# THE BATTLE AGAINST DDoS

## THEIR METHODS:

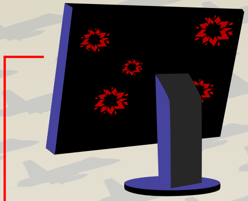
Commandeer networks of remotely controlled zombie or botnet (robot network) computers

Enlist millions of zombies to relentlessly attack at the same time, making them difficult to identify

Keep a low profile to stay well disguised

## THEIR MISSION:

Wreak havoc on businesses and individuals



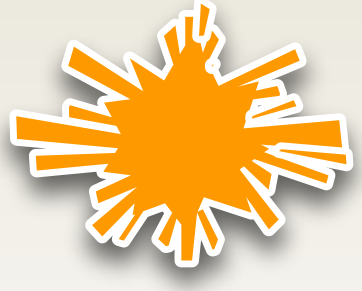
Make computer resources or entire networks unavailable for intended users

Continue to escalate attacks

"THIS JUST IN"

and create news headlines

## THE DAMAGES:



US$2.1 million

Estimated cost of 4 hours of website downtime*

US$27 million

Average financial damage for 24-hour outage*

US$17 million

2012 estimated cost per DDoS attack on a financial services company*

### Not to mention...

- Loss of customer satisfaction and brand reputation
- Increased security risk due to distraction
- Lower stock prices and investor confidence
- Lower Google search rankings

**GET PROTECTED WITH PROLEXIC!**

PROLEXIC

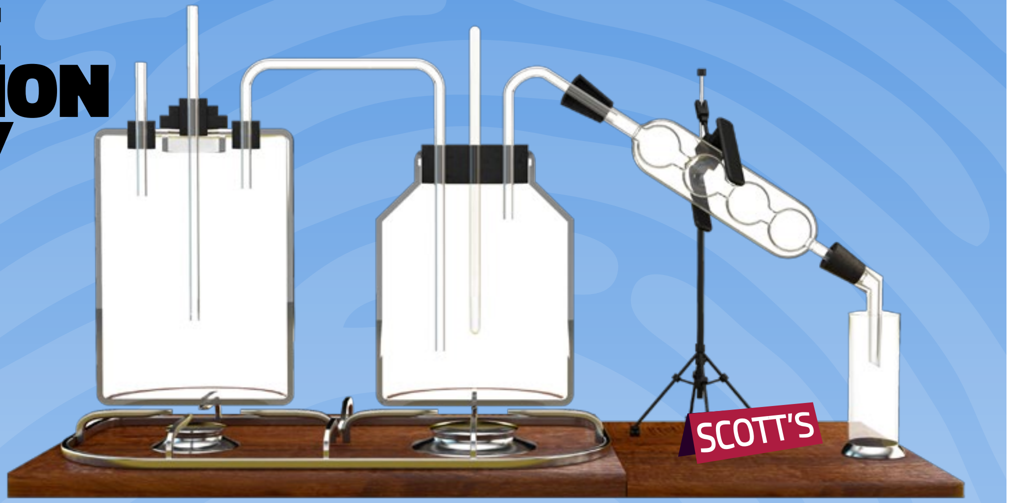
DDoS Attacks End Here.

