oncourse
systems for education

Prolexic Passes OnCourse DDoS Mitigation Test

OnCourse Systems for Education is a full-service provider of web-based tools that automate and streamline educational processes for public and private schools. OnCourse's products for lesson planning, attendance tracking, student information and more are delivered through a software-as-a-service (SaaS) platform, so it is critical that they can be accessed online by users 24/7. The company serves K-12 school districts across 40 U.S. states and has tens of thousands of daily users on its website (https://oncoursesystems.com).

Accessibility is especially important at the start of the day for school districts using the OnCourse attendance tracking tool. Recently, however, the digital roll call was disrupted at 8 a.m. on a Thursday by a distributed denial of service (DDoS) attack directed at the primary firewall of OnCourse's outsourced data center. After approximately an hour, the OnCourse CTO and the data center's IT staff determined that it was a UDP flood with malicious traffic coming primarily from Germany and the Netherlands. The OnCourse website and its SaaS products were taken offline for approximately four hours before the data center mitigated the attack by denying overseas sources of UDP traffic. In the meantime, the OnCourse customer support lines were overwhelmed with calls to complain about the outage.

> Company under a DDoS attack

OnCourse Systems for Education, a leading provider of web-based K-12 applications for school districts

> Type of DDoS attack

UDP floods

> Prolexic attack mitigation strategy

PLXproxy

> Time to DDoS mitigation

Cyber-attacks ceased after attackers detected Prolexic protection

"This was the first DDoS attack at OnCourse and we never thought that we would be a target," says Mark Yelcick, chief technology officer and partner at OnCourse. "There's no money or assets to be gained by attacking an SaaS provider of K-12 educational systems. We felt that the firewall, intrusion protection, and DDoS protection from our data center provider would be enough."

OnCourse began to question that assumption after the OnCourse website was brought down for four hours by another UDP flood denial of service attack the next morning. This time, the DDoS threat was directed at one of OnCourse's dedicated IP addresses rather than the data center's firewall. This attack was more difficult to mitigate because the malicious traffic source came from North America where most of the company's clients reside, so blocking traffic based on origin was not a viable option. After the DDoS attack subsided, Yelcick began looking for a DDoS mitigation provider. OnCourse chose a hosting company that offered DDoS mitigation services.

As OnCourse was implementing and testing the new mitigation service on the following Thursday, the company's site was attacked again at 8 a.m. with another UDP flood. Despite repeated attempts to activate the mitigation service, the vendor had issues with passing traffic on to OnCourse's web server farms and could not mitigate the DDoS attack. At that point, OnCourse switched its traffic over to a secondary data center with 10 Gbps inbound pipe capacity. However, within two hours the cyber attackers found and targeted two of OnCourse's IP addresses and once again brought them down.

PROLEXIC
DDoS Attacks End Here.

"That was the proof that OnCourse really was the target of these DDoS attacks," Yelcick says. "At that point we tried a second mitigation provider, but we had technical issues with their service, too. They partially mitigated the attack, but they could not handle our sophisticated way of caching. As a result, our data center footprint quadrupled and our bandwidth spiked."

Yelcick also notes that this mitigation provider's solution triggered a lot of false positives by tagging traffic from concentrated IP addresses that were actually legitimate customers. "They had difficulty adjusting the rule sets to allow our customers in while blocking the DDoS attack," he says. "Also, they couldn't tell us the size of the attack or where it was coming from, since they were trying to drop the traffic at the perimeter of their network. So next we called Prolexic."

Prolexic's DDoS mitigation strategy

OnCourse requested emergency provisioning of Prolexic's PLXproxy service to completely mitigate the denial of service attack. The cyber attackers ceased and disappeared as soon as they saw OnCourse's traffic flowing through Prolexic's globally distributed scrubbing centers – and OnCourse has not come under DDoS attack since.

"We were told that we may not see another DDoS attack once the attackers realized that we have Prolexic protection, and that has been true for us," Yelcick says. "We consider Prolexic to be the 'Cadillac provider' of DDoS mitigation services."

According to Yelcick, Prolexic provides all of the high-value capabilities that the other vendors could not. "Prolexic is the only one who could properly handle our caching and compression during a seamless implementation," he says. "Also, our bandwidth utilization went back to what we consider a normal state, and we no longer had any issues with communicating with our web farms through the data center's firewall. False positive alarms have been eliminated too, because Prolexic recognizes the concentrated IP addresses of our customers as legitimate traffic."

Prolexic also gives Yelcick and his IT team at OnCourse the visibility they need into network activity and attack forensics through a single dashboard in the Portal, a secure online resource only for Prolexic customers.

Staying protected with Prolexic

OnCourse continues to stay protected with Prolexic as a PLXproxy customer. Yelcick and his IT team chose Prolexic because of the massive amount of bandwidth that Prolexic brings to the table and the fact that Prolexic is a dedicated DDoS mitigation service provider. OnCourse has even recommended Prolexic to its data center hosting provider, which recently became a Prolexic customer.

"We have found that many data centers take it upon themselves to do their own DDoS mitigation, which isn't very effective if a UDP flood attack fills up all their pipes," Yelcick says. "Their answer is, 'We'll deal with it upstream,' but that's too slow contacting upstream providers. We also can't afford to be black holed for a long period of time. It's like kicking us to the digital curbside when an ISP says, 'We can't deal with the DDoS attack so we're shutting you down.' That's why we strongly recommended Prolexic to our hosting provider.

Knowing that our site is protected by Prolexic lets us ensure a good customer experience," Yelcick concludes. "It is very important that our site is responsive with no noticeable latency, especially in cases when our products, such as the student information system, need to be accessed quickly in case of an emergency. We simply cannot afford downtime brought about by a DDoS attack."

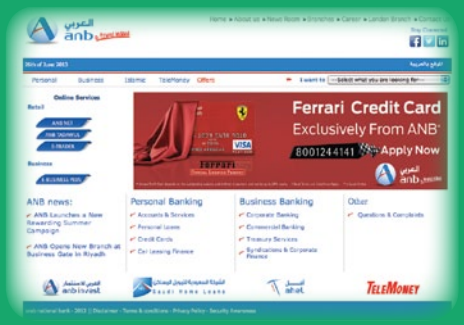
About Prolexic: Prolexic Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, 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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.100513

Arab National Bank Builds a Strong Defense Against DDoS Attacks with Prolexic

Arab National Bank (ANB) is a worldwide commercial bank serving more than 2 million corporate and retail customers. In addition to its 278 locations, 980 ATMs, and 10,000 point-of-sale terminals across Saudi Arabia, ANB also boasts a technologically advanced IT platform for supporting customer-friendly online banking services, including an e-trader stock trading site.

Financial services firms around the globe have become prime targets for distributed denial of service (DDoS) attacks over the past year in particular, so ANB took protective action. If its sites came under a DoS or DDoS attack, the impact would be severe. ANB's online banking customers would not be able to transfer money between accounts, check balances, or pay bills. Customers of ANB's e-trader site would not be able to buy or sell stock shares, resulting in potentially serious financial losses, not to mention damage to ANB's reputation as a safe, reliable financial services firm.



> Company under a DDoS attack

Arab National Bank, a commercial bank in Saudi Arabia

> Type of DDoS attack

Protection against all types and sizes of DDoS attacks

> Prolexic attack mitigation strategy

PLXrouted DDoS mitigation service and 24/7 monitoring

> Time to DDoS mitigation

Guaranteed mitigation within minutes under Prolexic's industry-leading service level agreement

"We were aware of the spike in DDoS attacks on financial services companies in our region, as well as internationally," says Jamil M. Barakat, ITG-Head of Telecoms at Arab National Bank. "We knew it was to our advantage to have a DDoS mitigation service provider to work with our IT team to minimize the risk and impact of DDoS attacks."

Prolexic's DDoS mitigation strategy

Barakat and the management team at ANB conducted an internal evaluation of both local and international DDoS mitigation service providers. They narrowed the selection to a short list, which included Prolexic. Each company had to meet the bank's stringent scoring criteria for technical expertise, support, reporting, monitoring, implementation, security, and cost. Prolexic scored the highest by exceeding all requirements for:

- 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
- DDoS protection/detection bandwidth scalability

PROLEXIC
DDoS Attacks End Here.

- Managed services terms for bandwidth scale and number of covered attacks
- Multiple international scrubbing sites
- Assurance of confidentiality when handling unencrypted traffic
- Maintaining a dual ISP/DSP redundancy setup
- Strong alerting capabilities
- Flexibility to adjust DDoS setting parameters per ANB's requirements
- Detailed reporting and traffic analysis
- Ability to capture the headers of packets being dropped

"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," says Alrebdi Al Rebdi, Head of Information Security at ANB. "That, plus a time-to-mitigate SLA, gave us the confidence that Prolexic could protect ANB against DDoS."

Barakat adds that out of the shortlisted companies, Prolexic offered the best proposal for pricing – a flat fee regardless of the number of attacks and bandwidth consumed. "Prolexic had the best combination of technical capabilities and price," Barakat says.

"Also, Prolexic's implementation was very smooth and we've had no issues with latency."

ANB is using PLXrouted, Prolexic's routed DDoS mitigation solution, and 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 deal with any local support and connectivity issues.

ANB chose PLXrouted because it meets the bank's criteria for providing maximum protection against the broadest range of DDoS attack types and defends against 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.

Staying protected with Prolexic

ANB has not come under a denial of service attack since engaging Prolexic's DDoS mitigation services. However, Barakat is confident that Prolexic will respond with a strong and successful defense if an attack occurs.

"Prolexic's support team has been excellent, including the local team at Cyberia," Barakat says. "They have been very responsive to all of our requirements and they're always on top of things in terms of alerting and communicating with us. Overall, the Prolexic team's response has been very good and reliable."

Now that ANB has Prolexic's DDoS mitigation service in place, Barakat encourages other financial services firms in the region, as well as globally, to be aware of escalating DDoS threats and implement protection against denial of service attacks.

"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," Barakat says. "As we have learned at ANB, it is critically important to have a good and reliable DDoS mitigation solution in place."

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, energy, 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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.080513

CLICK POINT! MEDIA
DIGITAL MARKETING

Prolexic Gets Clickpoint! Media Back Online After Layer 4 SYN Flood

Clickpoint! Media is a European network of web portals, e-mail marketing companies, search engine optimization (SEO) agencies, advertising networks, and media brokers. All of the company's network services are designed to help marketing and advertising organizations optimize their campaigns for greater return on investment, increased web traffic, and heightened brand awareness. Clickpoint! has offices in Italy, the U.K. and Spain.

Clickpoint! had never experienced a distributed denial of service (DDoS) attack before, nor did it have dedicated DDoS protection in place. Recently, IT staff began to notice a progressive increase in traffic to the company's websites over several days. The traffic appeared to be legitimate and traffic patterns did not change significantly, so the Clickpoint! engineers did not suspect a DDoS attack. However, a few days later, 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 progressed to 800 Mbps.

> Company under a DDoS attack

Clickpoint! Media, a European network of online media services for marketing and advertising companies

> Type of DDoS attack

Layer 4 SYN flood

> Prolexic attack mitigation strategy

Prolexic's PLXproxy mitigation service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

"The first attack brought our sites down for about four hours, and the same pattern repeated twice a day over the following days," says Roberto Siano, CEO and founder of Clickpoint! Media. "Our hosting partner initially null routed or 'blackholed' the spoofed inbound IPs that carried most of the malicious traffic, but then the attackers would change the source IPs of the attack. We tried to improve our infrastructure by changing our firewall and escalating to a router with a higher bandwidth capacity, but with no result."

During the downtime, Clickpoint! could not provide an important part of its media service and customer account access was limited. A large number of the company's back-end servers were also crippled. After trying to fight the series of DDoS attacks internally for almost a week, the company's hosting partner advised Clickpoint! to contact Prolexic.

Prolexic's DDoS mitigation strategy

The DDoS attack on Clickpoint! had already exceeded 800 Mbps when Prolexic's Security Operations Center (SOC) took over mitigation efforts. Prolexic's engineers were able to bring all Clickpoint! sites up within minutes after routing traffic through Prolexic's global scrubbing centers and restore media services to customers.

Using live monitoring best practices, proprietary techniques and equipment, Prolexic's engineers were able to quickly develop and launch countermeasures

PROLEXIC
DDoS Attacks End Here.

PROLEXIC
DDoS Attacks End Here.

to the changing attack vectors. With the DDoS attack blocked, the attackers soon gave up and moved on to other easier targets. Prolexic also provided real-time attack metrics on attack origins – Turkey and Romania – as well as other metrics that Clickpoint! can use to build a stronger DDoS defense with Prolexic as the cornerstone.

"We trusted the recommendation of our hosting partner and we were impressed by how quickly Prolexic answered our contact-form inquiry and solved our problem," Siano says. "Once our traffic began flowing through Prolexic, our sites became immediately accessible with no further downtime."

Staying protected with Prolexic

Clickpoint! changed its IP addresses after moving to Prolexic. Notably, the IP addresses Clickpoint! had been using before adopting Prolexic have been under continuous DDoS attack, even after Clickpoint! stopped using them. The company's hosting partner has had to block the entire subnet in order to avoid further damage and downtime.

Now under Prolexic protection, Clickpoint! no longer risks downtime that would prevent it from delivering mission-critical media services to major marketers and advertisers across Europe. In addition, Clickpoint! no longer has to depend solely on the limited cyber security services of its hosting provider.

"Prolexic's DDoS mitigation services are excellent," Siano says. "We have not suffered any other direct attacks since the Prolexic service was deployed and the Prolexic engineers always reply promptly to any inquiries or concerns we have. With Prolexic in place, our customers have greater confidence that the media services they rely on will always be available."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

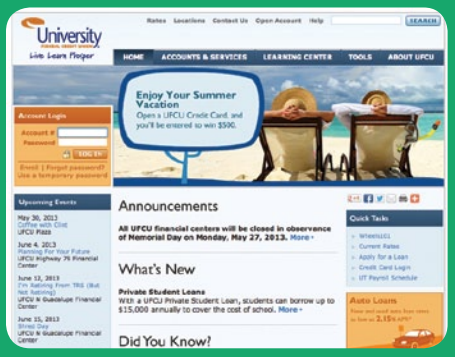
v.061013

University
FEDERAL CREDIT UNION

DDoS Attacks Against University Federal Credit Union (UFCU) End with Prolexic

University Federal Credit Union (UFCU) is the largest locally-owned financial institution in Austin, Texas with branches serving over 162,000 members throughout the Austin and Galveston areas. Online banking and other financial services are also available at www.ufcu.org. UFCU is one of the nation's larger credit unions with US$1.6 billion in assets. UFCU employs 450 people, including an IT staff of 27 technicians. The IT department hosts www.ufcu.org in-house at the company's own data centers.

Banks and other financial services organizations are often prime targets for Distributed Denial of Service (DDoS) attacks and credit unions are no exception. A February 2013 alert issued by the National Credit Union Administration (NCUA) even warns that DDoS attacks against credit unions are on the rise.[1] UFCU experienced the first of three DDoS attacks on January 24, which brought down UFCU's website for 2 hours and 36 minutes. A UDP flood on Port 53 (DNS) was directed at the credit union's URL and peaked at 5.4 Gbps.



> Company under a DDoS attack

University Federal Credit Union (UFCU)

> Type of DDoS attack

UDP and TCP floods on Port 53

> Prolexic attack mitigation strategy

PLXrouted service deployed to protect against future DDoS attacks

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

At first, the IT team thought the downtime was caused by an Internet Service Provider (ISP) issue, but as more of the network's internal and external monitoring devices began to issue alerts, they became aware of a more serious problem. UFCU's ISP confirmed that UFCU's site was under a DDoS attack.

The malicious traffic was automatically blocked by UFCU's firewall, but that did not prevent the high volume of traffic from completely filling up the pipe between the UFCU network and the ISP. When the distributed denial of service DDoS attack began to impact other ISP customers, the ISP eventually blackholed UFCU's traffic to stop collateral damage.

"This was the first time I've ever led an organization's defense efforts against a DDoS attack," says Glen Roberts, Infrastructure and Security Manager at UFCU. "The attackers definitely went after our domain name and IP address. I compared notes with my counterpart at another credit union that was also attacked and found they saw the same kind of attack signatures. They had tried playing games with the IP addresses and redirecting traffic to different servers, but that was ineffective defensively and the DDoS traffic just followed it. Nothing they tried worked."

During the 2 ½ hours of downtime, UFCU members were unable to access online banking, apply for auto loans, or download documents. The UFCU member service department was deluged with calls from confused members.

PROLEXIC
DDoS Attacks End Here.

Other than a firewall, UFCU had no specific DDoS mitigation plan in place. "From a risk management perspective, like many other credit unions of our size, we had just accepted the fact that if we were subject to a DDoS attack, our website was going to be offline. We didn't see ourselves as being in a position to prevent it," Roberts says. "Staving off a DDoS attack would be a huge challenge for us. Besides, the chances seemed remote that we would ever be targeted. Like many other financial institutions over the past few months, we were wrong."

After the attack was finally mitigated by blocking UDP traffic on Port 53 with the ISP, Roberts investigated the DDoS attack further and determined that there were only 91 computers in the botnet that launched such a massive amount of traffic. The IP addresses were located all over the world and were tied to what Roberts calls "amateurish" websites, some of which were labeled under construction. The attackers never made a ransom demand, nor did they make contact with UFCU in any way.

Roberts continued his research on DDoS and what kind of toolkits might have been used in the attack against UFCU. He came across an article authored by Prolexic. "Later I had spoken with a peer at another organization that had been hit by a DDoS attack," Roberts says. "They said they were thinking about getting DDoS mitigation service from Prolexic. There was that name again and I thought maybe there's something to that."

Roberts factored into the vendor selection process that the other organization had also chosen Prolexic as their first choice. He then formally recommended Prolexic to UFCU as a service that could help reduce the impact of future DDoS attacks. As internal deliberations were underway, UFCU was hit by another denial of service DDoS attack on February 25. UFCU's site was down for 4 hours and 6 minutes.

This time the DDoS attackers raised the stakes with a randomized attack. Traffic peaked at 10.1 Gbps. "This time we knew it was a DDoS attack rather than an ISP issue," Roberts says. "We were as ready as we could be without a DDoS mitigation service in place."

