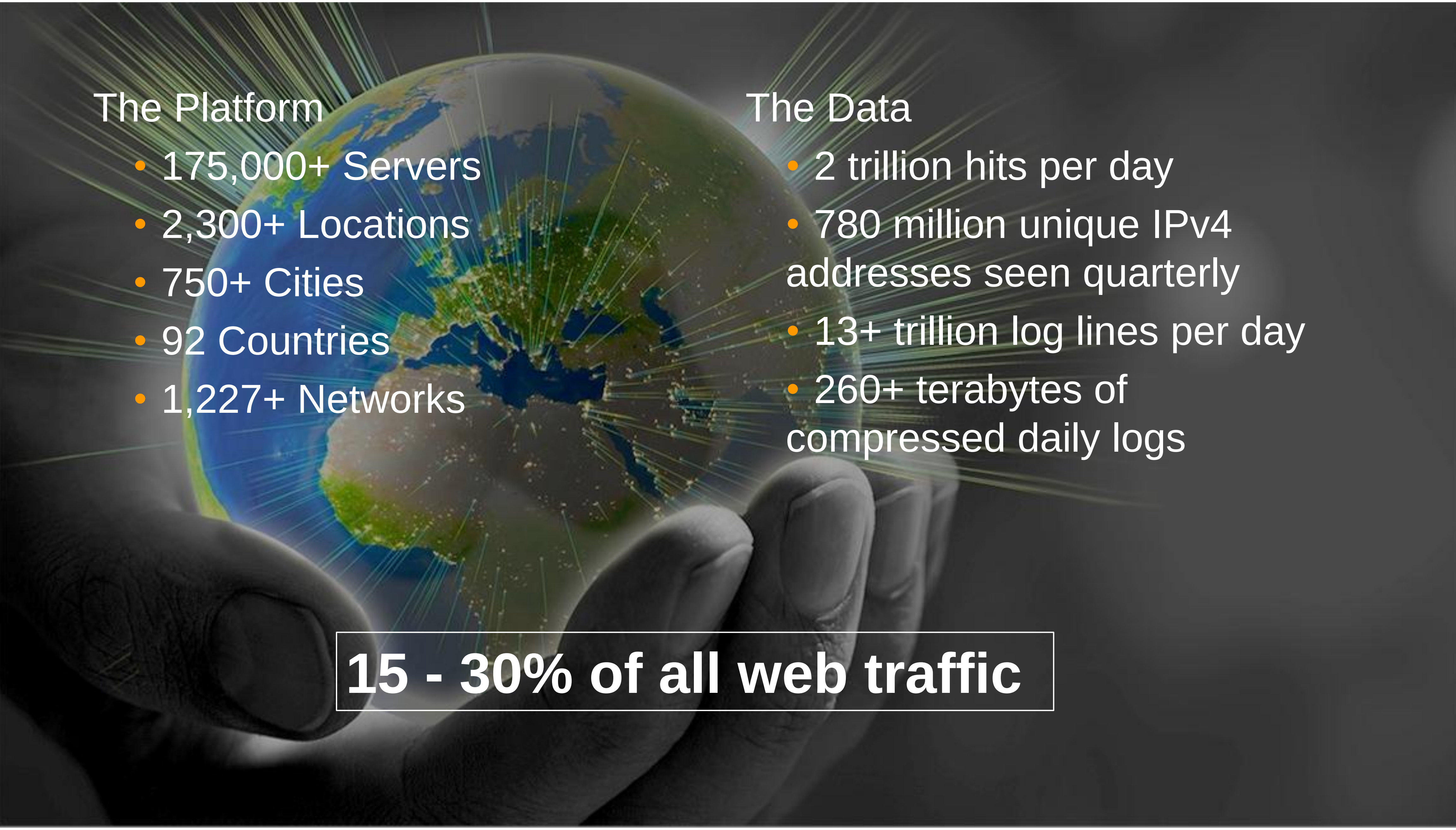
Akamai

FASTER FORWARD

War Stories from the Cloud: Rise of the Machines

John Summers
VP Security Products