**+1 (954) 620 6005**
www.prolexic.com

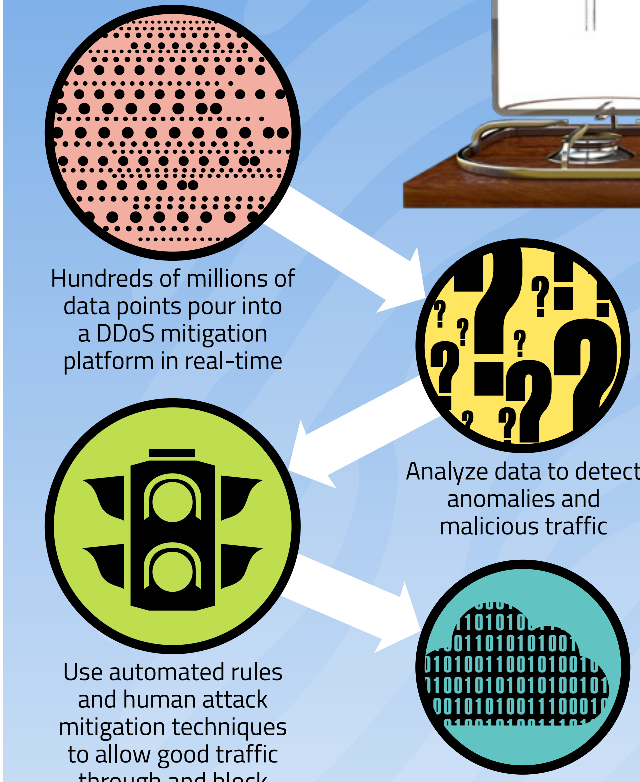
* Kindervag, John. "Develop a Two-Phased DDoS Mitigation Strategy." May 17, 2013. Forrester Research.

# FINGERPRINTING A DDoS ATTACK

## EFFECTIVE DISTILLATION IS THE KEY



### WHEN AN ATTACK TAKES PLACE:



Hundreds of millions of data points pour into a DDoS mitigation platform in real-time

Analyze data to detect anomalies and malicious traffic

Use automated rules and human attack mitigation techniques to allow good traffic through and block bad traffic

Store billions of traffic and attack data metrics in the cloud

**The Goal:**

- Make all incoming attack data useful to humans

**The Problem:**

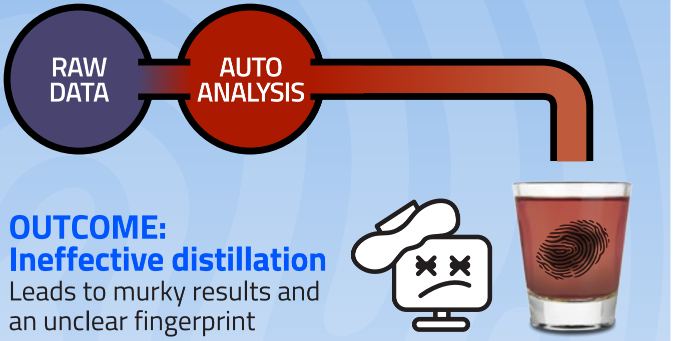
- There is a gap between what automated data analytics can do and what malicious attackers can do live behind their botnets
- Automatic decision making equipment is prone to false positives

**Conclusion:**

- That's why we need ***human*** DDoS mitigators

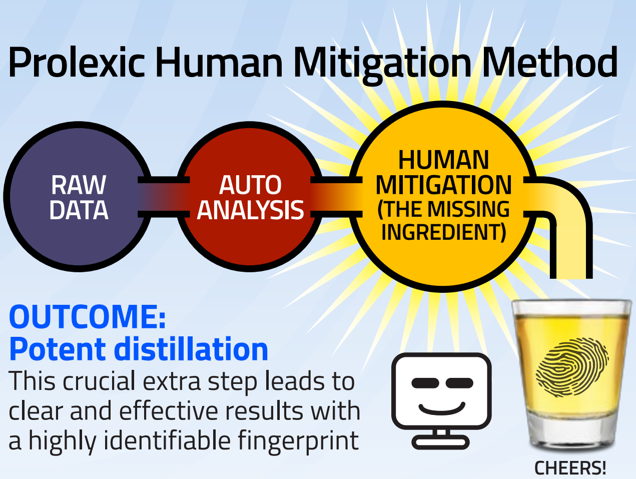
**COMPARE THESE 2 METHODS**

## Typical Automated Method



**OUTCOME:**
**Ineffective distillation**
Leads to murky results and an unclear fingerprint

## Prolexic Human Mitigation Method

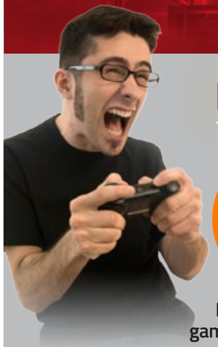


**OUTCOME:**
**Potent distillation**
This crucial extra step leads to clear and effective results with a highly identifiable fingerprint

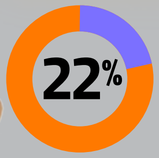
PROLEXIC
DDoS Attacks End Here.