As soon as the DDoS attack started, the IT team notified their ISP and looked at web server logs and the firewall to determine the scope of the attack. They saw that the attackers had launched repeated requests to download a PDF file on the site. When IT changed the name of the PDF file, the attack mode shifted to requesting documents that did not even exist. Then, UFCU technicians captured the IP addresses and blocked them with the firewall. In response, the hackers switched from the PDF download strategy and launched a new attack against UFCU's external DNS over the UDP and TCP 53 ports.

The February 25 attack was finally mitigated with assistance from the ISP. After this second attack, UFCU's management clearly saw the need for a DDoS mitigation service and went with Roberts' recommendation of Prolexic.

Prolexic's DDoS mitigation strategy

UFCU engaged Prolexic for always-on PLXrouted DDoS mitigation service to protect against all sizes and types of DoS and DDoS attacks – and just in time. UFCU's website was attacked again on March 7. But this time the DDoS attack did not cause any downtime.

"The March 7 attack had zero impact on our site thanks to DDoS protection by Prolexic," Roberts says. "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."

Even though the March 7 DDoS attack did not impact UFCU's site, Roberts still investigated the attackers' strategy. He found that the attackers had launched repeated requests for a PDF as they had in the second attack, but had no success. Ironically, the same group of attackers had bragged on their blog site about launching DDoS against UFCU on the two previous attacks, but this time they did not.

"Later that evening, I noticed that the attackers did not include us as one of their DDoS victims in their blog post," Roberts says. "It's interesting that they had nothing to brag about this time since we were able to prevail with Prolexic's mitigation service."

"The Prolexic run book has been a tremendous asset to us and we have been able to build it out for our needs."

PROLEXIC
DDoS Attacks End Here.

Staying protected with Prolexic

"After UFCU's experience with DDoS attacks, I would encourage any credit union with over US$500 million in assets to seriously consider purchasing DDoS mitigation services," Roberts says. "After considering it, they may decide to accept the risk of not doing it, but they should be ready for all steps required to purchase and implement something like PLXproxy in case it is needed during an actual attack."

As the number of DDoS attacks against credit unions continues to rise, the 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. "I really like the idea of the run book that Prolexic gave us," Roberts says. "Each company has its own incident response plan, but I think that every company should also have a DDoS-specific response plan, as well. Everyone needs to know exactly what to do in case of a DDoS attack. The Prolexic run book has been a tremendous asset to us and we have been able to build it out for our needs."

At UFCU, Roberts keeps the run book in a red binder that contains contact information for Prolexic, for the ISP, and for other credit unions that could possibly also be under DDoS attack. It 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. "It's a good idea to have a DDoS run book, because when you are under a DDoS attack, it's not the time to be digging up all of this information," Roberts says.

UFCU continues to be protected by Prolexic's PLXrouted DDoS mitigation service and has not been attacked since March 7.

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

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061713

1ink.com

Prolexic Protects 1ink.com's Network from Business Losses Due to DDoS Attacks

1ink.com is a retailer of replacement inkjet and laser toner cartridges, and the company is committed to high-quality products and excellent customer service. That commitment has made www.1ink.com and its network of e-Commerce domains trusted destinations for printer ink and toner for businesses and consumers. 1ink.com promises its customers a secure shopping environment, but that promise was threatened when a distributed denial of service (DDoS) attack took down one of the company's smaller websites, www.101inks.com, for more than 24 hours.

"We had no indication that we were going to be attacked, or even could be attacked," says Roland Davoudikia, chief executive officer at 1ink.com. "We had been in business for 13 years and had never had any issues with DDoS attacks."

> Company under a DDoS attack

1ink.com, one of the largest online retailers of replacement inkjet cartridges and laser toners

> Type of DDoS attack

SYN flood and DNS flood

> Prolexic attack mitigation strategy

Prolexic PLXproxy to protect against future DDoS attacks

> Time to DDoS mitigation

Under 5 minutes

The IT team at 1ink.com was able to reroute traffic from 101inks.com to the company's other domains, so the business did not suffer significant damage from the attack. However, Davoudikia still needed to bring the 101inks.com site back online. He also realized the potential impact of future DDoS attacks. After leaving voicemail messages with several DDoS mitigation providers, Davoudikia called Prolexic – and a live person answered.

"The last thing you want is to get a voicemail when your website is down because of a DDoS attack," Davoudikia says. "The Prolexic engineer gave me an idea of what was going on, how Prolexic could mitigate it, and how long it would take. Once we signed the contract, Prolexic brought our site back up within 5 minutes, just as they guaranteed."

Prolexic's DDoS mitigation strategy

Davoudikia engaged Prolexic to provide the PLXproxy DDoS mitigation service for protection against future denial of service threats.

"The first attack was not a major incident, but I realized the amount of damage it could have done if it had targeted our network or one of our larger, more heavily-trafficked domains," he says. "I decided to keep working with Prolexic as an insurance policy to protect all of our domains against DDoS attacks. Our business is growing and evolving, so we need DDoS protection in place in case we are attacked again."

Fast-forward 10 months to Dec. 19, Davoudikia was awakened at 3 a.m. by a phone call from Prolexic. This time the main www.1ink.com site – one of the larger domains, which processes thousands of orders daily – was hit with a large SYN flood DDoS attack that peaked at 70 Gbps. Fortunately, Prolexic had reassuring news for Davoudikia, even at that late hour.

"Had we not had Prolexic to mitigate the DDoS attacks, we could have suffered hundreds of thousands of dollars in losses, if not more."

PROLEXIC
DDoS Attacks End Here.

"I asked the Prolexic engineer what I needed to do, and he said, 'Nothing.' He told me that Prolexic was mitigating the DDoS attack and that he was calling me only because I had instructed them to notify me in case of an attack. Best of all, our site did not go down, nor was there any interruption or slowing of the site's performance because we had Prolexic DDoS protection in place."

Five days later, Davoudikia was awakened yet again with another early morning call from Prolexic. The DDoS attackers struck 1ink.com again, this time with a combination SYN flood and DNS flood that peaked at 40 Gbps. Again, Davoudikia did not need to take any action, nor did the 1ink.com site go down. Prolexic was already mitigating the DDoS attack, and there was no damage.

"Luckily, we had Prolexic protection already in place, so the DDoS attacks didn't affect our business," Davoudikia says. "Had we not had Prolexic to mitigate the DDoS attacks, we could have suffered hundreds of thousands of dollars in losses, if not more. Not only would we have lost sales, but we also would have damaged our relationships with our business partners. They don't want to work with a site that is constantly down or has performance issues. If they link to us and our site is not available, it makes us look unreliable and poor to work with."

Staying protected with Prolexic

Since the third DDoS attack, 1ink.com has not been targeted. Davoudikia believes these attacks were unusual, because they may have been a case of mistaken identity. Prolexic and the FBI both believe that 1ink was not the intended DDoS target; rather, they suspect the attackers intended to hit a different site with a similar name.

"We were not the true target, but nevertheless we got attacked," Davoudikia says. "Hopefully, it won't happen again. But in today's online environment, you can't take that chance. I can't imagine running my business without Prolexic's protection from DDoS attacks.

"The fact is that DDoS attacks happen all the time," Davoudikia continues. "You need DDoS protection to safeguard your business. We could lose hundreds of thousands of dollars per day if our site was brought down by DDoS attack – and we can't take that chance."

Even when 1ink.com is not under attack, the IT team relies on Prolexic to advise them on matters of server security. During a recent server relocation at 1ink.com, Prolexic engineers answered questions about both DDoS and non-DDoS related issues.

"Our programmers were very impressed with the level of service they received from Prolexic," Davoudikia says. "The Prolexic team has always been very professional and always gives us whatever information we need. Prolexic's customer support is excellent and we appreciate that."

Davoudikia notes that he has recommended Prolexic to other companies as the best insurance against DDoS attacks. "During a DDoS attack, you're desperate and you need a mitigation provider who can give you peace of mind and say, 'Don't worry, we've dealt with this before and we'll take care of it,'" he says. "That's what I was looking for in a DDoS mitigation provider and I found it in Prolexic."

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, energy, 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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.080713

entropay

Prolexic Protects Leading Provider of Prepaid Virtual Visa Cards Against DDoS Attacks

Ixaris Systems offers businesses and consumers a very flexible and instantaneous way of making and receiving online payments with virtual prepaid cards. The company's consumer web site, www.entropay.com, enables anyone to open and immediately fund an account to obtain a virtual prepaid Visa card. As the first and now most successful virtual prepaid card introduced in Europe, EntroPay provides consumers with another payment option that is safe, convenient and accepted by millions of merchants worldwide.

Like any online business that experiences success and recognition, EntroPay became a target for DDoS attacks. Three years ago, the site had its first DDoS attack. The attackers sent a ransom e-mail demanding US$15,000 per month from Ixaris management as "protection money." Management chose to ignore the ransom demand and forwarded it to the relevant authorities. The DDoS attackers followed through on their threat. Although no user data was compromised, the EntroPay site was brought down by a DDoS attack for a considerable length of time, making it impossible for users to create a new prepaid card account or load additional funds to their existing cards. A DDoS attack on EntroPay impacts other B2B sites since multiple URLs are linked by the same underlying application.

> Company under a DDoS attack

EntroPay.com, a virtual credit card web site owned and operated by Ixaris Systems

> Type of DDoS attack

Layer 4 with variations of SYN Flood, ICMP Flood, UDP Flood

> Prolexic attack mitigation strategy

Prolexic's proprietary mitigation tools and real-time response to changing attack signatures

> Time to DDoS mitigation

Within minutes after routing traffic through Prolexic's cloud-based scrubbing centers

"As a financial services provider, the security of our service is of the utmost importance to us, so any attack is something we take very seriously," says Tim Murfet, chief information officer at Ixaris Systems. "From a commercial standpoint, it is also vital we keep the EntroPay site running 24/7, 365 days a year. When the site is down, we not only miss out on revenue but our brand reputation is affected as well."

Prolexic's DDoS mitigation strategy

After the first attack, Ixaris relied on a hardware appliance from its ISP to protect EntroPay from future DDoS attacks. However, this solution failed when EntroPay was hit with another attack. A consultant recommended Prolexic as a DDoS mitigation provider who could quickly and successfully mitigate high volume attacks.

Once Ixaris IT personnel detected the attack and switched the IP address over to Prolexic's proxy service, EntroPay was back in business in minutes. After seeing the fast time-to-mitigation provided by Prolexic in an emergency situation, Ixaris management decided to expand its DDoS protection with Prolexic's PLXrouted service. With this service, DDoS attacks are detected by monitoring on-premise equipment. The traffic-routing service is activated using Border Gateway Protocol (BGP) to on-ramp network traffic to Prolexic's cloud-based denial of service DDoS mitigation infrastructure.

PROLEXIC
DDoS Attacks End Here.

"We like the way that Prolexic can stop attacks immediately when we route the traffic through their servers."

PROLEXIC
DDoS Attacks End Here.

Most recently, Prolexic has successfully mitigated a number of Layer 4 DDoS attacks against EntroPay, with the largest attack peaking at 700 Mbps. The site has been hit by a wide range of attack types – SYN Flood, ICMP Flood, UDP Flood – of various durations. 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 attackers in just minutes using more than 20 commercial and proprietary mitigation tools and technologies and real-time monitoring of changing attack signatures. Post-attack forensic information also helped Ixaris identify where the attacks originated.

"We like the way that Prolexic can stop attacks immediately when we route the traffic through their servers" says Denise Vella, information security officer at Ixaris. "Also, we're impressed with Prolexic's vast experience in DDoS mitigation. They have the industry reputation to prove it."

Staying protected with Prolexic

DDoS attacks on financial industry web sites by sophisticated hacktivist groups have increased dramatically in the early months of 2012, but EntroPay now has the same robust DDoS mitigation defense as 10 of the world's largest banks – Prolexic. Today, if EntroPay experiences a DDoS attack, the company's on-call IT personnel are informed immediately and are required to re-route all traffic to Prolexic for mitigation. IT also has access to Prolexic's 24/7 customer service if any questions or unusual issues arise.

"Prolexic's customer service is very efficient," Vella says. "They're there 24/7 and can address our issues within 5 to 10 minutes in emergency cases. Overall, Prolexic offers excellent service and once our traffic is routed through their network, we're immediately back in business."

Murfet compares DDoS protection from Prolexic to a disaster recovery plan that should be regularly tested to ensure that everyone in IT knows how to respond during an attack. "I recommend having good communication with your DDoS mitigation provider even in non-attack situations and testing the service regularly so you'll know it will work when you need it," Murfet says.

"Don't think that DDoS won't happen to you, because it will," Vella says. "If you don't have the tools in-house, it makes sense to have a DDoS protection service. For a company that requires 100 percent uptime like ours, I would recommend putting a highly experienced DDoS mitigation service like Prolexic in place."

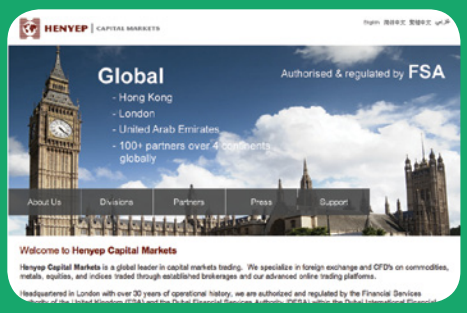
About Prolexic: Prolexic Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing 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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.060713

HENYEP

Prolexic Protects Henyep Online Trading Sites Against DDoS Attacks

Based in London, Henyep Capital Markets is a leading international online trading and financial services company with multiple secure websites serving clients in 150 countries globally in Europe, Asia and the Middle East. To ensure uptime and accessibility, Henyep has implemented a robust, redundant infrastructure across its globally dispersed data centers. However, even though the firm was prepared to deal with any network or connectivity issues, the severity and scale of a DDoS attack caused management to seek out specialized support for mitigation. The perpetrators demanded ransom in exchange for stopping the attack, but Henyep management stuck to its policy of not negotiating with cyber criminals.



> Company under a DDoS attack

Henyep, a leading international online trading and financial services company

> Type of DDoS attack

SYN Flood, GET Flood, ICMP Flood

> Prolexic attack mitigation strategy

Emergency mitigation provided by PLXproxy with ongoing DDoS protection under the PLXrouted mitigation service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

Although clients could still trade via other Henyep sites and trading desks, the distributed denial of service attack caused service disruption and made it difficult for customers to access information in real time on the crippled website. "We pride ourselves on uptime and this was the first time that our clients ever experienced downtime on a Henyep site," says the director of business development and operations at Henyep. "We wanted to quickly put a DDoS mitigation solution in place that would ensure that our sites would never again be held hostage to cyber attacks of any size or type."

The director and other senior executives at Henyep held an emergency meeting to seek out a DDoS mitigation provider. After contacting four vendors, Prolexic stood out as the obvious choice. "Prolexic came highly recommended by our colleagues at other financial services companies," the director says. "Most of all, Prolexic responded the fastest and in the most professional manner to our request for emergency DDoS mitigation. A Prolexic representative in Australia contacted a very knowledgeable engineer in the U.S. who immediately figured out what was going on with our website – all before we got any kind of response back from the other vendors."

Prolexic's DDoS mitigation strategy

Prolexic provided Henyep emergency mitigation through its PLXproxy service. After Henyep pointed its domains to Prolexic, all site traffic was routed through Prolexic's global scrubbing centers where any malicious DDoS traffic was removed. Customer accessibility to real-time financial trading data and services on the affected site was restored in just minutes.

Prolexic DDoS mitigation engineers in the U.S. quickly identified the attack as a SYN flood followed by multiple GET floods. Over two days, the series of attacks peaked at 35.30 Mbps (bits per second), 8.10 Kpps (packets per second),

and 122.00 Kconn (connections per second). All the while, Prolexic mitigation engineers were monitoring the attacks and counteracting the perpetrators' changing attack vectors. As a result, the attackers were unable to take down the Henyep sites again, nor disrupt services despite the length of the attack.

Throughout 2012, Henyep, like many other financial services companies, has continued to be the target of DDoS attackers, but those distributed denial of service attacks have gradually declined as the perpetrators have realized that the company has Prolexic DDoS mitigation services in place.

"What's great about Prolexic is that they offer different service options that you can tailor to the nature of your business," the director says.

Staying protected with Prolexic

Since the initial distributed denial of service attack on Henyep's trading site, other DDoS attackers have tried – and failed – to breach Prolexic's protection. GET floods and SYN floods have been launched against Henyep, but again, were intercepted by Prolexic 's PLXrouted service that Henyep had provisioned after the initial attacks.

More recently, DDoS attackers tried to take down Henyep's trading operations with a 30 Mbps ICMP and GET floods without success due to Prolexic protection.

Regardless of the number or bandwidth of the DDoS attacks, Henyep's sites always stay up and accessible to its international trading customers. "Our sites have not been down since we have been under the protection of Prolexic, even though attackers keep trying. It is important that our clients know that we only choose best-in-class service providers to complement our state-of-the-art trading platforms" says the director. "Internally, we call Prolexic the 'bomb shelter' and we think it's a first-rate service. Also, we're very happy with the way that Prolexic's DDoS mitigation engineers work with our internal IT team."

Henyep's director of business development and operations advises other financial services companies with an online presence and mission-critical e-Commerce to seriously consider DoS and DDoS protection as an insurance policy against all types of cyber attacks and ransom-demanding attackers.

"Typically, DDoS attacks come in droves and once these cyber criminals find you they will not leave you alone," the director says. "Having a strong DDoS mitigation service like Prolexic in place is the only way to stop them from taking down your mission-critical services on the Web.

"The fact that Prolexic protects some of the biggest banks in the world gave us confidence in their DDoS mitigation expertise," the director adds. "We pride ourselves on having great service providers come into our data centers and protect our client's trading activities, as we only want the best. We know that Prolexic's people will act professionally and will keep our sites up because they take a lot of pride in what they do. That's why we stay with Prolexic."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

seek

Australia's Leading Employment Website Ensures Uptime with DDoS Protection from Prolexic

Seek.com.au is Australia's number one online employment marketplace with 120,000 jobs posted online that receive over 21 million visits each month across multiple platforms. Over 6.2 million Australians have a relationship with SEEK; SEEK has unique insights into local labor markets and regularly conducts research into employment trends and job seeker sentiment including the SEEK Employment Index (SEI) and SEEK Job Market Update.

Not long ago, distributed denial of service (DDoS) attackers launched a Layer 7 attack at a specific application that SEEK had developed in-house for its job searching services. The GET flood was small, peaking at 30 Mbps, but it still consumed all of the resources of multiple servers. As a result, the Seek.com.au search function and other services were completely inaccessible to users. The site's hosting provider tried to help, but did not have the resources to identify and respond to an application layer attack.

