leading businesses and government agencies increases. "Our intelligence indicates that hacktivist tools are evolving rapidly. As a result, we expect the frequency of attacks will increase and they will be more successful unless organizations upgrade their defenses."

In a report issued on August 10 entitled, "*Hype Cycle for Infrastructure Protection, 2011,"* industry analyst firm Gartner predicts that DDoS defense will achieve mainstream adoption in less than two years and lists it as "highly beneficial" on its Priority Matrix.

"Gartner client calls on DDoS have increased and DDoS services are nearing 'must-have' status," said John Pescatore, vice president and research fellow at Gartner in the Hype Cycle report. "Any Internet-enabled application that requires guaranteed levels of availability should employ DDoS protection to meet those requirements."

Since 2003, Prolexic has been protecting Internet facing infrastructures against all known types of DDoS attacks at the network, transport and application layers with a distributed global network of scrubbing centers. By dedicating more bandwidth to attack traffic than any other provider – supplemented by proprietary tools, techniques, and experienced security experts – Prolexic has been able to handle the largest and most sophisticated DDoS attacks ever launched.

"It's interesting to note that more and more threats received from hacktivists are not financially motivated. It is a power play, plain and simple," said Hammack. "We often see extortion as motivation for a DDoS attack where the objective is to extract money from a company in return for not taking down its web site. In the near future, we are more likely to see hacktivists using the threat of DDoS attacks to control a company's actions."

Hammack believes hacktivism is entering a new era defined by increasing activity. "We know that the tools used by hacktivists and cyber attackers are becoming much more effective and the list of targets is increasing," said Hammack. "Hacktivism is not something that will quietly fade away. It's here to stay and that's why organizations who are victimized by these large and increasingly sophisticated DDoS attacks need a company like Prolexic so they can continue conducting business as usual."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Five of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Prolexic Media Relations
media@prolexic.com
+1 (954) 620 6017

Leading Industry Analyst Firm Cites Prolexic in Recent Hype Cycle Report

Firm believes DDoS services are nearing "must-have" status

HOLLYWOOD, FL — (August 24, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced that it has been mentioned as a sample vendor in a report entitled, "*Hype Cycle for Infrastructure Protection, 2011"* by respected industry analyst firm Gartner.

In the August 10 report, Gartner predicts DDoS defense will achieve mainstream adoption in less than two years and lists it as "highly beneficial" on its Priority Matrix.

A DDoS attack is an attempt to make a computer resource (i.e. web site, e-mail, voice, or a whole network) unavailable to its intended users. By overwhelming a web site and/or server with data and/or requests, the target system either responds so slowly as to be unusable or crashes completely. The data volumes required to do this are typically achieved by a network of remotely controlled Zombie or botnet [robot network] computers.

According to Gartner Vice President and Research Fellow, John Pescatore, Gartner client calls on DDoS have increased and DDoS services are nearing "must-have" status. In the report, he states, "DDoS mitigation services should be a standard part of business continuity/disaster recovery planning and be included in all Internet service procurements when the business depends on the availability of Internet connectivity. Any Internet-enabled application that requires guaranteed levels of availability should employ DDoS protection to meet those requirements." The report also lists 10 sample DDoS mitigation providers, including Prolexic.

"Because DDoS is all we do, we have more expertise, more experience and more network resources dedicated to fighting these attacks than any other provider," said Scott Hammack, chief executive officer at Prolexic. "That's why large, complex attacks that can overwhelm other providers always end at Prolexic."

Since 2003, Prolexic has been protecting Internet facing infrastructures against all known types of DDoS attacks at the network, transport and application layers with a distributed global network of scrubbing centers. By dedicating more bandwidth to attack traffic than any other provider – supplemented by proprietary tools, techniques, and experienced security experts – Prolexic has been able to handle the largest and most sophisticated DDoS attacks ever launched.

Prolexic's singular focus on DDoS mitigation also avoids potential conflicts of interest between business groups for companies that offer multiple service lines. This can occur when a DNS provider also offers "add on" DDoS mitigation services, for example. If the same infrastructure that supports DNS services is overwhelmed by a DDoS attack, it is possible that DDoS customers will be sacrificed to protect DNS customers and the company's core business. Pure play DDoS mitigation providers like Prolexic do not have this concern.

"Five of the ten largest global banks, e-Commerce providers, payment processors and others with mission critical Internet-facing infrastructures trust Prolexic to protect them from DDoS attacks and restore availability in minutes," said Hammack. "That's why Prolexic is the gold standard for DDoS monitoring and mitigation."

About the Hype Cycle

The Hype Cycle is copyrighted 2011by Gartner, Inc. and/its affiliates and is reused with permission. Hype Cycles are graphical representations of the relative maturity of technologies, IT methodologies and management disciplines. They are intended solely as a research tool, and not as a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Five of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Prolexic Media Relations
media@prolexic.com
+1 (954) 620 6017

Prolexic Becomes First DDoS Mitigation Provider to Gain PCI DSS Certification

Speeds service provisioning to mitigate encrypted Layer 7 attacks

HOLLYWOOD, FL — (August 11, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced that it is the first DDoS mitigation provider to secure PCI DSS (Payment Card Industry Data Security Standard) level 1 certification.