+1 (954) 620 6005
www.prolexic.com

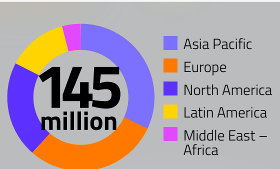
# Target acquired: Gaming website



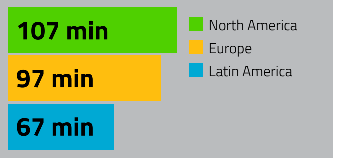
## By the numbers



Percentage of all gamers worldwide that are online each day[1]



Number of gamers from the top 5 continents that are online each day[1]



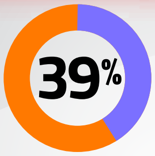
Average monthly minutes per gamer for top 3 continents[1]

Your gaming servers could be hijacked by malicious actors and used in DDoS attacks.

- Looking for poorly implemented security controls and configurations
- Harm gaming and non-gaming targets alike

**YOUR GAMING WEBSITE ALSO COULD BE TARGETED BY DDOS ATTACKERS. IF IT GOES DOWN, YOU WILL LOSE GAMERS, YOUR REPUTATION AND REVENUES.**

Number of dollars in worldwide revenues that will come from online games by 2017[2]



Percentage of console game revenue that will be via online distribution and online revenue source by 2017[3]

## Protect your site and your revenues

1. Apply patches and updates to your servers and applications so they cannot be used in DDoS attacks
2. Increase your level of DDoS protection - ISPs, DNS providers, Content Delivey Networks can only stop some attacks
3. Get Prolexic Protected against all attacks with an industry-leading time-to-mitigate Service Level Agreement

**1.954.620.6002**
www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

[1] Source: comScore MMX, Worldwide, April 2013, Age 15+, http://www.comscoredatamine.com/2013/06/asia-pacific-has-largest- daily-online-gaming-audience/
[2] Source: Online Game Market Forecasts, DFC Intelligence, 2012
[3] Source: Worldwide Market Forecasts for the Video Game and Interactive Entertainment Industry, DFC Intelligence 2012 http://www.forbes.com/sites/johngaudiosi/2012/07/18/new-reports-forecasts-global-video-game-industry-will-reach-82-billion-by-2017

PROLEXIC
DDoS Attacks End Here.