> Company under a DDoS attack

Seek.com.au, an Australian owned and operated job search site

> Type of DDoS attack

Layer 7 GET flood

> Prolexic attack mitigation strategy

PLXrouted deployed to protect against future DDoS attacks

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

Although the site outage only lasted 10 minutes and the attackers quickly moved on to other targets, it was long enough for SEEK management to ramp up their search for a distributed denial of service DDoS mitigation provider. Management considered an Internet Service Provider (ISP), but felt that there could be a conflict – would the ISP protect SEEK during a DDoS attack if other customers were at risk, or would the ISP blackhole their site?

"There aren't many pure Web-based businesses like ours in Australia that rely on site uptime in order to make money," says Andre Bertrand, security services manager at SEEK. "Therefore, the experience of DDoS mitigation providers in the country is limited. After becoming aware of Prolexic in the U.S., we moved quickly to engage them as our DDoS mitigation provider."

Prolexic's DDoS mitigation strategy

Seek.com.au was not under distributed denial of service attack when the Prolexic DDoS mitigation solution was deployed. Instead, company management engaged Prolexic as an insurance policy against future DDoS attacks of all types and sizes. Most importantly, SEEK management is confident that Prolexic can keep seek.com.au online and accessible to its millions of users if cyber attackers were to strike again.

"We have more substantial job data than anyone else in the Australian and New Zealand market, and it hurts our business when the site is down and people cannot access this data," Bertrand says. "The threat of a DDoS attack causing extended downtime motivated us to get DDoS protection from Prolexic."

PROLEXIC
DDoS Attacks End Here.

SEEK has not needed to use Prolexic's DDoS mitigation service yet, but 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 says. "Also, Prolexic has helped us test our DDoS mitigation strategy and develop a playbook so we can minimize downtime by quickly and confidently responding to a DDoS attack. Of course, Prolexic is our first line of defense in this strategy."

Staying protected with Prolexic

"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," Bertrand says. "We have always felt comfortable with Prolexic's notifications and provisioning of services. Also, they are always professional and give us great service even though we are a small customer."

Bertrand also notes that there was not enough information to identify the source of the DDoS attackers at the time of the Layer 7 attack, but now no one at SEEK has to worry about that in the future. "Now we are happy to have Prolexic as a specialist in that area," he says. "The next time a DDoS attack happens, we can turn over those matters to Prolexic and draw upon their expertise in attack forensics."

When anyone asks Bertrand why SEEK stays with Prolexic, he says it all comes down to experience. "Prolexic is a specialist in DDoS mitigation and that's all they do," Bertrand says. "DDoS mitigation is only an add-on service with ISPs and other providers. Even DDoS protection device vendors only provide hardware. It all comes down to how much experience the provider has in DDoS, which is a very specialized business. Most of all, DDoS is a top threat for us, so we wanted only the best protection, and we feel that Prolexic is clearly the best DDoS mitigation provider in the industry."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Prolexic Mitigates DDoS Denial of Service Attacks Against Auction Site

BidCactus.com is a popular online auction site where savvy bidders can walk away with name brand new merchandise such as electronics, fashions, gift cards, and more for up to 90 percent off retail price. Unfortunately, the site became a target for DDoS denial of service attackers. Earlier this year, a denial of service DDoS attack overwhelmed the site's firewall capabilities and requests were no longer being delivered to the load balancer.

The DDoS attackers sent a ransom demand for several thousand Euros in exchange for stopping the denial of service attack. Management at BidCactus refused to pay. While BidCactus.com had DDoS mitigation services from its hosting provider, a second attack overwhelmed its resources. The hosting provider nullrouted or "black holed" BidCactus.com in order to avoid collateral damage to its other hosted sites.

> Company under a DDoS attack
BidCactus.com, a popular online auction site

> Type of DDoS attack
Layer 3 denial of service attacks

> Prolexic attack mitigation strategy
PLXproxy

> Time to DDoS mitigation
Within minutes under Prolexic's industry leading service level agreement

"Our site went completely dark," says Jeffrey Dvornek, director of technology at BidCactus.com. "We had been attacked sporadically before, but those were generally smaller DDoS attacks that we could fight off with firewall rules. This time we were down for a total of six hours and we completely lost the opportunity to do business during the attack."

The site's customers flooded the company's customer service lines with calls and e-mails to complain about the outage. "It's difficult to put a dollar value on an outage, but it was definitely significant in terms of our reputation," Dvornek says.

BidCactus's hosting provider recommended Prolexic for DDoS mitigation, among a few others, and after evaluating the levels of protection, BidCactus selected Prolexic. "Prolexic responded to our initial request for help with great speed and our site was back online almost immediately," Dvornek says. "After Prolexic took over, the DDoS attackers never returned."

Prolexic's DDoS mitigation strategy

Prolexic provided emergency denial of service mitigation service to BidCactus.com through its PLXproxy service. As soon as BidCactus.com switched its domains over to the Prolexic PLXproxy service the site was back online and ready to accept bids. All traffic to the site was routed through Prolexic's cloud-based global scrubbing centers where Prolexic mitigation experts identified, analyzed and removed the malicious traffic.

Prolexic DDoS mitigation experts quickly identified the malicious traffic as a Layer 3 DDoS attack. They also determined that the attack originated in several Eastern European countries. Prolexic DDoS mitigation engineers used

"Prolexic responded to our initial request for help with great speed and our site was back online almost immediately."

PROLEXIC
DDoS Attacks End Here.

20 mitigation tools, many of them proprietary, to monitor DDoS activity and counteract the attacker's signature changes on the fly.

Staying protected with Prolexic

Today, BidCactus.com still relies on Prolexic's DoS and DDoS protection to keep its auctions online and available to its millions of global bidders. Dvornek has never uncovered the reason why BidCactus was singled out for this large DDoS denial of service attack, even though he knows that other online auction sites have been targeted in the past.

"Prolexic was very helpful throughout the whole DDoS mitigation process," Dvornek says. "Its engineers immediately answered any questions we had and they fully understood the urgency of our situation. With the site down, we couldn't serve our customers and time was of the essence."

"Because of the fact that there's no limit to incoming bandwidth, Prolexic will always help us mitigate whatever type of attack might come our way," continues Dvornek. "My advice to other online businesses would be to secure DDoS protection. The cost of denying service to a site is shockingly low. Everyone can be a target and anyone can be a potential DDoS attacker."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

americaneagle.com
REDEFINING THE INTERNET

Prolexic Protects Americaneagle.com's Network Against DDoS Attacks

Since 1995, Americaneagle.com has built and hosted some of the world's most high-profile websites in e-Commerce, sports, and the government sector. The Chicago Transit Authority, the United States Tennis Association, the Chicago Bears, and a high-end shoe retailer whose designs are worn by award-winning actresses on the red carpet, are just a few examples of Americaneagle.com's customer base of thousands of online businesses.

Over the last four years, Americaneagle.com's network experienced occasional DDoS distributed denial of service attacks of various sizes, but nothing that the company's hosting department couldn't handle on their own. However, that changed earlier this year.

> Company under a DDoS attack

American Eagle, a leading website development and hosting company

> Type of DDoS attack

Layer 7 web application attacks, SYN Floods, and other variants

> Prolexic attack mitigation strategy

PLXrouted DDoS mitigation service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

After experiencing its first major DDoS attack in February, various customers were attacked 15 times over the next two months. Not only did Americaneagle.com see far more DDoS attacks than in the past, but it also experienced multiple types of attacks. Some were Layer 7 that tried to overwhelm web servers while others were UDP floods designed to overwhelm network infrastructure. Company management knew it had to solve its DDoS problem as it takes customer uptime very seriously.

Chief Technology Officer Ryan McElrath and his team quickly began looking for solutions. They researched multiple DDoS mitigation services, including a service offered by one of their current ISPs. Prolexic was the clear choice.

"As we started to research our options further, we soon realized that there were certain requirements we needed in a provider. Above all, we wanted a company whose core focus was DDoS protection and one that had a proven track record defending against large attacks," says McElrath. "Due to the sharp increase in DDoS attacks across the Internet these last several years, more companies are starting to offer this type of service, but, for most of them, it's a secondary product. We didn't want to go through growing pains with a company as they tried to learn how to reliably fend off DDoS attacks. Prolexic had the experience and expertise that we needed right now – this was obvious when talking to Prolexic's engineers and comparing that to our calls with their competitors.

"Another differentiating factor was how overage fees were handled by the various DDoS providers," McElrath says. "For example, our Prolexic contract covers unlimited attacks against our general network and also doesn't charge overage fees based on attack size. None of the other DDoS providers that we talked to could provide us with a package that would eliminate the possibility of us getting handed a huge overage bill in the tens of thousands of dollars at the end of any given month. At that time, our customers were getting frequently

PROLEXIC
DDoS Attacks End Here.

PROLEXIC
DDoS Attacks End Here.

attacked and it was impossible for us to know how many more attacks were coming. Prolexic was the only DDoS provider that offered us a service that met our needs."

Prolexic's DDoS mitigation strategy

Prolexic's PLXrouted DDoS distributed denial of service mitigation solution was deployed to protect Americaneagle.com's network and hosting infrastructure.

"Prolexic was able to set up the service very quickly and we've been very happy with it," McElrath says. Since bringing Prolexic on board, Americaneagle.com can now offer its customers comprehensive DDoS protection packages through Prolexic for an additional fee.

Prolexic's protection was put to the test earlier this year when attackers launched a DDoS attack against the website of one of Americaneagle.com's e-Commerce customers who was paying for DDoS protection through the company. This attack was a combination 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 global reputation for reliable service.

Staying protected with Prolexic

Americaneagle.com is confident in Prolexic's ability to protect e-Commerce sites against the potentially devastating financial losses that occur when sites are brought down by DDoS attack. Many of the company's e-Commerce customers are high-profile brands that have been featured on the Oprah Winfrey show, and some have retail stores located on Fifth Avenue, Rodeo Drive and Michigan Avenue. If a DDoS attack brought down these or any of the firm's hosted e-Commerce sites, tens of thousands of dollars per hour could be lost.

"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."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

Prolexic Enables IPG to Protect Enterprise Payment Processing Services Against DDoS Attacks

IPG Holdings Limited is an independent, privately-owned technology company that specializes in the development, maintenance and support of an enterprise payment gateway platform. IPG provides this platform through Software-as-a-Service (SaaS) as a privately-labeled offering to sales organizations that market to merchants seeking a full-service payment service application. The company's infrastructure is a high availability, fault-tolerant environment serviced from three data centers located in Europe.

While IPG itself has not been the primary target of a Distributed Denial of Service (DDoS) attack, a merchant using IPG's payment platform has been attacked a number of times. IPG's monitoring systems picked up unusual spikes of data hitting a particular payment form URL, which was flooded when the merchant's sites were under attack. This attack took both IPG and the targeted merchant by surprise and while it caused minimal downtime to IPG's network, the attack disrupted service delivery to a number of customers being serviced on the same subnet.

> Company under a DDoS attack

Customers of IPG, provider of a cloud-based, private label, enterprise payment gateway platform

> Type of DDoS attack

Concurrent GET Flood, UDP Fragment, and RESET Flood peaking at 200 Mbps, 50,000 pps and 4.5 million connections per second

> Prolexic attack mitigation strategy

Prolexic's proprietary tools and real-time monitoring by Prolexic technicians

> Time to DDoS mitigation

Within minutes, once traffic started flowing through Prolexic's cloud-based scrubbing centers

"We host payment forms for some large direct merchants and payment service providers, and these front-facing forms have been the vulnerable points of attack," says Alan Conder, chief executive officer at IPG International Limited. "The merchants embed the URL of the IPG payment form in their websites, so the attackers scanning the websites have picked up the IPG URL and have included it in their attacks."

At first, IPG was able to mitigate these attacks by simply 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.

Prolexic's DDoS mitigation strategy

The DDoS attack on IPG's customer consisted of burst attacks that started on Friday and continued into the weekend for approximately 48 hours. These attacks reoccurred every week for three weeks. IPG management realized that they could not continue to black hole attacked IP addresses, despite the fact that doing so prevented the attacks from taking IPG down completely. Management had heard of Prolexic through word-of-mouth and decided to engage its mitigation services.

"Once we engaged Prolexic, the IPG payment form on the merchant's site was back up in minutes."

PROLEXIC
DDoS Attacks End Here.

It was no surprise when IPG was soon attacked again, but this time it was ready with Prolexic's industry leading cloud-based mitigation network. Prolexic technicians quickly identified two attacks for mitigation. The first was a short 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 realized their efforts were never going to succeed against Prolexic's 500 Gbps mitigation network.

The Prolexic team used 20 mitigation tools, many of them proprietary, and drew upon nearly a decade of experience in monitoring and blocking changing attack signatures in real time.

"Once we engaged Prolexic, the attack was mitigated within minutes," Conder says. "Even though there were more attacks on the merchant's site and IPG payment form later, the merchant was able to continue processing with only a minor disruption. The attack eventually ceased completely once the attackers realized that the Prolexic service was activated."

Staying protected with Prolexic

IPG continues to have confidence in Prolexic and has peace of mind that the company has the experience and tools to provide ongoing insurance against any type of DDoS attacks. "Prolexic's service was, and continues to be, exceptional," Conder says.

Today, IPG works with Prolexic to offer IPG customers a DDoS-protected payment form URL, which IPG manages on behalf of the merchant as part of its service. This protection has been put in place for all IPG merchants/customers who have come under DDoS attack to date.

"We are beginning to proactively market the form-based offering and are referring larger merchants to Prolexic to protect their front end sites," Conder says. "Overall, I would suggest to others 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."

IPG itself has not been attacked since engaging Prolexic, but one fairly new merchant/customer – who had not yet taken on IPG's protected form-based service – was the target of a DDoS attack through the payment form URL.

"IPG has instigated a no-tolerance policy in that if a merchant using one of our forms is attacked, and the attack filters down to us, we simply shut their form down and insist that they sign up for the PLX/IPG Payment Form solution," Conder says. "We won't bring their form back up until Prolexic protection is in place."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Prolexic Defends Blogging Website Against Six-Month DDoS Attack Campaign

Once a small start-up, this media company has grown rapidly and now operates a popular, global website and respected blogging platform with millions of users. Unfortunately, success can be too much of a good thing. With a high online profile, the company's blog site has been the target of multiple politically motivated DDoS attacks, specifically in protest against blog posts that criticize certain government leaders and ideologies, including a blog page suspected of exposing government secrets. These attacks affect performance and the availability of tools and services used by the site's bloggers. Even worse, when the site is taken offline, the company cannot deliver ads on behalf of its clients, which impacts revenues.

In November 2011, the site experienced the first significant DDoS attack in what would become a six-month long campaign of attacks that varied in size, signature, and duration. Despite the efforts of in-house administrators and having recently upgraded hardware and software, they could not mitigate the Layer 3 UDP Flood that characterized the first attack. Several DDoS mitigation vendors were contacted, but none could mitigate the attack. The company's senior management team was eventually referred to Prolexic.

> Company under a DDoS attack

A popular, global blogging website and platform

> Type of DDoS attack

An on-going DDoS campaign of Layer 3 and Layer 7 attacks lasting more than six months

> Prolexic attack mitigation strategy

PLXfbm (flow based monitoring), PLXabm (application based monitoring) and PLXrouted solutions

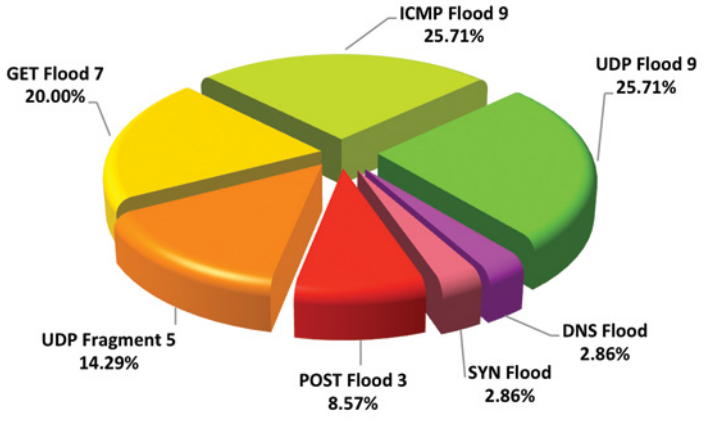
> Time to DDoS mitigation

Within minutes of routing traffic through Prolexic's cloud-based mitigation network

Prolexic's DDoS mitigation strategy

As soon as Prolexic's DDoS protection solution was provisioned and traffic began flowing through its cloud-based attack mitigation network, the world's largest at over 500 Gbps, clean traffic began flowing to the blogging website. Usually, attackers back off once they see that Prolexic has been provisioned for DDoS mitigation, but these cyber criminals continued to target the site with high volume and complex attacks of both short and long durations despite their failure to bring the site down.

Total Attack Types



PROLEXIC
DDoS Attacks End Here.

"Prolexic is the go-to company for handling large-scale DDoS attacks."

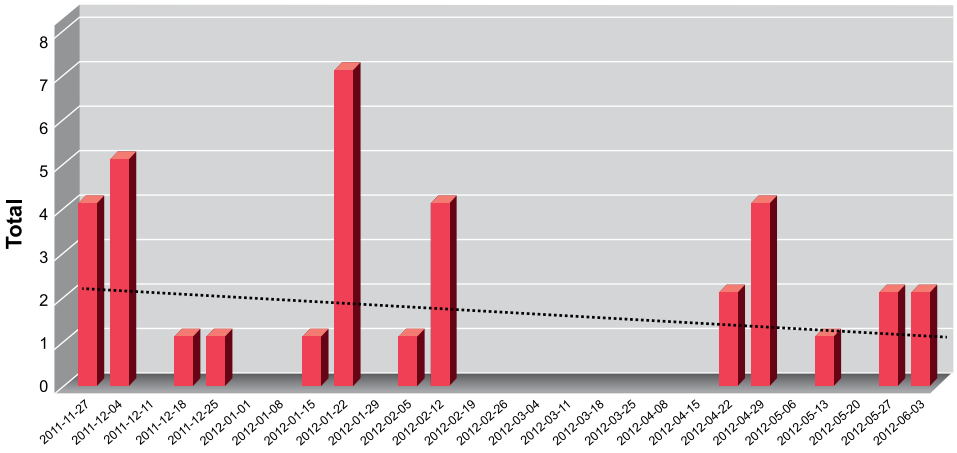
PROLEXIC
DDoS Attacks End Here.