PCI DSS is a worldwide program designed to help protect consumers from fraud by regulating payment card data security. The PCI DSS standard is the result of a collaborative effort by the major credit card brands (Visa, MasterCard, American Express, Discover and JCB) to build a set of requirements designed to ensure that all merchants that process, store or transmit credit card information maintain a secure online environment.

In the last few years, Prolexic has observed an increase in the number of encrypted attacks against web properties. Typically, these attacks use Secure Socket Layer (SSL) to start an application layer (Layer 7) attack. To monitor and mitigate these encrypted attacks effectively, Prolexic requires that a customer provide their data decrypting private keys.

"Achieving PCI DSS compliance makes it much easier for customers to deploy with us and leverage our unique capabilities to overcome encrypted attacks," said Paul Sop, chief technology officer at Prolexic. *"With this certification, customers know instantly that our key management and security procedures are in compliance with their PCI DSS policy without the time and expense of auditing Prolexic."*

While PCI DSS certification is not required because Prolexic does not store or process any credit card data, certification makes it much easier for a compliant organization to onboard with Prolexic. Critically, certification speeds deployment of remediation for compliant organizations during encrypted Layer 7 DDoS attacks.

Brightline, www.brightline.com, an external auditing company specializing in assurance and compliance services, found that Prolexic has taken sound measures to establish a solid set of security controls and procedures.

"Achieving compliance with this globally recognized data security standard is a significant milestone for Prolexic," added Sop. *"With more and more payment processing and e-Commerce companies coming under DDoS attack, this certification will further differentiate our capabilities and make Prolexic the logical choice for these types of organizations."*

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Five of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

###

Contact:
Prolexic Media Relations
media@prolexic.com
+1 (954) 620 6002

Prolexic Successfully Combats the Largest Packet-Per-Second DDoS Attack Ever Documented in Asia

Company believes attack indicates escalating magnitude of attacks in next 6-8 months

HOLLYWOOD, FL — (July 27, 2011) — Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) mitigation services, today announced it successfully mitigated another major DDoS attack of unprecedented size in terms of packet-per-second volume. Prolexic cautions that global organizations should consider the attack an early warning of the escalating magnitude of similar DDoS threats that are likely to become more prevalent in the next 6 to 8 months.

The attack was directed against an Asian company in a high-risk e-commerce industry. It generated larger than usual TCP SYN Floods and ICMP Floods, both of which are common DDoS attack methods. There was nothing common, however, about the magnitude of the attack.

According to Paul Sop, chief technology officer at Prolexic, the volume reached levels of approximately 25 million packets per second, a rate that can overwhelm the routers and DDoS mitigation appliances of an ISP or major carrier. In contrast, most high-end border routers can forward 70,000 packets per second in typical deployments. In addition, Prolexic's security experts found 176,000 remotely controlled PCs, or bots, in the attacker's botnet (robot network). This represents a significant threat as typically only 5,000-10,000 bots have been employed in the five previous attacks mitigated by Prolexic.

"The customer attempted to mitigate these repeated DDoS attacks for many months with solutions from its ISP and its carrier before approaching Prolexic," said Sop. "Defeating this attack is a testament to our unrivaled capacity and our unique position as the only global DDoS mitigation provider with the experience and bandwidth to successfully fight these gigantic attacks."

To mitigate this high-magnitude attack without putting the burden on a single carrier, Prolexic distributed traffic among several of its global Tier 1 carrier partners and scrubbing network centers. Prolexic was able to help the client maintain service availability throughout the duration of the attack. While Prolexic was fighting this particular threat, it simultaneously helped another client who was experiencing a 7 Gbps DDoS attack.

An "early warning" of escalating threats

"Prolexic sees this massive attack in Asia with millions of packets per second as an early warning beacon of the increasing magnitude of DDoS attacks that may be on the horizon for Europe and North America in the next 6 to 8 months," Sop said. "High risk clients, such as those extremely large companies in the gaming and gambling industries in Asia, are usually the first targets of these huge botnets just to see how successful they can be."

Prolexic cautions that the next quantum leap in DDoS attacks will not necessarily center on bandwidth, but rather on increasing the volume of packets per second to such a high level that carriers cannot handle the overload. According to Sop, these extremely high packet-per-second DDoS attacks are especially insidious because they can cause collateral damage to carriers long before the "bad traffic" ever reaches its intended target.

Overwhelmed by the deluge of Internet traffic, carriers try to cope by passing around the excessive traffic like a "hot potato" from one to another. Ultimately, the carriers must "black hole" the IP address of the attack target and in doing so they unwittingly help the hacker to achieve the goal of creating a "zero route" which crashes the victim's site. In addition, the continuous shifting of traffic from carrier to carrier can seriously affect the performance of multiple web sites, not just the intended target.

"Prolexic has invested millions to be ready for this type of DDoS attack and while we have only seen this botnet once in the Western Hemisphere to date, it is likely to follow a common pattern and become much more prevalent," Sop said. "The good news is that Prolexic is already well ahead of the game and has proven that we can stop attacks of this magnitude."

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Five of the world's ten largest banks and the leading companies in e-commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit www.prolexic.com.

Contact:

Prolexic Media Relations

media@prolexic.com

+1 (954) 620 6017