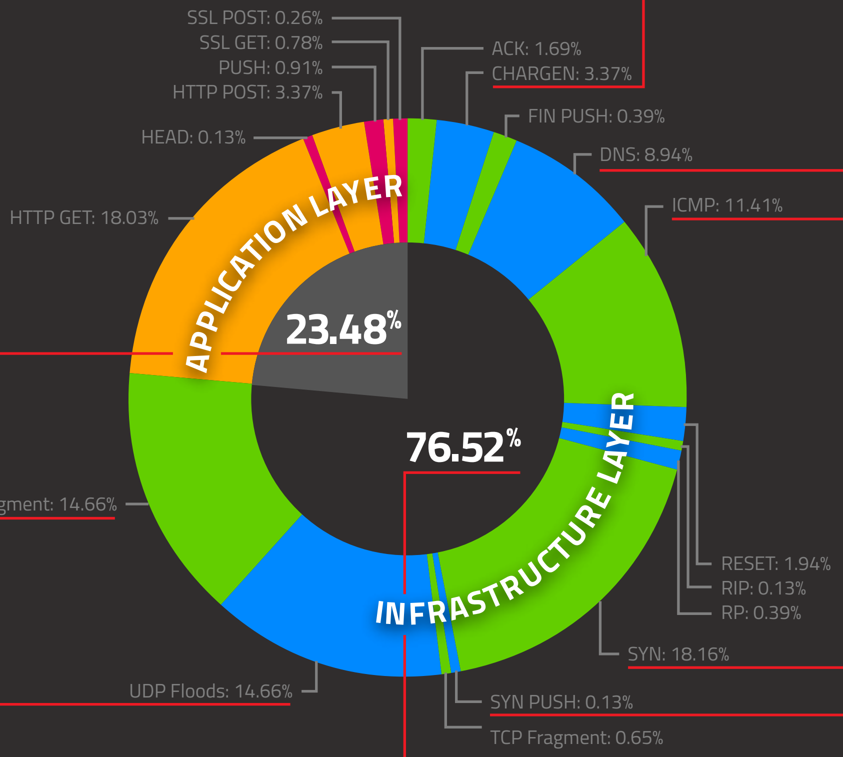
# Q3 2013 Global DDoS Attack Report

## DDoS perpetrators changed tactics to amplify attack sizes and hide identities

Use of the CHARGEN protocol increased 3.37% when compared to other infrastructure attack methods. Adoption of the UDP-based CHARGEN protocol has been rapid as it is widely available on the DDoS-as-a-Service market.

Application attacks declined slightly to 23.48%, down from 25.29% in Q2 2013. Compared to Q3 2012, application attacks have increased by almost 6% (from 17% to 23%).

8.9% of infrastructure attacks were based on the DNS attack protocol, a 4% increase compared to Q3 2012 (5%).



Traditional attack methods, such as ICMP floods, dropped this quarter. The movement away from ICMP floods toward reflected amplification attacks is due to a shift in attack offerings among DDoS-as-a-Service stressor services.

The UDP attack vector totaled 29.32% of all attacks – a 10% increase compared to the previous quarter, returning to levels seen in Q2 2012. A significant portion of UDP floods were reflected amplification attacks using DNS and CHARGEN.

Infrastructure attacks increased 2% compared to Q2 2013. Compared to Q3 2012, infrastructure attacks fell by almost 6% (81.40 to 76.52&)

At 18.16%, the percentage of SYN floods has decreased this quarter compared to Q2 2013 and Q3 2012, but SYN floods still remain the most popular of all infrastructure attacks, most likely due to the proliferation of easy-to-use stress-testing tools that are freely available.

## THE BOTTOM LINE:

There was a significant shift to reflection-based attack vectors in Q3 2013, rising 69% compared to the previous quarter, and 265% when compared to the same quarter a year ago.

www.prolexic.com

# DDoS Attacks & Defense

DDoS ATTACKS

## MOTIVATION

Hacktivism ▪ Extortion ▪ Retaliation By Competitors
Angry Employees or Customers ▪ Hacker Experiments

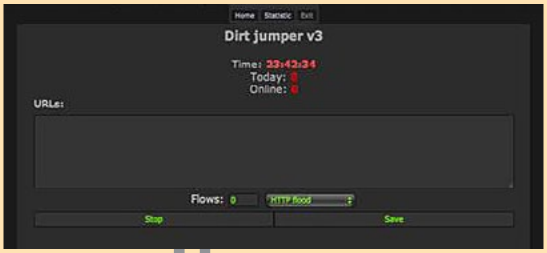
## IDENTIFY TARGET

Web Servers ▪ DNS Servers ▪ Email Servers
FTP Servers ▪ Network Devices

## INVESTIGATE TARGET

Footprint Network ▪ Port Scan

## LAUNCH DDoS ATTACK



Dirt jumper v3

Time: 23:42:34
Today: 0
Online: 0

URLs:

Flows: 0 HTTP flood

**Use tool to specify:**

- Target
- Port
- Attack Types (Layer 3, 4 & 7)
- Attack Vectors (DNS, UDP, SYN, etc.)
- Duration

DDoS DEFENSE

**No Protection, Appliance, CDN, Telco, ISP**

50 Gbps

- Attack too big
- Attack too complex

ERROR 404
File not found

The page might have been removed, or is temporanly unavailable

50 Gbps

Malicious Traffic

**Prolexic DDoS Protection**

- Monitoring/alerting
- 15-minute mitigation SLA
- 1.5 Tbps cloud platform
- 24/7 SOC