"The blogging site has been repeatedly hammered for the last six months by DDoS attackers," says a DDoS technician at Prolexic. "From the forensics we've gathered, we can see that this attack campaign is most likely politically motivated, and not so much targeted at the blogging site itself, but rather at the often incendiary political views that certain bloggers post there."

During provisioning of Prolexic's service and over the following months, Prolexic's Security Operations Center monitored a wide variety of attack types. "Often a DDoS attacker will use two or maybe three attack types at most, but the attacks on the blogging site were somewhat unique because they were so varied," says the Prolexic technician.

Prolexic's forensic evidence also revealed that the majority of the botnets used in the attacks were located in Russia and China, with other bots spread throughout Europe.

Total Attack Types
Interval: week



The attack campaign eventually peaked at 11.80 million packets per second – the largest ever experienced in the site's 12-year history. Attack events varied in lengths from 1 to 26 days and spanned more than 6 months. The site was hit an unprecedented 106 days out of 180. Fortunately, Prolexic protection was in place, so the blogging site avoided the downtime and inconvenience that DDoS usually causes.

"We found that there are many DDoS mitigation providers, and even ISPs claim to offer protection against DDoS attacks," says a senior executive responsible for the blogging site. "But ISPs are severely limited in mitigation bandwidth and expertise. Prolexic was the only vendor we found with the capacity, knowledge, and experience to stop these DDoS campaigns and do it quickly."

Staying protected with Prolexic

Although politically motivated DDoS attackers still attack the blogging site, Prolexic continues to actively repel even the largest and most complex DDoS attacks against the site.

"Prolexic is the go-to company for handling large-scale DDoS attacks," the senior executive says. "Every time we're on the phone, it's with engineers that know their stuff. Ultimately you're going to want to have a mix of internal mitigation and one or several providers if you're a big target. My personal experience is that when you're dealing with a DDoS of this scale or complexity you need Prolexic. There is simply no one else that can handle this level of traffic."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

DDoS Attack Halted on RealVision as soon as Prolexic Services Engaged

RealVision manages the websites and domain names for a popular online movie subscription service. On a recent Saturday afternoon, the movie subscription site was brought down for about 12 hours by a Distributed Denial of Service (DDoS) attack. Subscribers were not able to download and view movies and the movie site could not accept new member subscriptions, which is the main source of revenue for the service.

"We had minimal protection with a hosting company, but nothing that could handle what we were hit with," says Mark Johnson, chief financial officer at RealVision. "The DDoS attack took down the entire hosting company, as well as our movie subscription website. Because the attack was targeted at us, the hosting company literally unplugged our server because they didn't know any other way to mitigate the attack."

> Company under a DDoS attack

An online video/movie subscription service operated by RealVision, a domain management company

> Type of DDoS attack

High bandwidth Layer 3 attack

> Prolexic attack mitigation strategy

Routing the client's traffic through Prolexic's global scrubbing centers

> Time to DDoS mitigation

Immediate – the attack was abandoned as soon as attackers became aware of Prolexic protection

Johnson conducted a fast online search for a DDoS mitigation company. He found several providers and quickly contacted them by phone. But only one company stood out as the right choice: Prolexic.

"I spoke with Prolexic and felt that we had the best communication about our problem," says Johnson. "Prolexic were the most straightforward and transparent in describing their solution and they understood exactly what we were going through and the risks involved to our business. They were able to draw up a contract very quickly and started the process to get us the DDoS protection we needed."

Prolexic's DDoS mitigation strategy

After RealVision began routing traffic to its movie subscription site through Prolexic scrubbing centers, DDoS attackers struck again – this time with an attack on RealVision's header IP addresses. But this time the attackers were in for a surprise. They quickly abandoned their attack as soon as they realized that RealVision had changed its IP addresses to direct traffic through Prolexic's global network of scrubbing centers.

According to Neal Quinn, Prolexic's vice president of Operations, attackers can tell when a site's traffic is routed through Prolexic and that can be a deterrent. "Attackers are very shrewd," says Quinn. "They are looking for easy targets that require minimal resources to take down. They know they cannot take out Prolexic's scrubbing centers and vast attack mitigation network so they move on."

PROLEXIC
DDoS Attacks End Here.

Staying protected with Prolexic

Johnson believes having DDoS mitigation protection with Prolexic is good insurance for RealVision because cyber attacks are becoming larger, more prevalent and increasingly damaging to online businesses. In fact, many clients view Prolexic's mitigation services as an insurance policy against DDoS attacks and prolonged outages. And just like insurance, it's available when you need it most.

"We really were not aware of how big and how strong a DDoS attack could be, and how much it could really affect our business, until we got hit by one" Johnson says. "You hear about DDoS, you know about it, but you think it really won't happen to you. We never really understood how much protection we needed – we learned the hard way. So we're taking preventative measures with Prolexic."

Johnson notes that RealVision's management was impressed by Prolexic's fast response time. "They say it's 24/7 service and it really is," Johnson says. "That's a comforting feeling when your site is under DDoS attack."

"The DDoS attacks we experienced weren't child's play," Johnson adds. "Someone intentionally attacked us, but as soon as they saw we had Prolexic protection they stopped. Prolexic gives us the strong insurance policy against DDoS attacks that we were looking for."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

yola build. promote. succeed.

Prolexic Protects 6 million Websites Against DDoS Attacks for Yola Hosting Service

Yola was launched in October 2007 in South Africa with an innovative concept – provide free basic website building and hosting services to small businesses to help them build their online presence with a professional looking, ad-free website. Yola also offers premium web hosting services at a fee, such as custom domains, add-on advanced features, and premium styles when customers are ready to take their business to the next level. Yola quickly grew to 10,000 customers and then experienced very rapid growth when it was incorporated in the U.S. in 2008 and opened a joint headquarters in San Francisco. Suddenly, Yola's user base jumped to millions of customers from around the world.

Around the same time, Yola began to experience Distributed Denial of Service (DDoS) attacks. The attacks were targeted at Yola's customers, whose websites were hosted on shared servers. This infrastructure made all of Yola's customers more vulnerable – an attack on one site could bring down all of the others residing on the shared server. Yola has very strong IT resources in-house and a very technically advanced data center, so the company was able to manage attack mitigation for about a year.

> Company under a DDoS attack

Yola, a global website builder and hosting service

> Type of DDoS attack

High packet-per-second (6.2 Gbps) Layer 4 UDP Flood

> Prolexic attack mitigation strategy

Prolexic's proprietary tools and real-time monitoring by Security Operations Center technicians

> Time to DDoS mitigation

Within minutes once attack traffic started to flow through Prolexic's scrubbing centers

"The number and size of the DDoS attacks were increasing, so we started purchasing bigger and bigger routers and firewalls to absorb and mitigate them," says Lisa Retief, vice president of Engineering at Yola. "But we were still struggling. I was aware of expensive hardware for DDoS mitigation, but that wasn't a good solution for our hybrid data center/cloud production infrastructure. Also, our business relies on being a distributed network, with the ability to route our customers' traffic to one or more virtual IPs anywhere. So purchasing our own hardware and putting it all in one place would be insufficient."

Yola experienced its largest and most intensive DDoS attack last year – and the IT staff could not mitigate it despite working through the night. The attack caused outages not only for Yola's customers, but also brought down Yola's data center and affected upstream Internet Service Providers (ISPs) in a large part of Boston and the surrounding area. The upstream ISPs refused to bring Yola's servers back up in order to protect their other clients and gave Yola an ultimatum: find a reliable DDoS mitigation solution first.

Engineers on Yola's 24/7 e-mail customer support group and public forum were deluged with inquiries from customers whose sites were completely unavailable. For nearly 3 days, dealing with the DDoS attack was the only focus at the company – all other business and projects were put on hold. To this day, Retief has no idea why Yola's customers were attacked or by whom.

PROLEXIC
DDoS Attacks End Here.

"This was when I first became aware of Prolexic," say Retief. "We did some research and we knew we wanted an 'always on' mitigation solution. Everywhere we inquired, we were told that Prolexic was the best. We made the decision to go with Prolexic around midnight and we had to wake up our CFO for approval. It was a very stressful time for our company."

Prolexic's DDoS mitigation strategy

Prolexic technicians quickly determined that the DDoS attack was a very large Layer 4 UDP flood with peak bits per second of 6.2 Gbps and peak packets per second of 650 Kpps. As a result of Prolexic's industry leading attack mitigation capacity, the attack was mitigated almost immediately. Prolexic also collaborated with Yola's in-house IT department on a solution to protect both Yola's corporate website and its 6 million-plus customer sites against DDoS attacks. Because Yola was able to provision Prolexic's services so quickly, both teams had to scramble to re-route 6 million customer sites to the new virtual IP addresses provided by Prolexic – and it took only 3 days.

Yola has a number of virtual IP addresses with Prolexic and its customer web sites point to those addresses. Traffic requests to the customer sites are filtered through Prolexic scrubbing centers and then passed on to Yola's infrastructure. When Yola gets the requests, its IT department routes them to the particular server that hosts the customer sites.

"Prolexic stops any malicious traffic from getting through to us or our customers," Retief says. "We tell our customers that they are getting premium DDoS attack protection from Prolexic and that has increased the value of our service, as well. In the year we've been working with Prolexic, we've built a very strong relationship with them."

That relationship, however, was almost short lived as the contract renewal date with Prolexic approached. In its race toward profitability, Yola was implementing some cost cutting measures and considered using another DDoS mitigation solution that would cost less. "As we came closer and closer to the date we would switch to another vendor, my lead engineers and I were unhappy with the technical solution that we were being pushed toward and with the competence of the people we would have to deal with. At that point, we went to Prolexic to try to see if there was a way to continue our relationship. They worked out a solution to keep our business and that further strengthened the relationship between Yola and Prolexic quite a bit."

Staying protected with Prolexic

Prolexic continues to protect Yola and its 6 million customer websites with always-on DDoS mitigation services that combine the latest proprietary mitigation and decryption tools, plus the live human expertise of 24/7 monitoring by Prolexic technicians in the company's Security Operations Center (SOC). Retief says that she has been very impressed with Prolexic's customer service and technical knowledge, as well as the company's detailed attack reports.

"It's wonderful to get an e-mail at 2 a.m. and be told that you're under attack and to be able to go back to sleep and not worry about it, whereas in the past we'd have to wake up five engineers, be working with our data center and be talking to our users in the middle of the night," Retief says. "We suffered quite a bit of brand degradation around the time we were getting so many attacks. It took almost a year to break that association and it helped to use Prolexic's DDoS protection as a selling point."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.060713

Betstar Bets on Prolexic for Distributed Denial of Service Protection

Betstar.com.au is a popular online betting site that offers Internet betting on Australian and international sports and racing. Personalized service is the hallmark of Betstar's reputation in the bookmaking industry, so it is important that the online betting site is always available and responsive. Site performance and availability are particularly critical during the weeks of the Spring Carnival leading up to Australia's most famous horse racing event, the Melbourne Cup. Millions of bettors – some of whom place their only bets during the year on these internationally known races – rely on Betstar to provide them with easy, reliable online betting for the event.

> Company under a DDoS attack

Betstar.com.au, a popular Australian online betting site

> Type of DDoS attack

High-volume Layer 3 infrastructure attack on a shared data center

> Prolexic attack mitigation strategy

PLXproxy service with Prolexic's protected DNS

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

Recently, during the first weekend of the Spring Carnival racing season, cyber attackers launched a high volume DDoS distributed denial of service attack against the IT infrastructure of one of Betstar's competitors. Both companies share infrastructure at the co-location data center, so when the 10 Gbps DDoS attack on the competitor's website brought down the entire data center, both sites experienced outages. Betstar was down for 30 minutes before switching over to a redundant system, while the competitor's site was down for an entire day. Two other online betting sites were also taken offline by DDoS attacks that weekend, which served as a clear warning that the entire Internet bookmaking industry was at high risk. In fact, the DDoS attacks continued every Saturday for four weeks straight.

"The weeks leading up to the Melbourne Cup are extremely busy," says Bryan Dunne, IT manager at Betstar. "This time period makes the year for every online bookmaker in Australia. If you experience website outages during Spring Carnival, then you can wipe out a nice chunk of your profits for the year."

Prolexic's DDoS mitigation strategy

When Dunne realized that the online bookmaking industry was a prime target for DDoS attacks, he began to look for a DDoS mitigation service. Betstar's infrastructure provider recommended Prolexic for distributed denial of service protection. After contacting Prolexic, Dunne was impressed with its quick response and understanding of the urgency of the situation with a critical seasonal event just a few weeks away.

Prolexic and Betstar made it a priority to get the PLXproxy (non-emergency) DDoS mitigation service in place on time. Dunne and his contacts at Prolexic worked over a weekend to get the contract signed and approved by both parties. Next, Dunne's IT infrastructure team worked with Prolexic's mitigation engineers on the deployment. Betstar tested the Prolexic solution on Friday and

PROLEXIC
DDoS Attacks End Here.

on Saturday Dunne and his IT team were confident that the Betstar site was fully protected against DDoS attacks – in plenty of time to ensure site availability for customers betting on the Melbourne Cup.

"You never know when you'll be the target of a DDoS attack, so we moved forward quickly with the decision to go with Prolexic," Dunne says. "The cost of a site outage due to DDoS far outweighed the cost of protection, and Prolexic gave us a very fair price."

Almost immediately after the Prolexic solution was deployed, Betstar experienced a DDoS attack indirectly. The company shared a name server and data center with a competitor and when that firm was targeted by a DDoS attack, the Betstar website experienced a brief period of downtime due to collateral damage.

The DDoS attack came through one server that was not protected due to the fact that its DNS name change had not yet replicated completely around Australia. Betstar needed to keep that server available so that people could still access the site, but despite that vulnerability to attack and a brief outage, Betstar was able to switch to a redundant server and continue serving customers.

"When the DNS name change was complete and we were fully protected by Prolexic, our site never went down again," Dunne says. For additional peace of mind, Betstar uses Prolexic's protected DNS service for all of its domains.

Staying protected with Prolexic

The DDoS attacks against the online gaming industry ended after the close of the Spring Carnival and the running of the Melbourne Cup. There was no ransom demand and no one has ever come forward to take responsibility for the attacks. Dunne notes, however, that online betting has long been a high risk target for DDoS, which is why Betstar continues to rely on Prolexic for reliable and proven protection.

Dunne is pleased that the Prolexic solution causes no latency issues, despite routing Betstar's site traffic from its Australia-based network through Prolexic scrubbing centers in the United States.

"Latency is a key concern for our website, and we were concerned that routing traffic to the U.S. would add seconds to page-load times, which could have a massive impact on our business," Dunne says. "Prolexic assured us that latency would be less than a half second, and it has been, even at very busy times. I think that's very impressive."

Most of all, with DDoS distributed denial of service protection by Prolexic, Betstar no longer risks losing revenue or potential customers at the company's most profitable time of the year.

"We plan all year for the Melbourne Cup," Dunne says. "Betstar spends a very large portion of its IT budget to make sure our website can scale to massive loads of site logins and spikes in traffic. We also spend a lot on testing and optimizing our website. But in the end, if we received a DDoS attack and didn't have Prolexic protection in place it all would be for nothing."

Dunne advises other online betting companies to be proactive in their DDoS mitigation strategies. If an online betting site is down for even an hour at the time of the Melbourne Cup, it would have an immediate and disastrous effect on revenues.

"I've recommended Prolexic to other companies," Dunne says. "Any company that relies on seasonal peaks, such as Spring Carnival, as a profitable time of the year should have DDoS protection in place. Our experience has shown that it's only a matter of time before you will be attacked."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.060913

paypro

Prolexic Protects Secure Transaction Servers Against DDoS Threats for PayPro Global

PayPro Global, headquartered in Toronto, Canada hosts an online reselling and distribution infrastructure for software developers worldwide. The company draws upon its wealth of e-Commerce expertise to help developers generate more revenue through a secure and easy online purchasing experience for local and international buyers. Dedicated to customer service, PayPro Global has an excellent reputation for support and service.

In August 2012, PayPro Global became the target of a major DDoS distributed denial of service attack. After an investigation, PayPro Global Marketing Manager, Valeriu Braghis, learned that the DDoS attacker was a disgruntled customer who had not received a refund quickly enough for a software product return. "In the attacker's eyes, this was payback for what was perceived to be poor customer service" says Braghis. "We didn't receive a ransom demand, but our company's reputation was damaged."

> Company under a DDoS attack

PayPro Global, a leading Canadian software reselling and distribution service

> Type of DDoS attack

Layer 7 attack against secure transaction payment servers

> Prolexic attack mitigation strategy

PLXrouted deployed to protect against future DDoS attacks

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

In late November 2012, the company was attacked again. This time the secure HTTPS module of PayPro Global.com was brought down for 16 hours by a distributed denial of service DDoS attack. The Layer 7 attack targeted the company's servers that are used to process secure payment transactions for its software developer customers. In the past, smaller DDoS attacks were able to be blocked by a firewall at the data center where PayPro Global hosts its servers. But this time the distributed denial of service attack was too large and complex.

"Being down for nearly an entire day and unable to accept payments is devastating in terms of lost revenue for our customers," Braghis says. "We lost half of our daily sales while the secure site was down, and some of our biggest customers in Russia threatened to go to another provider."

Prolexic's DDoS mitigation strategy

PayPro Global engaged Prolexic for DDoS mitigation services after a business partner recommended Prolexic. Braghis also did extensive online research on DDoS mitigation and found that Prolexic stood out as the most highly experienced and successful company against DDoS threats.

Prolexic's DDoS mitigation technicians were able to bring the secure PayPro Global site back up as soon as they began to route the site's traffic through Prolexic's global scrubbing centers. They continued to fight the attack using live monitoring techniques so they could instantly counteract any change

PROLEXIC
DDoS Attacks End Here.

in attack vectors in real-time. Prolexic's team also drew upon an arsenal of more than 20 proprietary and best-in-class commercial DDoS mitigation tools to augment their live mitigation tactics.

Prolexic continues to protect PayPro Global with its PLXrouted DDoS mitigation service. When Prolexic's Security Operations Center (SOC) personnel detect that PayPro Global is under DDoS attack, the PLXrouted service is activated using Border Gateway Protocol (BGP), and the site's traffic is automatically routed to Prolexic's global network of scrubbing centers.

Staying protected with Prolexic

With Prolexic protection in place, PayPro Global has a strong defense against all types and sizes of distributed denial of service DDoS threats throughout the year, whether they are launched by a disgruntled customer or sophisticated criminal organizations. Most importantly, this e-Commerce company has reduced its risk of devastating revenue loss for its customers due to DDoS attacks and has taken its already stellar customer service to a higher level.

"We have been very happy with the way Prolexic does its job of DDoS protection," Braghis says. "We have been attacked several times since bringing Prolexic on board, but our site never went down. Prolexic was successful against every DDoS attack."

PayPro Global's experience also proves that just about anyone can launch a DDoS attack since it is easy and inexpensive to deploy bots and/or malicious DDoS tools. The bottom line is that any website is at risk. "We're not sure what happened to the DDoS attacker who targeted us," Braghis says. "But we are confident that Prolexic will not allow this person or any other cyber attacker to take down our site down."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Prolexic Fights Off DDoS Attack to Keep e-Commerce Deals Flowing for a "Daily Deal" Website

The "daily deal" website is run by a UAE-based company that sources exciting products and services from local small and medium-sized businesses at great discounts, enabling its subscribers to take advantage of group buying. Launched in 2010, the site pledges to find its subscribers something cool to do in their local area every day with exclusive discount incentives. Each activity or deal requires a minimum number of people so businesses gain access to greater numbers of new customers.

In August, the site's technical team noticed a sudden increase in website traffic. It was so noticeable that they instantly knew the traffic was not due to a surge of genuine requests. Malicious traffic was tying up system resources and bandwidth, and as a result, legitimate customers were finding it increasingly difficult to access the website.

> Company under a DDoS attack

A leading UAE-based e-Commerce "daily deal" website

> Type of DDoS attack

Encrypted Layer 7 attacks from multiple geographic locations

> Prolexic attack mitigation strategy

Use Prolexic's proprietary tools and real-time monitoring techniques to block attack

> Time to DDoS mitigation

Two hours

"At such an early stage of developing our business in a region that has yet to fully embrace home-grown e-Commerce, any loss of accessibility to our site is a potential disaster," says the company's chief operating officer. "It's not just the lost business, it's the perception of our reliability that's on the line."

While the company was completely unprepared for such an unprecedented volume of traffic, its directors were determined to keep the website with its signature daily offers and updates accessible to subscribers. In addition, management made every effort to inform customers what was happening.

"It was difficult to communicate exactly what was happening during the attack as customers had little to no access to our site," the COO says. "However we were able to respond to individual queries via social media. We had to make it clear that the intended target was not our source code or customer details, but rather an attempt to inhibit our trading and damage our business."

When the attack started, company management contacted several of the largest hosting partners in the U.S. for help. The site migrated to the two companies that claimed to have DDoS mitigation tools that would stop the attack. When neither company could mitigate the attack, the "daily deal" website turned to Prolexic Technologies.

"One after another the hosting partners stated that the attack was too complex for their mitigation tools and that there was nothing more they could do," the COO says. "We had already begun to research who the leaders in DDoS mitigation were and, after talking to many engineers, Prolexic was the name that kept coming up."

PROLEXIC
DDoS Attacks End Here.

"We can mitigate all DDoS attacks, generally within minutes from when traffic is properly routed through our 'in-the-cloud' network."

PROLEXIC
DDoS Attacks End Here.

Prolexic's DDoS mitigation strategy

Company management contacted Prolexic via Prolexic's online emergency form and got an immediate response. After their traffic started flowing through one of Prolexic's globally distributed scrubbing centers, Prolexic's 24/7 Security Operations Center (SOC) team was able to mitigate the attack and provide full accessibility of the site to customers within two hours.

Prolexic's technicians identified the malicious traffic as a Layer 7 attack with both GET flood and SYN flood characteristics. For the next week after Prolexic's intervention, the attackers continued to target the "daily deal" site with variations on the attacks. However, Prolexic's skilled SOC engineers were monitoring the site's traffic in real-time and could immediately thwart any new attacks with Prolexic's proprietary Layer 7 mitigation tools. Prolexic technicians were also able to identify the locations and sizes of the botnets, ranging from as few as 95 to 11,900 machines in Asia, Africa, South America, Australia, and the U.S.

"We mitigate hundreds of attacks each week and while this attack type was a hybrid that we hadn't seen previously, we have the tools, the technology, and the processes at our fingertips to effectively adapt our protection," says Dan Goetz, Prolexic's director of service delivery. "We can mitigate all DDoS attacks, generally within minutes from when traffic is properly routed through our 'in-the-cloud' network."

Staying protected with Prolexic

The "daily deal" site now receives ongoing protection from Prolexic's mitigation service to ensure it does not lose any more uptime due to malicious attacks.

Now that the site is back up and running with its coveted daily deals, the company's management is sold on the value of Prolexic's high level of DDoS protection against increasingly sinister online attacks.

"The DDoS attack on [our site] was a malicious sabotage of our business and a very serious cyber crime," says the site's chief executive officer and co-founder. "We have no idea who launched the attack, but as a young e-Commerce business that relies 100 percent on the availability of our online storefront, the attack prevented us from trading, and no doubt this was the intention of whoever perpetrated the attack."

"I had my doubts about whether we would be able to find a solution to the attack we were experiencing," the COO says. "We were so impressed by the way Prolexic handled the whole situation and how proactive they were!"

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Spafinder Wellness 365™

Prolexic Restores Peace of Mind to Spafinder.com with Fast DDoS Attack Mitigation

At Spafinder.com visitors can view numerous wellness articles or find wellness and spa providers where they can redeem gift certificates or points earned. While the chairman and CEO thought it unlikely that the company's website would be attacked, he was proactive and had put in place a DDoS mitigation solution provided by its hosting company. This was a defensive move to protect the site against any attacks that might be launched during the company's busiest time of the year – the fourth quarter – when holiday sales usually generate a significant percentage of Spafinder's annual revenue. "We can't afford to go down at holiday time," says Spafinder's Chairman and Chief Executive Officer, Pete Ellis.

Unfortunately, when it really counted – during an attack – the mitigation solution provided by the hosting company did not live up to expectations. "The solution from our hosting company was supposed to monitor any spikes in traffic and be able to isolate and divert the traffic to limit our exposure to an attack. We found out that the protection they were offering us was like a 1960s car alarm. It did nothing for us except give us false peace of mind."

> Company under a DDoS attack

Spafinder, a global online resource for spa and wellness services and products

> Type of DDoS attack

A randomized series of Layer 4 and Layer 7 attacks

> Prolexic attack mitigation strategy

Prolexic's proprietary tools and real-time monitoring by Prolexic technicians

> Time to DDoS mitigation

Within minutes after traffic began flowing through Prolexic's mitigation network

When the attack started, Spafinder's 24/7 call center was flooded with complaints that customers could not access the website to view wellness content, redeem gift certificates or spend rewards points. Ironically, the call center agents needed to access the website to respond to customer requests, but they could not since the site was down. All they could do was take the customers' names and numbers and promise to call back.

"In addition to generating revenue through our site, we also get about 30,000 customers coming to the site looking for places to spend their certificates or rewards," Ellis says. "The attack was a double whammy on our sales and on customer service, as well."

When the hosting company could not mitigate the attack after trying for about four hours, Ellis realized that he needed a more experienced DDoS mitigation company. He called the CEO of another wellness product company that had been attacked earlier for advice.

"I could see that the attack could go on for days or longer if I didn't do something immediately," Ellis says. "On the recommendation of the CEO of our strategic partner, I called Prolexic, and our site was up and running at full capacity by 6 a.m. the next day."

Prolexic's DDoS mitigation strategy

Prolexic technicians began mitigating the attack around 2 p.m. As they began the provisioning process, they realized that the hosting company's DDoS mitigation tool was causing some issues.

They also discovered that one of Spafinder's servers was not operating properly. The Prolexic technicians teamed up with Spafinder's IT staff and the hosting company's technicians to troubleshoot and resolve both problems.

"Prolexic went above and beyond to help Spafinder ensure that their network would integrate properly with ours," says Neal Quinn, vice president of operations at Prolexic. "Even though we experienced a few external issues, we were still able to work with all parties to restore accessibility to their website the same day."

The Spafinder website became accessible to customers as soon as Prolexic was able to route the site's traffic through its globally distributed scrubbing centers. Spafinder was able to service a percentage of its normal daily volume of customers that evening and gained full capacity by early the next morning.

Although Spafinder's hosting company had told Ellis that this was a very sophisticated DDoS attack that was difficult to mitigate, Prolexic technicians immediately recognized it as a combination Layer 4 and Layer 7 attack – a common type that they had dealt with many times before. In addition, using a combination of Prolexic's proprietary mitigation tools and real-time monitoring, they were prepared to counteract every move the attacker made over two days of randomized attacks.

"As we deployed our mitigation tools and real-time monitoring, the attack would trickle down to almost nothing, and then another wave of attacks with a different signature would start," Quinn says. "The attack actually spanned 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 could send at us."

Prolexic identified the IP addresses of the top ten sources of the DDoS attacks, which included Kazakhstan, Belarus, Peru, and the United Arab Emirates. "I don't think that these attackers were after any kind of financial gain," Ellis says. "On the Internet, hackers are now doing things just to prove they can do it. I think the attack on Spafinder just got someone a 'merit badge' but that doesn't lessen the damage they did to our revenue and customer service."

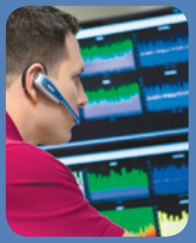
Staying protected with Prolexic

Since Prolexic mitigated the August 18 DDoS attack, Spafinder has not experienced another – a common occurrence once attackers see that a site is protected by Prolexic. With fourth quarter holiday sales season approaching quickly, Spafinder is gearing up for site traffic that will generate a significant percentage of total yearly revenues. A DDoS attack during the holidays would be a disaster, but now Spafinder is well prepared against that threat with Prolexic.

"If Prolexic had approached me with their solution six months ago without ever having been attacked, I would have said that Spafinder is not the type of company to have this type of problem," Ellis says. "But the reality is that we do 20 percent of our business online with 50 percent of that revenue coming in the fourth quarter. If there were any interruption to business at that time, it would cost us millions of dollars. Now I have no doubt that I need a solution from Prolexic, and it also makes me want to put protective measures in other areas of our business."

Ellis notes that it was easy to do business with Prolexic. "I felt that everybody wanted our business, from the company president on down," Ellis says. "Everyone was extremely responsive."

Ellis also has this advice for CEOs who believe that their companies aren't on an attacker's radar. "I never would have thought that we needed DDoS protection," Ellis says. "At the end of the day, the proliferation of attacks on all types of companies is becoming more serious. Now that it's happened to Spafinder, I say you have to have a DDoS mitigation solution from a company like Prolexic, especially if you have any type of e-Commerce platform."



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, energy, 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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

Prolexic Stops DDoS Denial of Service Campaign Against Partsgeek.com After Others Fail

Parts Geek® (www.partsgeek.com) is a popular e-Commerce website where auto repair shops and car enthusiasts can find discount auto parts and accessories from an online catalog of more than 10 million products. More than 100,000 daily site visitors rely on partsgeek.com to get the best deals and fast delivery of new, OEM, aftermarket, and rebuilt parts from trusted manufacturers.

Online orders ground to a halt, however, when a distributed denial of service (DDoS) attack hit partsgeek.com one Saturday evening earlier this year. The site was down for eight hours, resulting in thousands of dollars in lost revenue. The DDoS attackers returned and brought the site down for several hours on Sunday and Monday nights as well. The company's management looked to their Internet hosting provider for help with DDoS mitigation.

> Company under a DDoS attack

Partsgeek.com, a popular e-Commerce site for discount auto parts and accessories

> Type of DDoS attack

Layer 3 denial of service attacks

> Prolexic attack mitigation strategy

PLXproxy

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

"When the site went down on Saturday, our hosting provider told us that we were under a distributed denial of service attack," says Brian Tinari, president of partsgeek.com. "They told us that it was a huge volumetric attack ranging from 25 to 40 Gb per second and the bad news was that they did not have the resources to mitigate it. These DDoS attacks were causing 100 percent disruption to our business so we had to do something to stop them fast."

When the denial of service attacks continued through the next two evenings, Tinari approached another DDoS mitigation service provider, who also failed to mitigate the DDoS denial of service attacks. The issue was the same – the attack size was too big for them to handle.

"At that point we searched online for another DDoS mitigation provider and found Prolexic," Tinari says. "The denial of service attacks stopped as soon as Prolexic deployed their mitigation solution and we haven't been attacked since. The high-volume attacks seemed to be no problem for Prolexic."

Prolexic's DDoS mitigation strategy

Prolexic provided emergency denial of service mitigation to partsgeek.com through its PLXproxy service. After the site switched its IP addresses to Prolexic, all site traffic was routed through Prolexic's global scrubbing centers where any malicious DDoS traffic was removed. Prolexic's DDoS mitigation experts identified the denial of service DDoS attacks as high-volume Layer 3 attacks targeting the network infrastructure and routers.

"Setting up and provisioning the Prolexic DDoS mitigation service was incredibly easy," Tinari says. "I was very impressed with the knowledge and professionalism of the Prolexic team. They responded very quickly to our request

PROLEXIC
DDoS Attacks End Here.

for service and they were the only company that could stop these high-volume DDoS attacks."

Prolexic's engineers reported some spikes in traffic after provisioning the DDoS mitigation service but the distributed denial of service attacks against partsgeek.com stopped. This is not unusual since attackers have ways of knowing which sites are protected by Prolexic and they know that their tactics are no match for Prolexic's DDoS mitigation expertise, live monitoring and countermeasures.

Staying protected with Prolexic

Today, partsgeek.com still relies on Prolexic to protect its e-Commerce site against future DDoS distributed denial of service attacks. While Tinari had no warning of the previous attacks and still doesn't know who attacked or why, he is now very aware of the threat of DDoS and other cyber crimes that target e-Commerce sites in particular.

"I never thought that partsgeek.com needed DDoS protection," Tinari says. "I thought it would never happen to us, but the escalating size of the DDoS attacks over the three days disrupted our business 100 percent. I would advise other e-Commerce businesses to get DDoS protection before an attack even happens."

Tinari also recommends Prolexic. "I've been very happy with Prolexic's response and their customer support," Tinari adds. "Their team is very professional and quick and they were able to do what our hosting provider and other DDoS mitigation providers could not."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Leading Trading Platform Provider Global eSolutions Chooses Prolexic

Established in 2002, Global eSolutions (Hong Kong) Ltd provides sophisticated, customized IT solutions and services to members of the global financial industry. One of its clients 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 innovative proprietary trading technology from Global eSolutions to enable fast trade execution via personal computer and mobile devices.

This firm got caught in the wave of DDoS attacks against online financial services companies during the early months of 2012. Until management received an e-mail with a ransom demand in exchange for not being attacked, the firm had never experienced anything to do with DDoS. Days later, after receiving no response from management, Layer 3 and Layer 4 volumetric floods brought down the website for approximately four hours. A second, more damaging application layer attack occurred three weeks later, which rendered the trading platform almost inaccessible to online traders.

> Company under a DDoS attack

A U.K.-based online Forex trading firm that is a client of Global eSolutions

> Type of DDoS attack

Layer 3 and Layer 4 bandwidth floods

> Prolexic attack mitigation strategy

Use PLXrouted to direct traffic to Prolexic's cloud-based scrubbing centers in the event of attack

IT technicians at Global eSolutions detected the 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, IT 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.

"Most of the customers were unable to trade or access our application platforms during the second attack," says Ramon Chan, system architect at Global eSolutions. "Since we provide a real-time online trading platform, network performance and stability are important components of our system. Our reputation and customer trust will be damaged and need time to recover if a DDoS attack causes any service interruption."

Company management decided to tell clients that site availability had been interrupted by DDoS attackers. With the potential for ongoing financial losses if the attacks continued, clients demanded that the firm take steps to avoid any more prolonged outages. Chan did an online search to find DDoS mitigation service providers. Among the companies considered, Prolexic stood out as the most professional and experienced.

"Prolexic appeared to have the strongest defense against DDoS attacks," Chan says. "We were most impressed with their experience in successful DDoS mitigation for the financial industry. Prolexic also has more bandwidth to fight off very large

PROLEXIC
DDoS Attacks End Here.

attacks and they have a scrubbing center in proximity to our ISPs in Asia. All of these strengths added up to make Prolexic the obvious choice."

Prolexic's DDoS mitigation strategy

In event of an attack, the firm will leverage Prolexic's PLXrouted mitigation service. The preferred method of activating DDoS mitigation for enterprise-class businesses, this service provides protection for all services, ports and protocols while providing total control over when network traffic is filtered. DDoS attacks are detected by monitoring on-premise equipment and the traffic-routing service is activated using Border Gateway Protocol (BGP) to on-ramp network traffic to Prolexic's cloud-based denial of service DDoS mitigation infrastructure.

Staying protected with Prolexic

As an online trading group, the firm is still a prime target for complex DDoS attacks from hacktivist groups who continue to make headlines by bringing down the sites of large, global financial services companies. However, Global eSolutions is now protected by Prolexic.

"With a high availability network infrastructure plus Prolexic protection against DDoS, we can give our customers the confidence that our Forex trading platform is always secure and available," Chan says. "Also, we are protected against the huge financial losses that we and our customers would suffer if our platform went down. I would advise other online trading services companies to be proactive and have a DDoS mitigation service in place."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

VIRTUALROAD.ORG
SECURE HOSTING PROVIDER

Prolexic Partners with VirtualRoad.org to Provide Protection Against Politically Motivated DDoS Attacks

VirtualRoad.org (www.virtualroad.org) is a web hosting company with a bold mission – to provide a safe online presence for independent news media and human rights organizations in countries whose regimes forbid freedom of expression. Because these websites are prime targets for politically motivated cyber attacks – often coming from within the government regimes themselves – VirtualRoad.org fulfills its mission by providing a high level of protection against a wide range of web-based threats, including DDoS attacks.

Clients of VirtualRoad.org can choose from three standard packages of web hosting services or create a custom service package. "Resistance to Distributed Denial of Service (DDoS) attacks" is at the top of the list of services, followed by security against other online threats, secure backup of sensitive data, secure transfer of webmail, and a full complement of other professional web hosting services. Since its inception, the company has grown in DDoS mitigation expertise, and its highly trained technicians regularly advise clients on tailored solutions for DDoS protection.