Clean Traffic

Clean Traffic

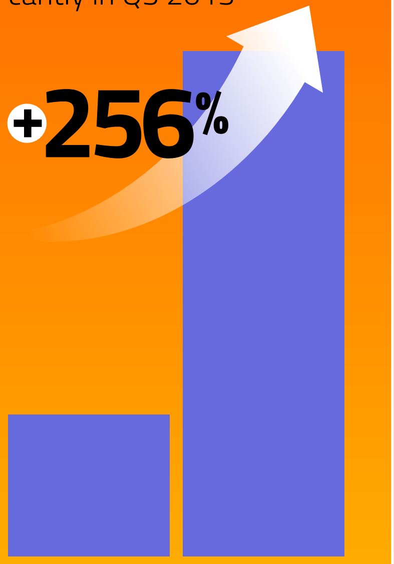
PROLEXIC
DDoS Attacks End Here.

www.prolexic.com

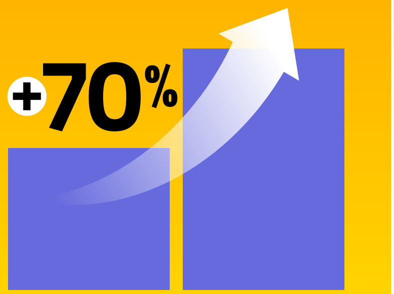
# THE Rise OF DrDoS ATTACKS

## An emerging DDoS threat

Distributed reflection denial of service (DrDoS) attacks increased significantly in Q3 2013

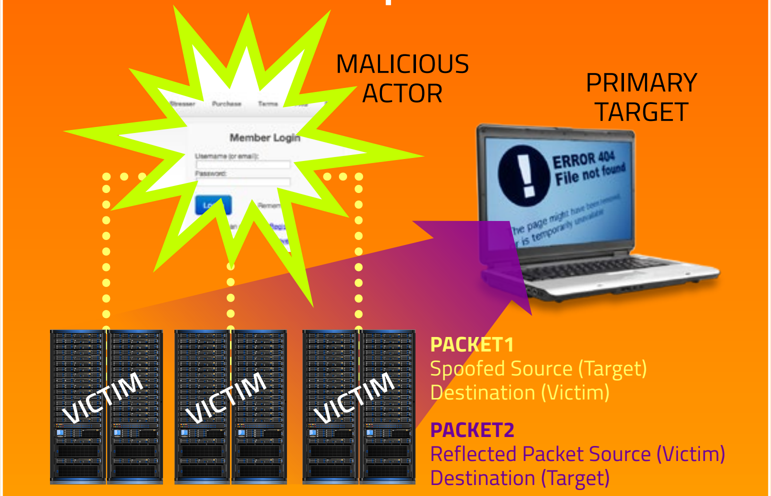


**Compared to Q3 2012**



**Compared to Q2 2013**

## DrDoS attacks explained



**PACKET1**
Spoofed Source (Target)
Destination (Victim)

**PACKET2**
Reflected Packet Source (Victim)
Destination (Target)

- Intermediary victim machines unwittingly participate in an attack against the perpetrator's target
- Requests to the intermediary victims are redirected (reflected) from the secondary victims to the primary target

## Why DrDoS usage is increasing

- Can obscure attack source (anonymity)
- Can hijack bandwidth of intermediary victims to multiply attack size (amplification)
- Increase in misconfigured servers worldwide
- Easier to obtain lists of misconfigured servers and IP addresses from underground Internet communities

## The industries at risk

DrDoS attacks are being seen in most industries:

## What you can do

✓ Turn off the CHARGEN service to stop this attack method

✓ Download the latest updates and patches for your servers

✓ Download Prolexic's ***Q3 2013 Quarterly Global DDoS Attack Report***

# LEARN MORE

To learn more about DrDoS attacks and read a detailed case study of this emerging threat, download a complimentary copy of Prolexic's Q3 2013 Quarterly Global DDoS Attack Report from ***www.prolexic.com/attackreports***.