> Company under a DDoS attack

Clients of VirtualRoad.org, a secure web hosting company serving human rights organizations and independent news outlets in countries where freedom of expression is threatened

> Type of DDoS attack

Layer 7 GET floods and attacks on DNS servers

> Prolexic attack mitigation strategy

Prolexic's proprietary tools and real-time monitoring to quickly mitigate large, complex attacks

> Time to DDoS mitigation

Within minutes after routing traffic through Prolexic

However, as DDoS attacks have escalated in size and sophistication in recent years, the DDoS mitigation team at VirtualRoad.org began to have difficulty mitigating Layer 7 and other more complex attacks. Management began to search for a DDoS mitigation services partner with the proven expertise and infrastructure to quickly stop this attack type. After reviewing a long list of providers, Prolexic emerged as the one partner who could meet all of VirtualRoad.org's requirements.

"The frequency and scale of the DDoS attacks were growing to a point where they were driving away audiences from our clients' sites," says Thomas Hughes, director, Media Frontiers, the parent company of VirtualRoad.org. "Our clients were finding it very difficult to survive online in this increasingly hostile environment and we knew we needed to ramp up our DDoS mitigation services. Our partnership with Prolexic is now a crucial element of the mitigation services we roll out to our clients."

Prolexic's DDoS mitigation strategy

VirtualRoad.org and Prolexic have had a formal partnership for nearly two years, although the informal relationship dates back longer. During that time, DDoS attacks that are too large and complex for VirtualRoad.org's mitigation services are immediately handed over to Prolexic.

For example, in March 2012, one of VirtualRoad.org's independent news media clients in Asia was hit with a Layer 7 GET flood and the sophistication of the attack was too complex for VirtualRoad.org's mitigation services.

PROLEXIC
DDoS Attacks End Here.

"We can now give peace of mind to our clients that they are protected against DDoS attacks."

PROLEXIC
DDoS Attacks End Here.

After routing site traffic to Prolexic's scrubbing centers, mitigation experts based at Prolexic's Security Operations Center (SOC) quickly determined the type of attack. They discovered that it was launched through a large multi-hop proxy network in order to mask the attackers' source IP address. As a result, a DDoS attack that may have brought the site down for many days or weeks was mitigated in just minutes by Prolexic. The attackers tried for several more hours to permeate Prolexic's defenses, but to no avail.

"Just yesterday, one of our client sites was hit with an attack on their DNS server," says Tord Lundstrom, chief technology officer, VirtualRoad.org. "The server was down for about 35 minutes and everything we tried didn't work. So we called Prolexic to help us quickly solve the problem. Although we can mitigate most attacks, we can give our clients the confidence that even if we can't solve the problem, our partner Prolexic can. In that way, we can promise them 100% protection against any type of DDoS attack."

"The collaboration between VirtualRoad.org and Prolexic works so well because we can leverage Prolexic's proven experience in protecting large enterprises against DDoS attacks," Hughes says. Simply put, we can now give peace of mind to our clients that they are protected against DDoS attacks, no matter how large or sophisticated – and we can mitigate these attacks faster and with a guaranteed success rate."

Staying protected with Prolexic

Today's "for hire" and politically motivated cyber attackers are more active than ever. Even worse, they are using increasingly sophisticated DDoS attack signatures that can easily overcome most hosting services and content delivery networks – but not VirtualRoad.org. Even though its clients' websites continue to be DDoS targets due to the nature of their content, they are far less vulnerable to being taken down or disrupted because VirtualRoad.org's DDoS protection services are backed by Prolexic.

Hughes and Lundstrom agreed that VirtualRoad.org's partnership with Prolexic is a unique, value-added service that translates to a key selling point with both potential and existing clients alike. "Prolexic not only provides us with a strong guarantee of security for our hosting service, but it also lets us show our clients that we have the fire power to back up our promise of DDoS mitigation," Hughes says. "Our clients must exist without disruption to continue their goal of promoting human rights issues and freedom of expression. Knowing that our organization and Prolexic are there to defend them against DDoS attacks is a fantastic guarantee."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.060713

Prolexic Stops Layer 7 DDoS Denial of Service Attack Campaign Against e-Commerce Company

At the beginning of the year, an e-Commerce company's website received an unusually large volume of traffic. This overwhelmed the site and made it unavailable to customers for approximately 30 minutes. After a thorough analysis, the company's IT team discovered that the outage was caused by a Distributed Denial of Service (DDoS) attack that came through the circuit between the site and the Internet Service Provider (ISP). Other customers of the ISP were also affected. Days later, the site was attacked again resulting in a three hour outage, so the company began searching for a DDoS mitigation service provider. A business partner in the same industry recommended Prolexic, whose DDoS mitigation technicians quickly provisioned its PLXproxy mitigation service to stop the attack.

After selecting Prolexic, the company decided to install a firewall against future DoS and DDoS threats as part of its internal defense strategy. The firewall was scheduled to go live, but another, more complex Layer 7 denial of service attack hit the site just a few days beforehand. The company immediately activated the Prolexic PLXproxy service.

> Company under a DDoS attack
An e-Commerce company

> Type of DDoS attack
GET Flood

> Prolexic attack mitigation strategy
PLXproxy mitigation service

> Time to DDoS mitigation
Within minutes under Prolexic's industry leading service level agreement

"This DDoS attack didn't bring the site down, but it flooded the bandwidth of the ISP circuit," says the CTO of the e-Commerce company. "It appeared that the site was up and running, but the server was overwhelmed with customer order requests and could not authenticate them. This situation had the potential to severely impact revenue since it was our busiest and most profitable month. It could have been far worse if not for Prolexic."

Prolexic's DDoS mitigation strategy

Prolexic mitigated each attack in the campaign (all Layer 7) on the e-Commerce site within minutes. The customer activated PLXproxy after detecting the first service attack. Within minutes, Prolexic diverted all site traffic to its scrubbing centers where malicious traffic was removed and clean traffic routed on to the e-Commerce site.

The first DDoS attack in the campaign started one afternoon – just a few days before the installation of the new firewall – and ended in the early morning hours the next day. This GET Flood peaked at 500.00 Kbps (peak bits per second), 4.00 Kpps (packets per second), and 25.00 Kcon (connections per second). DDoS attackers struck again less than 30 minutes later with another, stronger GET Flood that peaked at 6.50 Kpps and 50.00 Kcon. Yet another GET Flood of similar size followed a few minutes later and continued into the next day. The campaign continued for two weeks. Throughout the campaign, Prolexic's technicians used proven DDoS detection and DDoS monitoring techniques to identify the attack vectors and respond in real-time to the

PROLEXIC
DDoS Attacks End Here.

attacker's changes in strategy to ensure that no malicious traffic would reach the e-Commerce site's network and applications.

"I must commend the Prolexic DDoS mitigation team who were on the attacks like a watchdog," says the CTO. "That gave us the confidence that our site would be protected and available for business."

The CTO notes that his IT team was able to deploy the firewall as planned despite the DDoS attacks. "While Prolexic was mitigating the service attacks, it gave us time to put our applications behind the firewall and deploy our new IP addresses," the CTO says. "We were able to proceed with some planned outages, as well, because we had a DDoS mitigation plan in place with Prolexic. We were ready."

Staying protected with Prolexic

The e-Commerce site has not been attacked again since the DDoS denial of service campaign ended in early April. The company's IT team monitors the firewall to watch for DDoS attacks that exceed its bandwidth and the size of the ISP circuit. If such a threat occurs, they can immediately activate the PLXproxy service for DDoS mitigation in just minutes.

"We have Prolexic in case we detect a threat that we cannot mitigate with the firewall, or that cannot be mitigated by our ISP," the CTO says.

"The Prolexic technicians explained to us that their DDoS mitigation service works whether our site would be attacked directly or through our ISP. We're happy with Prolexic because they are DDoS specialists and they have demonstrated that with their quick response and successful mitigation. DDoS mitigation is their core domain of expertise and that gives us confidence."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Prolexic Restores Automated Utility Bill Payment System Brought Down by DDoS Attack

Prolexic's customer is a large metropolitan utility company that provides services to an estimated 1 million electric, water and sewer customers. Distributed denial of service (DDoS) attackers had launched a sophisticated, combination Layer 4 PUSH flood and ACK flood that took down the utility company's website and its pay-by-phone automated billing system for 48 hours.

More than 100,000 utility customers pay their bill online or through the automated telephone system, but during the DDoS attack they had to pay in person at the utility company's main office or local payment centers. Utility customers could still call in to pay their bills, but the calls were being handled by live customer care agents and there were long delays. The distributed denial of service attack also caused problems for the utility's employees, who could not receive external e-mails.

> Company under a DDoS attack

A U.S. metropolitan utility company that provides electric, water and sewer services

> Type of DDoS attack

Combination Layer 4 attack

> Prolexic attack mitigation strategy

Prolexic's PLXrouted service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

"We have a dedicated IT team just to prevent this sort of thing, but no matter how well you build your system, there are people out there who will try to break it," says a representative of the utility company. "The good news is that no customer information has been compromised."

Prolexic's DDoS mitigation strategy

Around 11 p.m. of the second day of the attack, a representative of the utility company called Prolexic and requested emergency DDoS mitigation services. After contracting services, the Prolexic Security Operations Center (SOC) immediately opened up lines of communication at both the technical and management levels per SOC best practices. Prolexic's DDoS mitigation engineers examined the attack vectors and quickly determined that the attackers were very skilled and were targeting backend IPs directly. Armed with this knowledge, the Prolexic team developed and launched a specially crafted routed DDoS defense that immediately began to reduce the strength of the attackers' sophisticated tactics. In this case, Prolexic installed full border gateway protocol (BGP) peering and generic routing encapsulation (GRE) tunneling to enable the utility company to connect to Prolexic in only a few hours.

"Despite the severity of the DDoS attack, Prolexic's mitigation engineers worked diligently and calmly with our IT staff to walk them through the process of building GRE tunnels and BGP sessions using a private autonomous system number or ASN – configurations that our IT staff had never dealt with before," said a representative of the utility company.

PROLEXIC
DDoS Attacks End Here.

Prolexic mitigation engineers continued to fight the distributed denial of service attack and quickly changed defense strategies as the attackers modified their attack signatures. The combination attack peaked at 3.3 Gbps and 5.7 Mpps (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," says 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."

Staying protected with Prolexic

The Prolexic PLXrouted DDoS mitigation solution continues to protect the utility company against future distributed denial of service threats. Prolexic is also working closely with the utility company's information technologies, compliance and security divisions and an outside investigative firm hired by the utility company to identify the attackers and bring them to justice.

"Utilities are another vertical that is likely to be increasingly targeted in the coming months as attackers look for maximum impact beyond daily targets like e-Commerce and financial services," says Stuart Scholly, president at Prolexic. "While we may never know the reason behind this DDoS attack, this utility knows for sure that it will be protected against all types and sizes of distributed denial of service attacks with Prolexic."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

Attack on Spanish-Language News Site is Abandoned When Traffic Routes to Prolexic

A high-profile Spanish-language news website with 15 million visits and 58 million page views per month became the target of a devastating DDoS distributed denial of service attack. Some DDoS attackers in Russia had noticed the site and began sending extortion e-mails and making threatening comments on the website's blogs two months prior to launching a denial of service attack. They demanded "150 bitcoins" or the equivalent of US$2,500 or else they would attempt to bring down the website with a DDoS attack. Management did not respond to these threats in line with company policy and furthermore, the website's hosting company would provide DoS and DDoS mitigation services in the event of any attack.

> Company under a DDoS attack

A popular global Spanish-language news site

> Type of DDoS attack

High bandwidth Layer 7 attack

> Prolexic attack mitigation strategy

Routing the client's traffic through Prolexic's global scrubbing centers

> Time to DDoS mitigation

Immediate, as soon as traffic reached Prolexic's global scrubbing centers

One Sunday afternoon, a journalist informed the president of the news outlet that the site was down. "Usually when the site is down it is a minor thing and our hosting company takes care of it," says the co-founder and president. "At first, the hosting company thought it was a faulty router, but later they realized it was a DDoS attack. Unfortunately, the attack was so large that their DDoS mitigation equipment couldn't stop it. There was nothing they could do."

The president asked the technicians at the hosting company to recommend some solutions for mitigating the distributed denial of service DDoS attack. They told her to buy some time and get the site back up for a few days by changing site IP addresses. "Someone at the hosting company also told me to just let the attack run its course and take a week off and go on vacation," she says. "Obviously, that was not an option. We were already offline for eight hours and could not fulfill our live coverage of elections in Colombia, which was a significant news story at the time. Finally, another person at the hosting company said that we should contact a company that specializes in DDoS mitigation and they recommended Prolexic."

Prolexic's DDoS mitigation strategy

Prolexic technicians quickly determined that the Spanish-language news site was experiencing a Layer 7 DDoS attack of 30 Gbps. They assisted the site's IT staff in changing its DNS name servers to route all site traffic to servers in Prolexic's global scrubbing centers, stopping any malicious traffic from reaching the news site. Once the site traffic was flowing through Prolexic's scrubbing centers, it took about an hour to route the DNS changes to Prolexic.

The DDoS attackers abandoned the attack as soon as they saw that the news site's traffic was being routed through Prolexic. According to Neal Quinn, Prolexic's chief operating officer, it is not uncommon for Prolexic to deter attacks.

PROLEXIC
DDoS Attacks End Here.

"Potential attackers can find out when traffic is routed through Prolexic and they typically move on to other easier targets," Quinn says. "Prolexic can also be viewed as an insurance policy against distributed denial of service attacks and prolonged downtime. When attacks happen, clients can draw upon Prolexic's mitigation services as needed to ensure 'business as usual' and guard against significant financial loss."

"It took me longer to fill out the contract forms, scan them, and e-mail them back to Prolexic than it took to get our server up and running again," the president of the news outlet says with a laugh. "It took almost no time. In about a half an hour, the DDoS attack was over."

The president says that she was surprised that the global news site was so vulnerable to a DDoS distributed denial of service attack and that the hosting company's DDoS mitigation solution could not mitigate it. Yet she is aware that DDoS attacks are happening more frequently.

"This is happening to other news websites," she says. "The editor of another site has complained that they have been attacked at least twice over the past six months. The Layer 7 attack is the kind that can really hurt your business and you're vulnerable all the time."

Staying protected with Prolexic

"The fact that we had Prolexic in front of us caused the attacker to turn away," the president says. "The fact is that anyone, from a 15-year-old to professionals, can easily plan and orchestrate a DDoS attack today. My advice would be to be prepared for attacks of the magnitude we experienced and call a professional DDoS mitigation firm like Prolexic to defend your site. We've heard sites that are known to be protected by Prolexic don't get attacked and we've seen proof of that."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

Prolexic Mitigates Layer 7 Attacks for Options Trading Firm and Delivers Immediate ROI

In May, two large U.S. online options trading firms received e-mails demanding nearly US$60,000 from anonymous DDoS attackers. If they didn't pay up, the attacks would continue, potentially costing the firms tens of thousands of dollars if their trading platforms became unavailable for an extended period. After reporting this threat to a government agency, the companies were referred to Prolexic.

Company A had a strong in-house technical team who had been able to fend off previous attacks and prevent its website from going offline – at least at first. "Our team was doing a pretty effective job and the attacks weren't affecting our business," says the company's chief technology officer (CTO). "But as the attacks continued, the attacker began to change vectors and signatures more frequently. To continue our defense, we saw that we would have to go deeper into our application stack to make coding changes and that posed a high risk to the stability of our site. Obviously, we didn't want to do that."

> Company under a DDoS attack

A leading online options trading firm in the U.S.

> Type of DDoS attack

Encrypted Layer 7 attacks from multiple geographic locations

> Prolexic attack mitigation strategy

Use Prolexic's proprietary tools and techniques to block on-going attacks

> Time to DDoS mitigation

One hour

Faced with an increasing number of more sophisticated attacks, both companies realized that they needed outside help. Company A selected Prolexic while Company B sought out DDoS mitigation services from a large Internet services company.

Prolexic DDoS mitigation experts were able to stop the latest attack within one hour as soon as Company A's network traffic starting flowing through Prolexic's globally distributed scrubbing centers. The company's website remained online and available to traders while Prolexic experts fought the attack behind the scenes. In contrast, it was a full 48 hours before the Internet services company was able to overcome the latest attack for Company B. As a result, its website was unavailable during that period – resulting in a damaged brand reputation and lost revenues.

Prolexic's DDoS mitigation strategy

It was immediately apparent to the Prolexic technicians that encrypted Layer 7 attacks were being used. Using proprietary tools and techniques, Prolexic was able to stop the latest attack in minutes, eliminating the risk of the attacker hacking into the company's primary trading platform, a scenario that would have been devastating for both the business and its customers.

PROLEXIC
DDoS Attacks End Here.

PROLEXIC
DDoS Attacks End Here.

While encrypted Layer 7 attacks pose a significant and growing threat to companies worldwide, they are no match for Prolexic. The company's proprietary tools enable technicians based at its Security Operations Center (SOC) to decrypt Layer 7 traffic "on the fly". As a result, the Prolexic team was able to identify the attacker's bot signatures, which originated primarily from locations in Asia and Eastern Europe. In addition, they were able to respond immediately to the attacker's changing tactics with real-time monitoring of Layer 7 traffic.

"Prolexic provided us with a complete list of the attacking IP addresses so that we could follow up with the FBI and try to catch the offenders," says the CTO. "Prolexic gave us a very complete report with a variety of graphics that helped us understand where the attack came from and how it was done."

Prolexic's report uncovered more than 65,500 IP addresses used in the attack. Prolexic was also able to pinpoint the geographic locations of the botnets, ranging in size from as few as 9 machines to 35,500. Other key data gathered by the Prolexic team included attack types (GET Flood and SSL GET Flood), bits per second, packets per second, and connections per second (as many as 16,000 per second throughout most of the attack).

The company's CTO was so impressed with Prolexic's expertise and responsiveness he called the other options trading firm that was still under attack – a competitor – and recommended they use Prolexic.

"It's not unusual to see attackers turn their attention and launch intensified attacks on other companies in the same industry once they see that their primary target's traffic is now routing through Prolexic," says Paul Sop, CTO at Prolexic. "Attackers know that we're on the front lines protecting our clients against even the largest and most complex Layer 7 attacks so they move to easier targets."

Staying protected with Prolexic

Online financial services companies in particular must ensure the stability of any or all of the websites under their domain – especially when the financial resources of its customers are at stake. Today, Prolexic's customer remains protected against Layer 7 DDoS attacks without having to make changes to its application and network infrastructure. In addition, the company will never have to wait 48 hours or longer for attack mitigation like its competitor did.