**+1 (954) 620 6005**
www.prolexic.com

PROLEXIC
**DDoS Attacks End Here.**

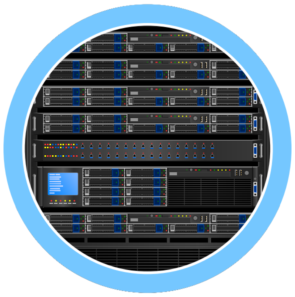
# Safeguarding e-Commerce Revenues from DDoS Attacks this Holiday Season

## 4 warning signs your website could be targeted

Others in your industry have been attacked. ***Pay attention!***

Hackers sometimes announce their targets on social media sites. ***Monitor!***

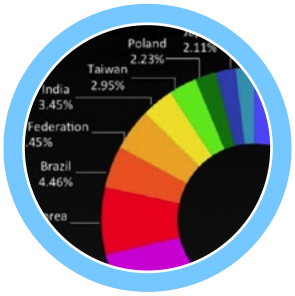
You receive an extortion or blackmail attempt. ***Don't ignore!***



Your network has experienced undiagnosed problems. ***Investigate!***

## 4 ways to ensure Q4 site availability

**Learn how different types of DDoS threats can affect your IT infrastructure.** Then select a DDoS mitigation service that will protect it.



**Keep up with trends in DDoS attack signatures and toolkits.** Prolexic has a wealth of information and threat reports at www.prolexic.com.

**Have a single source for DDoS mitigation services.** Multiple appliances and vendors add to complexity, downtime and costs.

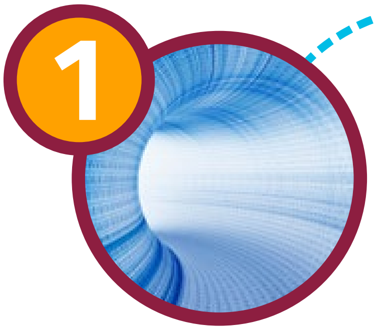
**Make DDoS part of your disaster recovery plan.** Choose team members, validate your plan, and organize information for easy, fast accessibility to eliminate panic.

**Follow these tips and you're likely to have a happy – and prosperous – online holiday shopping season.**

**+1 (954) 620 6005**
www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

# How to Select a DDoS Mitigation Provider

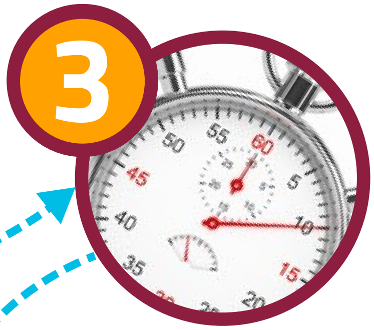


### Attack Bandwidth Capacity

Look for a provider with bandwidth dedicated to DDoS mitigation and enough capacity to support multiple attacks against multiple clients.

### Specialists and Generalists

Providers of "add on" DDoS mitigation services are adequate for small, simple attacks, but if doing business online is critical to day-to-day business operations, then a specialist provider is often the best, lowest risk choice.



### Responsiveness

Look for a documented time-to-mitigate service level agreement. Examine the fine print for how long it takes the provider to develop/release blocking signatures to stop DDoS attacks.

### Flat Rate Pricing

The safest, simplest option is to look for a provider that offers mitigation for a flat rate regardless of the number of attacks or bandwidth consumed.

### Direct Access

Look for a provider that offers direct, immediate access to the people fighting the DDoS attack on your behalf. Avoid providers that only offer a call center to contact.

### Mitigation Experience

Look for a provider that fights multiple attacks on a daily basis and ask for evidence of the attacks that have been mitigated and how they were stopped.

### Layer 7 Expertise

Look for a provider with a proven track record against stealth, sophisticated Layer 7 attacks that target applications. Be sure the provider has audited, documented key handling and management practices.

### Web Portal

Look for a provider that offers instant access to a secure online portal where data is refreshed frequently.

## Want more in-depth guidance?

Be sure you choose the right level of protection for your business by asking the right questions. For more in-depth and technical resources that can help in your evaluation process, go to prolexic.com/choose to download:

- IDC Analyst Connection: Distributed Denial of Service: What to Look for in a Provider
- White Paper: Twelve Questions to Ask a DDoS Mitigation Provider

**+1 (954) 620 6005**
www.prolexic.com

PROLEXIC
**DDoS Attacks End Here.**

# Monitor Manage Mitigate

## *What to look for in a DDoS mitigation provider portal*

### Accessibility

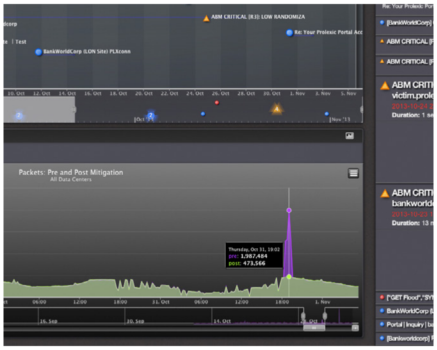
The provider portal should be optimized for mobile devices so you can access information anytime, from anywhere.

### Security

Robust security is essential so only authorized personnel can view network and DDoS attack/mitigation data.

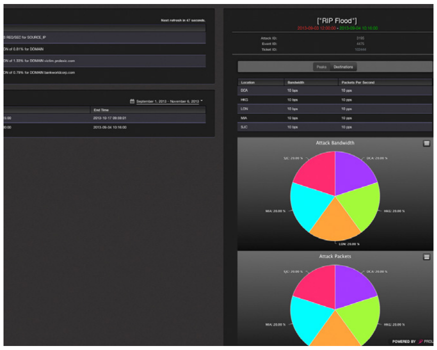
### Data Refresh Rate

You can't make the best decisions using outdated data. Look for a provider that updates network and mitigation data every few minutes.



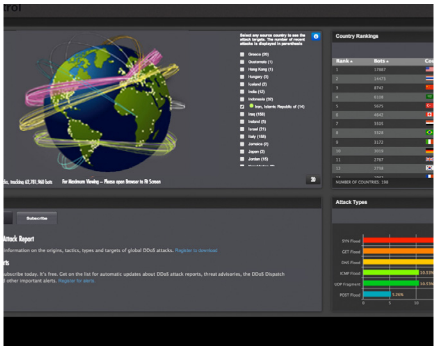
### Deep Network Visibility

Your mitigation provider should provide up-to-the minute visibility of their mitigation efforts on your behalf. And you should be able to see the big picture in one dashboard view.



### Real-Time Analytics

Your mitigation provider should deliver real-time analytics for a wide range of network and attack metrics, including HTTP and HTTPS request patterns for live traffic, as well as attack traffic distribution and attack behavior.



### Rich DDoS Forensics

Any good portal should also offer insight into current DDoS activity around the world so you can stay informed and be proactive.

## If you are not getting this level of insight from your current DDoS mitigation provider's portal, contact Prolexic.

PLXportal, available to all Prolexic customers, provides the most in-depth, real-time insight through countless drill down data views. To see what you've been missing, go to prolexic.com/ddosportal to watch the PLXportal video and download the brochure.

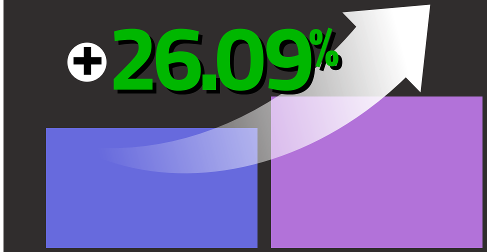
+1 (954) 620 6005
www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