"What we've learned is that even if you have some DDoS mitigating skills in house, it's not worth the risk of making significant changes to your infrastructure to fend off Layer 7 attacks," says the CTO. "There's always the possibility of making an application change and taking down your site yourself. So from a quality assurance perspective, we know that bringing in a proven DDoS expert like Prolexic is our best defense against Layer 7 attacks."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

FOUNDATION Source®
Making More Foundations *Great* Foundations™

Prolexic Answers Late Night Weekend Call to Mitigate DDoS Attack for Foundation Source

It was supposed to be a restful weekend for Gerry Battista, vice president of Information Technology Operations, and his staff at Foundation Source, the nation's largest foundation management firm. On a Friday evening, the network monitoring system sent out an alarm. Pages wouldn't load completely at www.foundationsource.com and the company's clients could not log in to their accounts to make gifts and grants.

"We checked our firewall and saw that there were 6,000 to 7,000 active connections going through it, whereas we usually have an average of 600 connections max when all of our clients are on the site," Battista says. "So we knew that we were under some kind of automated attack."

> Company under a DDoS attack
Foundation Source, the nation's largest foundation management firm

> Type of DDoS attack
A series of high requests-per-second GET Flood attacks

> Prolexic attack mitigation strategy
Prolexic's proprietary tools and real-time monitoring by Prolexic technicians

> Time to DDoS mitigation
Within hours after engaging Prolexic

After further investigation, Battista's IT team confirmed that the site was under a DDoS attack, so they tried to block the attack using their firewall. They also went through a very tedious process of identifying the IP addresses that were making the connections and blocking them one by one. They also tried blocking the IP addresses outside of the U.S., but these measures worked for only a short time. The attack stopped completely a few times during the weekend, but then reoccurred three times stronger than before. At that point, it was evident to Battista that the company's firewall just could not handle the deluge of malicious traffic. The company's ISP was unable to help because it couldn't weed out the malicious traffic without affecting other clients. Battista and his staff began an online search to find a DDoS mitigation vendor – around 9 p.m. on Sunday.

"There are many providers out there who will host your applications in the cloud to provide DDoS mitigation services, but there are very few who will do it while your site is under a DDoS attack," Battista says. "After narrowing down our short list to Prolexic and another provider, we chose Prolexic. We saw that Prolexic had far more experience in successfully mitigating these kinds of attacks. Most of all, Prolexic was the only provider who actually called our operations manager back at 11 p.m. on Sunday night."

Prolexic's DDoS mitigation strategy

By noon on Monday, management at Foundation Source had signed the contract to give Prolexic the green light to start DDoS mitigation. Deployment of the Prolexic DDoS mitigation services required minimum involvement on the customer's part, with Battista's IT group only having to make minor changes to the client log-in URL and the URL used for administering client accounts.

PROLEXIC
DDoS Attacks End Here.

PROLEXIC
DDoS Attacks End Here.

As this was an emergency situation and new client for Prolexic, technicians did not have the luxury of profiling and identifying typical site traffic for www.foundationsource.com. Despite this hurdle, Prolexic's Security Operations Center staff were still able to quickly determine that the site was being attacked by a strong and widely distributed GET Flood, develop blocking signatures, and mitigate the attack in minutes as soon as traffic starting flowing through Prolexic's scrubbing centers.

Prolexic's mitigation technicians provided Battista's IT group with several IP addresses to which they would direct the site's DNS. The IT group reconfigured the firewall to allow only Prolexic IP addresses to come through. Prolexic's technicians also monitored the attack traffic 24/7 and immediately countered any changes that the live attacker would make in the attack signature, size, and complexity – something that automated mitigation tools alone cannot do. By 9:30 p.m. on Monday night, the DNS had been fully propagated and the Foundation Source website was reopened to its clients and the public.

Battista was very happy with the responsiveness of the Prolexic team, as well as the flexibility of the terms of the contract. "The other company on our short list had a more attractive price upfront, but there would be significant costs if we wanted to stay on the service for a set amount of days after the attack," Battista says. "That would have cost us thousands of dollars per day. Prolexic offered us a better deal all around."

Staying protected with Prolexic

Battista notes that the company was fortunate that the DDoS attack occurred on a weekend, when client traffic to the site is less than during the business week. "Our business week was not impacted by the attack and we had plenty of time to try to mitigate the issues," he says. "We also had a workaround plan in place, so our offices could still administer client accounts while we kept the bad traffic blocked. An attack during the week would have been a different story, because having the site inaccessible would have damaged our client relationships."

Foundation Source's relationship with Prolexic is very good, according to Battista. "Everything was top notch with Prolexic," he says. "Their people were very responsive and everyone was kept in the loop throughout the mitigation process. Prolexic's track record as an expert in DDoS mitigation was clearly evident."

Today Foundation Source continues its mission of administering gifts, donations, and grants with DDoS protection from Prolexic. Staying protected is critical to ensuring that the website will be accessible to its foundation clients who must meet annual regulations for dispersing funds.

"To this day, we have no idea why our website was attacked," Battista says. "We had never been attacked before, but it can happen to anyone."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.060913

Prolexic Mitigates Anonymous Mexico DDoS Attack Against Junta Central Electoral

On March 29, 2012 the hacktivist group Anonymous Dominicana threatened Junta Central Electoral (JCE) that it would launch Operation 20 de Mayo (OP20M). The intent of this politically motivated Distributed Denial of Service (DDoS) attack against JCE's website was to disrupt the country's election process by casting doubt on the validity of results in the coming May 20, 2012 national presidential elections. As the central electoral board of the Dominican Republic, JCE is commissioned with processing, recording, and reporting election results securely and accurately.

Anonymous Dominicana announced its DDoS threat to the national press and to the Dominican Republic's two major political parties involved in the election by publishing its intent on a blog and through social media outlets. As a result, the eyes of the nation were on JCE to see how the board would respond to protect the integrity of its election results.

> Company under a DDoS attack

Junta Central Electoral (JCE), the central electoral board of the Dominican Republic

> Type of DDoS attack

Layer 3 and Layer 7 DDoS denial of service attacks

> Prolexic attack mitigation strategy

PLXproxy mitigation service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

"If our election data did not match that of the two political parties, which also track results, then the people of the Dominican Republic would deem the election invalid and demand a new election," says Daniel Joseph, website administrator for the Junta Central Electoral. "If we allowed our elections to be manipulated by a DDoS attack, the credibility of JCE, the political parties, and our nation would be severely impacted."

Shortly after Anonymous Dominicana's announcement of a denial of service attack and just a few weeks before the elections, the Dominican Republic police arrested six members of the hacktivist group. This action only heightened the hacktivists' zeal in publicly planning the denial of service DDoS attack.

Joseph knew that JCE needed network protection against DoS and DDoS attacks, so he took pre-emptive measures and immediately alerted JCE's President Roberto Rosario and Chief Security Officer Luis Leger. With less than two weeks before the May 20 election, Joseph contacted Prolexic for DDoS mitigation services. "When Election Day came and Anonymous launched a massive DDoS attack as promised, JCE was prepared with Prolexic," Joseph says.

Prolexic's DDoS mitigation strategy

While Anonymous Dominicana had threatened JCE publicly, it was Anonymous Mexico that launched a DDoS denial of service attack against JCE's website on Election Day, Sunday, May 20 starting at 2:49 PM EST. However, Prolexic's Security Operations Center (SOC) engineers were already providing DDoS monitoring services for traffic going to the JCE website. At 2:45 PM EST they noticed network abnormalities indicating a DDoS attack and notified JCE

PROLEXIC
DDoS Attacks End Here.

immediately via e-mail and phone. They rapidly investigated and noticed a high amount of UDP Flood and UDP Fragment Flood traffic targeting JCE's virtual IP addresses. Prolexic's engineers immediately created DDoS mitigation filters for these volumetric Layer 3 attacks in just a few minutes. Because all traffic flowing to the JCE site was routed and filtered through Prolexic's scrubbing centers, malicious DDoS traffic from the hacktivist attack was removed while clean traffic from legitimate users was sent on to JCE.

Anonymous Mexico wasn't going to give up easily, however. The hacktivists changed tactics. Instead of continuing to use Layer 3 attacks to "flood" and overwhelm network devices with excessive bandwidth, they launched a more sophisticated Layer 7 GET Flood attack, a denial of service attack that targeted the application layer of JCE's network and sought to overwhelm JCE's web server directly. Prolexic's engineers remained engaged and were able to write mitigation rules on the fly to block the Layer 7 GET Flood. The attacks lasted until 8:00 AM Monday, May 21 when Anonymous Mexico finally abandoned its efforts.

"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."

Staying protected with Prolexic

Thanks to Prolexic's web server and network protection and JCE'S high level of security, the DDoS attackers were unable to complete their threat.

"Prolexic played a very important role in helping JCE keep its credibility during the May 20 elections," Joseph says. "We have a commitment to our citizens to ensure that our election results cannot be manipulated on our website. DDoS protection from Prolexic helps us keep that promise."

Today, JCE remains protected by Prolexic against denial of service DDoS attacks. Joseph notes that JCE has given the attack forensics gathered by Prolexic to Dominican Republic law enforcement to help apprehend other members of Anonymous involved in the Election Day DDoS attack.

"In addition to being an electoral board, JCE also is the registry for confidential identity information for our citizens," says Joseph. "Because we have Prolexic for DDoS protection, we no longer have to worry that our site, services, and information can be brought down by a DDoS attack."

JCE is led by its president, Doctor Roberto Rosario Marquez. He is also president of the Inter-American Union of Electoral Organizations.

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

WorldofWatches.com

Prolexic Mitigates DDoS Attacks Against worldofwatches.com

Swiss Watch International (SWI) is 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. It sells watches directly to customers through its own website at www.worldofwatches.com (WoW) as well as to other wholesalers and retailers worldwide.

According to SWI Chief Technology Officer Darin Grey, the WoW website has more than 33,000 unique visitors daily and often generates revenues in excess of US$100,000 each day. Not surprisingly, any period of downtime has the potential to significantly impact company revenues and brand reputation. Fortunately, despite the site's popularity, during the last four years, Distributed Denial of Service (DDoS) attacks had been few and far between. Attacks directed at the site were small and had been handled effectively using the company's firewall. All of this changed one Saturday evening in December.

> Company under a DDoS attack

Swiss Watch International, a designer, manufacturer and distributor of timepieces through www.worldofwatches.com and other sites

> Type of DDoS attack

Bandwidth flood

> Prolexic attack mitigation strategy

Proprietary tools and real-time monitoring by Prolexic's Security Operations Center

> Time to DDoS mitigation

Within minutes of traffic flowing through Prolexic's global network of scrubbing centers

At around 10 p.m., a 130 Mb bandwidth flood was directed at the WoW site, far exceeding network capacity. "The attack came in on a well-known gaming port with hundreds of thousands of connections," says Grey. "We were blocking them with our firewall, but it was still flooding our network. With the amount of traffic being pumped through at that time of night, no one at our hosting facility could help us out."

Grey believes the WoW site was targeted because it is a well-known e-Commerce site. Unfortunately, SWI had other sites running on the same network, including editorscloset.com and fractionprice.com, so this one attack brought down multiple websites for approximately 12 hours.

Prolexic's DDoS mitigation strategy

A number of business associates had mentioned Prolexic to Grey months before and he had kept the company's number for just such an emergency. Grey spoke with his CEO and they called Prolexic on Sunday morning. "The person we spoke to at Prolexic said they could mitigate the attack in minutes so we signed a contract. Prolexic gave us a virtual IP 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."

After the attack was over, SWI increased network capacity to avoid a similar scenario. However, one month later, the WoW site was attacked again, this time with an attack that was three times larger than the first.

PROLEXIC
DDoS Attacks End Here.

"We have a successful site and we don't want it to go down so that's why we keep Prolexic's service."

PROLEXIC
DDoS Attacks End Here.

"There are two types of DDoS attacks – those that follow the domain and those that follow the IP address," explains Grey. "The first attack followed the domain so rerouting it to Prolexic was effective. The second attack stayed with the IP address, so we discussed with Prolexic a number of mitigation options. The attack was hitting our hosting provider, but they could handle that amount of bandwidth on their network versus our rack. We ended up having our hosting provider set up a whitelist so the site could only receive (clean) traffic from Prolexic IP addresses."

This strategy worked once everything was put in place and the WoW site was back up quickly.

When it comes to effective mitigation, Grey believes that relying on an external provider is the best strategy.

"Some attacks overwhelm your bandwidth and some overwhelm your hardware," explains 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."

Staying protected with Prolexic

With Prolexic's on-demand mitigation services in place, Grey now has peace of mind that the WoW site is fully protected against future DDoS attacks.

"We have small attacks all the time, but nothing that our firewall and DDoS protection cannot handle," says Grey. "For the larger attacks we go to Prolexic. We have a successful site and we don't want it to go down so that's why we keep Prolexic's service."

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 says. "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."

Grey is complimentary about the service he has received to date. "Prolexic has done a great job," he says. "Having someone to call 24 hours a day that can shape your traffic if you are having issues is definitely a plus. Having someone you can go to with the knowledge of how to react to issues right away is a big advantage."

With Prolexic's cloud-based mitigation network standing between the WoW site 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 them," concludes Grey.

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113

Prolexic Scores Points with Content Rating Organization

From television shows and motion pictures to video games and websites, rating content is increasingly important – especially as it becomes easier for children and teens to access it. While one such rating organization could help protect children from viewing inappropriate content, it could not protect itself against a series of Distributed Denial of Service (DDoS) attacks. With no defense systems in place, the rating agency's website was taken offline for several days. Senior management called Prolexic for help.

"We took the emergency call and started to immediately reroute its website traffic through one of our scrubbing centers," says Dan Goetz, Prolexic's director of service delivery. "In just a few minutes the site was back up and clear of malicious traffic and senior management was so impressed that they signed on for a one year contract for our mitigation services."

> Company under a DDoS attack

A leading content rating organization

> Type of DDoS attack

Multiple attacks ranging from Layer 3 to Layer 7

> Prolexic attack mitigation strategy

Routed traffic through Prolexic's scrubbing centers as IP proxy "wall of defense"

> Time to DDoS mitigation

Several minutes

Prolexic used proprietary mitigation tools and real-time monitoring services to detect and block the attacker's changing signatures and bandwidth floods throughout the attack. Because Prolexic technicians had mitigated similar attacks before, they used familiar tactics to identify the attacker's patterns, determine what was new or different, and apply a new signature block in just a few minutes.

Despite being a very satisfied Prolexic customer, when its DDoS mitigation contract came up for renewal one year later, the rating agency decided not to renew. "Our site hadn't come under attack during the months that Prolexic was protecting it, so we believed that we had fallen off of the radar of the person or persons who had been attacking us," says a rating agency spokesperson. "We felt that we didn't need Prolexic's protection, but we were wrong."

All of the traffic coming into the rating agency's website had been routed to a private Prolexic IP address serving as a wall of defense against DDoS attacks. After the Prolexic contract ended, the website went back to its original public IP address – and it didn't take long for DDoS attackers to realize that the rating agency was no longer protected by Prolexic.

Within days of the Prolexic contract ending, the rating agency's website was under attack again – a SYN flood of such excessive bandwidth that it quickly consumed the site's resources. Having tried every mode of attack from Layer 3 to Layer 7, the attackers had scaled up the attack to 3.3 Gbps and 9 million packets per second. This brought down the site once again, compromising the rating agency's business continuity.

" … as long as Prolexic is protecting us, we know our site is safe."

PROLEXIC
DDoS Attacks End Here.

Prolexic's DDoS mitigation strategy

"We realized that DDoS attacks were still a serious threat to our business, and that we needed a level of defense we could only get from Prolexic," says the spokesperson. "The Prolexic mitigation technicians explained to us that attackers are always watching and can tell when traffic is or is not routed through Prolexic. Attackers had left us alone for the previous year because they knew they didn't have the capacity to win against Prolexic's attack mitigation network, but as soon as we were unprotected, they attacked."

The rating agency engaged Prolexic once again. Fortunately, Prolexic still had the provisioning data so Prolexic engineers could just "flip the switch" and return the rating agency's website to its protected status. Prolexic mitigated the attack and had the site back online in just a few minutes.

Staying protected with Prolexic

Today, technicians in Prolexic's Security Operations Center provide 365-day monitoring to ensure business continuity for the website. "We'll be staying with Prolexic," says the spokesperson. "We've learned the hard way that our site is always likely to be on some attacker's radar. But as long as Prolexic is protecting us, we know our site is safe."

"The moral of this story is that companies and organizations of any size and in any industry can be the target of a devastating DDoS attack and there is often no rhyme or reason why the attackers strike," Goetz says. "This situation was not unusual. Attackers can tell when a site's traffic is routed through Prolexic, so they leave that one alone until they see that our contract hasn't been renewed. It's a harsh reality, but that's the kind of people we are dealing with."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061013

Online Gaming Site Plays On with Prolexic DDoS Denial of Service Mitigation

A popular Asian gaming website became the target of DDoS attacks. Having suffered increasingly disruptive DDoS denial of service attacks every two to three months, it was clear that the availability of its custom application was becoming increasingly compromised. Currently, the site is one of the most popular gaming communities and has millions of registered users from 153 different countries. To protect its business and maintain a high level of service and availability for its worldwide customer base, the company's directors decided to search for a proven DoS and DDoS mitigation service.

> Company under a DDoS attack

One of the world's most popular gaming communities

> Type of DDoS attack

SYN flood of approximately 4 Gbps on a 1 Gbps link

> Prolexic attack mitigation strategy

Proprietary mitigation tools, real-time monitoring, and advanced scrubbing centers

> Time to DDoS mitigation

Within minutes

While the gaming site had experienced several DDoS attacks, it had always bounced back, even though some were quite large. Initially, it dealt with the denial of service DDoS attacks in-house by installing built-in scripts that checked high request rates and blocked offending IP addresses. Using this DDoS protection approach, the company was able to minimize the impact of DoS and DDoS attacks, which consumed system resources rather than bandwidth.

"Any business using the Internet to operate has to accept that it is vulnerable to a denial of service attack, so we were not surprised to be targeted and decided to tackle it when we could and ride it out," says a spokesperson for the company. "As the DDoS attacks grew larger and more frequent it stopped customers from accessing our gaming platform so we could no longer ignore the attacks."

In simple terms, the denial of service DDoS attacks were flooding the online gaming site with more traffic than it could handle – up to 4 Gbps on a 1 Gbps link. This null routed the login servers, stopping a portion of the site's more than 500,000 concurrent users from accessing the online gaming platform for hours at a time. As the company's business revolves around an online gaming community that must log in to play games, the disruption from a denial of service attack was unsustainable. Online gaming is a very competitive market and disgruntled users would quickly find other more reliable sites if unavailability continued. It was critical for the company to get network protection from DoS and DDoS attacks.