# DDoS ATTACK REPORT Q4 13

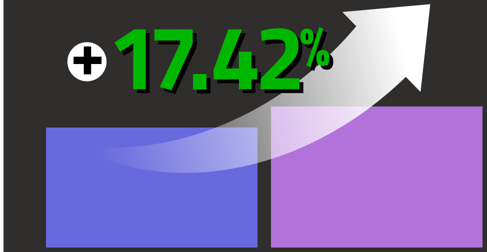
## Compared to Q4 2012

🟦 Q4 12 🟪 Q4 13



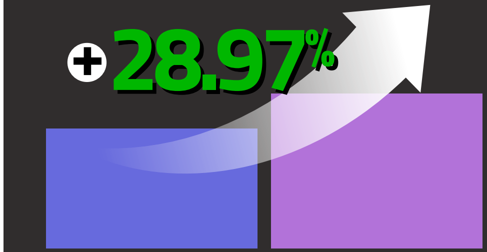
+26.09%

Increase in total DDoS attacks



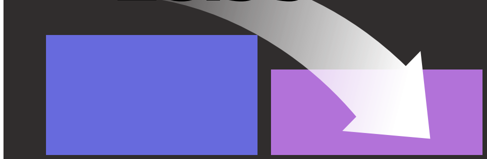
+17.42%

Increase in application layer (Layer 7) attacks



+28.97%

Increase in infrastructure layer (Layer 3 & 4) attacks

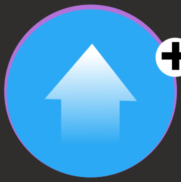


-28.95%

Decrease in average attack duration: 32.21 vs. 22.88 hours

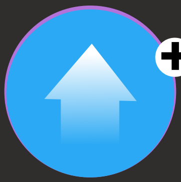
## Compared to Q3 2013

● Q3 13 ● Q4 13



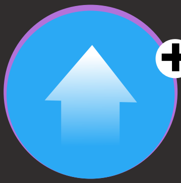
+1.56%

Increase in total DDoS attacks



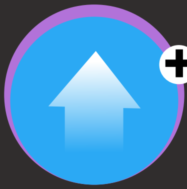
+0.55%

Increase in application layer (Layer 7) attacks



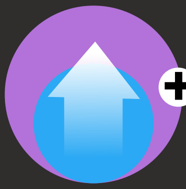
+1.86%

Increase in infrastructure layer (Layer 3 & 4) attacks



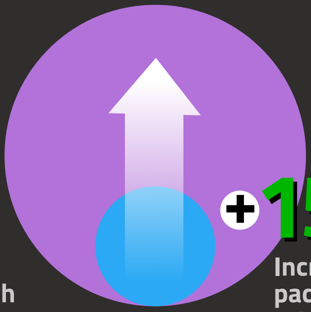
+7.25%

Increase in average attack duration: 22.88 vs. 21.33 hours



+48.04%

Increase in average peak attack bandwidth from 3.06 Gbps to 4.53 Gbps



+151.21%

Increase in peak packets-per-second rate from 4.22 Mpps to 10.60 Mpps

## Four Q4 Facts to Remember

1. Prolexic mitigated the most DDoS attacks in a single quarter
2. Prolexic mitigated the largest DDoS attack it has faced to date, which peaked at 179 Gbps
3. Prolexic saw evidence of mobile devices and apps being used in DDoS attacks
4. DDoS attacks are still increasing in size, frequency and complexity

+1 (954) 620 6005
www.prolexic.com

PROLEXIC
DDoS Attacks End Here.

# DDoS 2013 The Top 10 Trends

## 1 Attack volume

Prolexic mitigated 32.43% more distributed denial of service (DDoS) attacks in 2013 than it did in 2012.

## 2 Attack frequency

In a month-by-month comparison, DDoS attacks increased 10 out of 12 months in 2013 vs. 2012.

## 3 Application attacks

Layer 7 attacks rose approximately 42%.

## 4 Infrastructure attacks

Layer 3 & 4 attacks increased approximately 30%.

## 5 Actor vectors

Attack vectors that increased: DNS, UDP and CHARGEN.

## 6 Actor vectors

Actor vectors that decreased: SYN and ICMP floods.

## 7 Attack sizes

Prolexic mitigated numerous high bandwidth attacks over 100 Gbps, the largest peaking at 179 Gbps.

## 8 Attack methods

Distributed reflection (DrDoS) amplification attacks emerged as a popular attack method.

## 9 Mobile devices

Mobile devices and apps began participating in DDoS attacks.

## 10 Asian countries

Asian countries were the main source of DDoS attacks.

+1 (954) 620 6005
www.prolexic.com

PROLEXIC
DDoS Attacks End Here.