"These DDoS attacks had a massive effect on our client base as gamers were unable to use our service until the problem was rectified," the spokesperson says. "The sites came back online after the attacks had been stopped, but we could not continue risking our customer base."

"We found that only Prolexic stood up to the level of protection that we needed and checked all the boxes."

PROLEXIC
DDoS Attacks End Here.

Prolexic's DDoS mitigation strategy

The online gaming company started its search for DDoS mitigation services and contacted many providers. It needed more than just basic denial of service mitigation however, because its flagship service is not web-based, but resides on custom application servers. Furthermore, the company has a number of servers colocated in SoftLayer data centers and it was not an option to move those servers to another Internet Service Provider or data center.

"Some providers had limitations on the level of bursts they could handle – some were limited to about 3-5 Gbps DDoS attacks," the spokesperson says. "Others could only protect our websites, not our servers. Finally, we needed a partner that could provide the service without any major changes on our side. We found that only Prolexic stood up to the level of protection that we needed and checked all the boxes."

Once engaged, Prolexic's DDoS mitigation technicians drew upon their vast experience in DDoS mitigation techniques to identify the attacker's bot signatures, which originated in Eastern Europe. After routing traffic through Prolexic's distributed global network of scrubbing centers – and monitoring the attacker's every move in real time – Prolexic was able to stop the DDoS attack and bring the gaming site back online almost instantly.

In addition, by tracing IP addresses, Prolexic technicians were able to pinpoint the geographic locations of the botnets used in the distributed denial of service DDoS attack, and eventually identify the attackers – "kids" in Eastern Europe who had exchanged e-mails with staff at the company.

Staying protected with Prolexic

Since engaging Prolexic DDoS mitigation services for network protection, the online gaming site has been attacked with SYN floods as large as 9 Gbps, but Prolexic has successfully countered every one. Prolexic's DDoS mitigation service enables the company to instantly activate high-level DoS and DDoS protection from the largest and most complex DDoS attacks around the clock. By working with the hosting company, SoftLayer, Prolexic has put simple processes in place that enable the gaming company to route traffic through the globally distributed Prolexic DDoS mitigation network on demand.

This online gaming site is one of a number of Asian businesses that have selected Prolexic as their preferred DDoS monitoring and mitigation partner. In fact, Asia has been one of the fastest growing markets for Prolexic over the last three years with clients from China, Hong Kong, Philippines, Malaysia, Singapore and Cambodia increasingly being affected by DoS and DDoS attacks.

"Unfortunately cyber attacks like DDoS are an increasing threat to both public and private enterprises," says Neal Quinn, chief operating officer at Prolexic. "As DDoS denial of service attacks can be used to damage competitors, exact revenge on ex-employers or make political statements, in additional to traditional cyber scams like DDoS extortion, more enterprises need to include DDoS detection, DDoS monitoring and mitigation in their business continuity and risk strategy."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.060913

KrebsonSecurity

Prolexic Defends Krebs on Security Blog Against Dirt Jumper/Pandora DDoS Attacks

Krebs on Security (www.krebsonsecurity.com), authored by Brian Krebs, an independent investigative reporter, is a popular blog on emerging cyber crime trends, DoS and DDoS toolkits, and the perpetrators themselves. On average, the blog receives 10,000 views or more per day. Not surprisingly, the site has been the target of DDoS attacks and other cyber threats. However, during the last week of July 2012, the denial of service DDoS attackers took a new, more pernicious approach using Pandora, a variation of the Dirt Jumper DDoS toolkit.

On the morning of July 27, Krebs was in Las Vegas for the Black Hat convention and was minutes away from a live interview with one of the conference leaders when availability of krebsonsecurity.com became spotty and eventually went down. Krebs contacted his hosting provider, who delivered the bad news that junk traffic was being pushed to the site by a DNS amplification DDoS denial of service attack.

> Company under a DDoS attack

Krebsonsecurity.com, a popular blog that unveils the latest types of cyber threats and their perpetrators

> Type of DDoS attack

DNS amplification attack and Layer 7 flood using Dirt Jumper/Pandora

> Prolexic attack mitigation strategy

PLXproxy mitigation service

> Time to DDoS mitigation

Within minutes under Prolexic's industry leading service level agreement

"My hosting provider said, 'Brian, the DNS attack is really starting to affect our other customers.' Thankfully, even as I was conducting the interview, they were able to help me transition the site's DNS to Prolexic's and help mitigate that portion of the attack," Krebs said.

Ultimately, a series of four escalating denial of service attacks were launched against the site. Krebs speculates that the DDoS attacks came in response to a story he had posted several hours before. The site was down for approximately five hours, during which time visitors could not access the site or read content via RSS feeds.

"I make a career out of making people upset with the stories I post, because I tend to expose the things that the bad guys are doing – and who they are. They don't really like that," Krebs says. "The story I had posted, right before the attack started, was about a service for mass registering of domain names for malware and spam. They didn't send me a note or threat, so it's hard to say where the attack really originated."

Krebs has a good relationship with the head of his hosting provider, so Krebs asked for a recommendation. "I respect this person and know that he has experience with DDoS mitigation providers, and I wanted to make his life easier, too," Krebs says. "I knew that Prolexic has a good reputation and thought it would be a good fit. When I asked my hosting provider which vendor he would feel most comfortable with, he said Prolexic. That was enough for me."

Prolexic's DDoS mitigation strategy

Prolexic DDoS mitigation experts quickly identified that the malicious traffic was part of a DNS amplification attack combined with changing attack vectors

PROLEXIC
DDoS Attacks End Here.

launched via the Pandora toolkit. Using more than 20 mitigation tools, many proprietary, Prolexic's engineers were able to write new countermeasures and mitigate each changing signature on the fly. Consequently, availability of Krebs' blog site was restored in minutes and remained protected as all traffic from krebsonsecurity.com was routed through Prolexic's scrubbing centers.

Prolexic's analysis indicated a series of increasingly strong DDoS denial of service attacks over four days as characterized by the following peaks in activity:

- July 24 – GET Flood that peaked at 5.00 Mbps (bits per second), 2.50 Kpps (packets per second), and 35.00 Kcon (connections per second)
- July 25 – GET Flood and POST Flood 105.00 Kbps (peak bits per second), 6.00 Kpps (packets per second), and 25.00 Kcon (connections per second)
- July 28 – UDP Flood and UDP Fragment, 552.00 Mbps (peak bits per second), 121.00 Kpps (peak packets per second)
- July 29 – GET Flood, POST Flood, 275.00 Kbps (peak bits per second), 0.10 Kpps (peak packets per second), 0.15 Kcon (peak connections per second)

Prolexic's DDoS mitigation engineers also determined that all of the various traffic signatures for the GET and POST floods seemed to be created by the same individual using Pandora, a Dirt Jumper DDoS toolkit, which is sold in the cyber underground. Prolexic found that more than 1,500 Pandora-infected bots were used in the denial of service DDoS attack on the site.

"The traffic signatures strongly suggested the involvement of two Dirt Jumper progeny: Di-BoTNet and Pandora," Krebs wrote on his blog. "Pandora is the latest in the Dirt Jumper family, and features four different attack methods. According to Prolexic, one of the methods used against KrebsOnSecurity.com was Attack Type 4, a.k.a. Max Flood; this method carries a fairly unique signature of issuing POST requests against a server that are more than 1 million bytes in length."

Staying protected with Prolexic

With Prolexic protection, the Krebs on Security site will remain protected against all DDoS denial of service threats, including DDoS attacks launched via the Dirt Jumper toolkit. Dirt Jumper is a high-risk DDoS toolkit that can be used to launch application layer attacks on websites. This prepackaged toolkit 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. Prolexic has 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.

"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."

Prolexic informed Krebs that the DDoS attackers compromised open recursive (unmanaged) DNS servers to create extremely large floods of traffic in the DNS amplification attack. These types of unmanaged servers are favorite targets for a denial of service attack because they are configured to accept queries sent from anywhere on the Internet, including forged or "spoofed" queries that are characteristic of DNS amplification attacks.

"In the case of DNS DDoS attacks, I think that ISPs should avoid the use of open recursive servers that get abused over and over again to launch these attacks," Krebs says. "The problem will never go away completely, but we need to change the status quo on protecting servers against DDoS attacks."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

Prolexic Shines in Mitigating Layer 7 DDoS Attack for Leading American Jewelry Designer

When the website of a premier American jewelry designer was taken down due to a DDoS attack, the company's chief security officer (CSO) called the site's hosting service. That firm had mitigated an attack on the site several days before, so the CSO expected a similar response. Unfortunately, this time was different.

After nearly three days of downtime – and millions of dollars in lost revenue – the hosting service still had not been able to mitigate the latest attack. Scrambling for a solution, the hosting provider recommended the one company that could definitely solve the problem – Prolexic.

> Company under a DDoS attack

A premier American jewelry designer whose web presence offers unique collections of jewelry, watches, fine gifts, and fragrances

> Type of DDoS attack

A dual vector encrypted/non-encrypted Layer 7 attack from multiple geographic locations

> Prolexic attack mitigation strategy

Use Prolexic's proprietary tools and leverage the experience of its security experts to counter the changing tactics employed by a live attacker in real time

> Time to DDoS mitigation

Less than one hour after the initial emergency call to Prolexic

"Understandably, the hosting company simply didn't have the capabilities needed to handle large, dual vector Layer 7 attacks because DDoS is not their primary business," says Paul Sop, chief technology officer at Prolexic. "In order to keep the network up for thousands of other customers, hosting companies usually just route the traffic of the business under attack into a 'black hole,' making the website unavailable. Prolexic specializes in DDoS mitigation, so we can get sites back up in minutes even during the largest and most complex attacks."

The jewelry company's senior management immediately gathered to place an emergency conference call to Prolexic. "This was a critical situation that was costing us millions every day," says the company's CSO. "We thought we were protected against all DDoS attacks, but we found out – to our cost – that wasn't the case. After a few minutes talking with Prolexic, we were convinced that they could help us. The situation was so grave that our CFO gave immediate verbal approval to Prolexic to start their mitigation services."

Prolexic was able to capture and route the Layer 7 DDoS traffic through its scrubbing centers just minutes after the initial emergency call. Consequently, the jewelry designer's website was back online in less than an hour.

Prolexic's DDoS mitigation strategy

Prolexic's technical experts determined that this was a dual vector Layer 7 attack. One vector was a normal Layer 7 attack while the other was an encrypted layer. "We put the site's encryption certificates on our systems in order to look at the encrypted traffic," Sop says. "Our proprietary tools allow us to decrypt traffic on the fly with the same strong capability and visibility that we have in regular Layer 7 attacks. We saw that the majority of the signatures came from Latin America, but overall the attack was evenly dispersed geographically."

PROLEXIC
DDoS Attacks End Here.

PROLEXIC
DDoS Attacks End Here.

Surprisingly, the DDoS attackers continued to target the jewelry designer's site even after Prolexic began mitigating the attack. Even though the attackers changed the encryption signature 10 times, they were no match for Prolexic's real-time traffic monitoring and mitigation services. Prolexic stayed in touch with the jeweler's IT staff to ensure that they could identify what was normal traffic and what wasn't, which is especially important when fighting Layer 7 attacks.

"We're constantly checking to see if this URL is valid, are these protocols valid – what is normal?" Sop says. "What we do requires a constant stream of communication with the customer. In this case, the attack jumped around in terms of size and intensity, sometimes going up to 150,000 connections, which is very large. We stay on top of things with real-time monitoring, because automated tools just can't catch and identify all of the changes."

Despite the size and complexity of the attack, Prolexic technicians suspected that the attacker was an amateur. That theory proved to be correct. As Prolexic mitigated the attack, the jewelry company's CEO got a phone call from the attacker who was furious because the CEO had not responded to e-mails demanding payment or else the website would be brought down. The e-mails had been caught by a spam filter, so the CEO had never seen them. The attacker gave no reason for targeting the jewelry designer.

"The moral of this story is that it's ridiculously easy to launch Layer 7 attacks," Sop says. "There is no rhyme or reason as to why people do it, or to the sophistication or stupidity of the attacker. Any website could be next."

A brilliant future with Prolexic

The jewelry company officially contracted Prolexic to provide DDoS mitigation services after seeing how quickly and effectively Prolexic responded to their emergency situation. "Even though this is a premium service, we have seen the value firsthand," says the CSO.

The jewelry designer's site has not been attacked since engaging Prolexic, but that doesn't mean someone won't try. "We're confident that we're protected with Prolexic," says the CSO. "We were baffled as to why anyone would want to bring down our website, but this experience has taught us that sometimes it just doesn't make any sense. Anyone can be attacked, and even the most inexperienced hacker can cause millions of dollars in damage to a large company – that's why you need companies like Prolexic guarding the gate."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

Prolexic Fights Off Massive Layer 7 DDoS Attack for Global Fragrance and Beauty Products Retailer

In June, a DDoS attack was launched on the complex, image-heavy website of a leading global retailer of women's fragrances and beauty products – a company that also reported more than US$350 million in online sales. On the day of the attack, customers who attempted to visit the popular, trendy site saw only a blank page that would try to load over and over again for a long period of time. Finally an error message would appear instead of the expected colorful array of lipstick, eye shadow, and blush. In addition to losing the potential revenue from those site visitors – some industry analysts estimate that 24 hours of downtime for a major e-Commerce site can reach US$30 million – the online retailer also risked losing brand equity in a competitive business. Customers spread the news on Twitter that the website was out of service, and rumors started that perhaps the company itself might be out of business.

> Company under a DDoS attack

Popular online retailer of many unique brands of fragrances, makeup, and other beauty and bath product lines

> Type of DDoS attack

A stealth, randomized Layer 7 attack disguised as a bandwidth attack

> Prolexic attack mitigation strategy

Use proprietary tools for Layer 7 attack mitigation and the expertise of Prolexic's operations team to monitor traffic patterns and thwart the attacker's countermoves in real time

> Time to DDoS mitigation

The retailer's website was back online within 5 minutes from when Prolexic service was engaged and remained online despite frequent changes to the attack

The retailer fought back at first using the resources of two major service providers that provided a basic level of DDoS mitigation. However, the nature of this Layer 7 DDoS attack was too complex and its volume was too large for those companies to mitigate. The retailer called Prolexic on a Thursday, but had to wait until Monday to get approval to proceed from its corporate management and legal teams. As a result, the retailer's site was offline for a damaging 72 hours.

Prolexic wasn't surprised to get that call. Several days before the retailer was attacked, Prolexic had been contacted by two other companies in the fragrance and beauty industry whose sites were under a similar Layer 7 attack. Both companies immediately engaged Prolexic, whose operations engineers were able to mitigate the attacks in about 5 minutes. As a result, their sites were back online and ready to process weekend sales.

Prolexic's DDoS mitigation strategy

After the beauty product retailer received management's approval to engage Prolexic on Monday, the Prolexic team was ready to mitigate almost immediately. Within five minutes of the network traffic being routed through the Prolexic scrubbing centers, the retailer's site was back online and ready for business.

"These attacks were of a nature we hadn't seen before," says Paul Sop, chief technology officer at Prolexic. "Years ago, we identified an emerging trend where complex Layer 7 attacks were increasing and proactively developed monitoring, alerting, and mitigation tools to address them before they became mainstream. We were ready to block this attack quickly and were able to easily and rapidly bring this retailer's site back online."

PROLEXIC
DDoS Attacks End Here.

"This was one of the larger Layer 7 attacks that we had seen at that point in time."

PROLEXIC
DDoS Attacks End Here.

"The attackers used a DDoS method that made it look like it was only an attack on bandwidth," Sop continues. "But since we had just fought off a similar combination Layer 7 attack just days earlier for the other fragrance companies, our solution for this client was really plug and play. We saw that the attacker was using the same botnet, so we already had the signatures in place to fight the attack."

Using proprietary tools and drawing upon the team's previous experience, Prolexic was quickly able to determine the attacker's strategy:

- Avoid the caching of the retailer's existing DDoS mitigation provider by targeting the back-end application server directly
- Each bot used a low-request-rate to avoid threshold mitigation, easily bypassing commonly used commercial off-the-shelf (COTS) hardware solutions designed to mitigate DDoS attacks
- Employ HTTPS attack components to avoid Intrusion Prevention System (IPS) and most mitigation systems
- Construct queries which peg CPU and overload back-end databases

"This was one of the larger Layer 7 attacks that we had seen at that point in time, and one that reflected a trend we had been watching," Sop says.

"In this case, the attack started with a massive Layer 4 attack with bandwidth to distract from the more insidious Layer 7 attack that is at a lower bandwidth level and harder to detect. That's where Prolexic's experience came in. We knew to expect this combination attack and we looked for it. A DDoS service provider with less experience might take things at face value and miss the real threat."

Prolexic also drew upon its team's expertise in responding to the attacker's countermoves on-the-fly in real time in randomized attacks. When fighting Layer 7 attacks, Prolexic's team knows that there is usually a human attacker at the other end pulling the strings.

"We often see the attacker making offensive moves, and that happened with this cosmetic retail client," Sop says. "Our operations personnel constantly monitored the traffic, noticed any changes, did the pattern recognition, figured out what was new and how to block it. We then applied a new signature block all in the course of a few minutes. We've had to do that as many as 40 times in some cases. There is no automated device on the planet that can react in real time like our operations people can."

Putting on a fresh, confident face with Prolexic

Since becoming a client, the beauty product retailer has relied on Prolexic to protect its e-Commerce website from future DDoS attacks. Today, just as its customers face the world more confidently using the beauty products it sells, this retailer operates online with confidence, knowing that Prolexic will respond quickly with a proven DDoS solution to keep the site running smoothly should another attack occur. But additional attacks aren't as likely since potential attackers know that this website is protected by Prolexic. But that doesn't mean they won't try.

"Attackers know when a website's traffic terminates with Prolexic, so it's not unusual for us to see our customers get attacked about 12 months after the contract is signed, because they want to see if we are still protecting the site," Sop says. "The following year, we had given this retail client an additional 30 days to negotiate a contract renewal. Attackers didn't know this and just 13 days after the supposed contract expiration, they launched an attack out of nowhere that was quadruple the size of the one the previous year. This time the attackers never had a chance to bring this site down for 72 hours again – not with Prolexic on the front lines."

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 www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

v.061113