The Platform

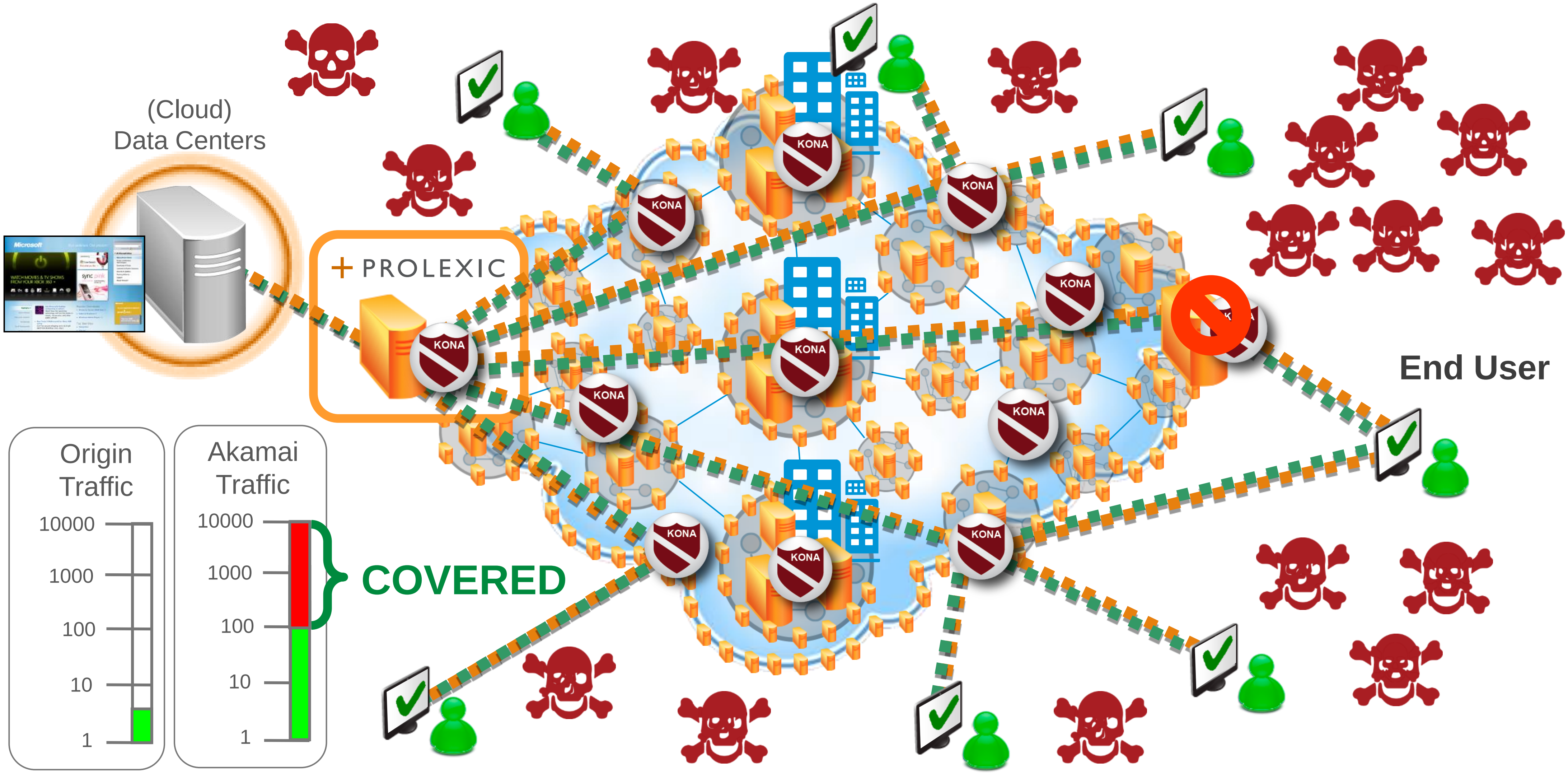
- 175,000+ Servers
- 2,300+ Locations
- 750+ Cities
- 92 Countries
- 1,227+ Networks

The Data

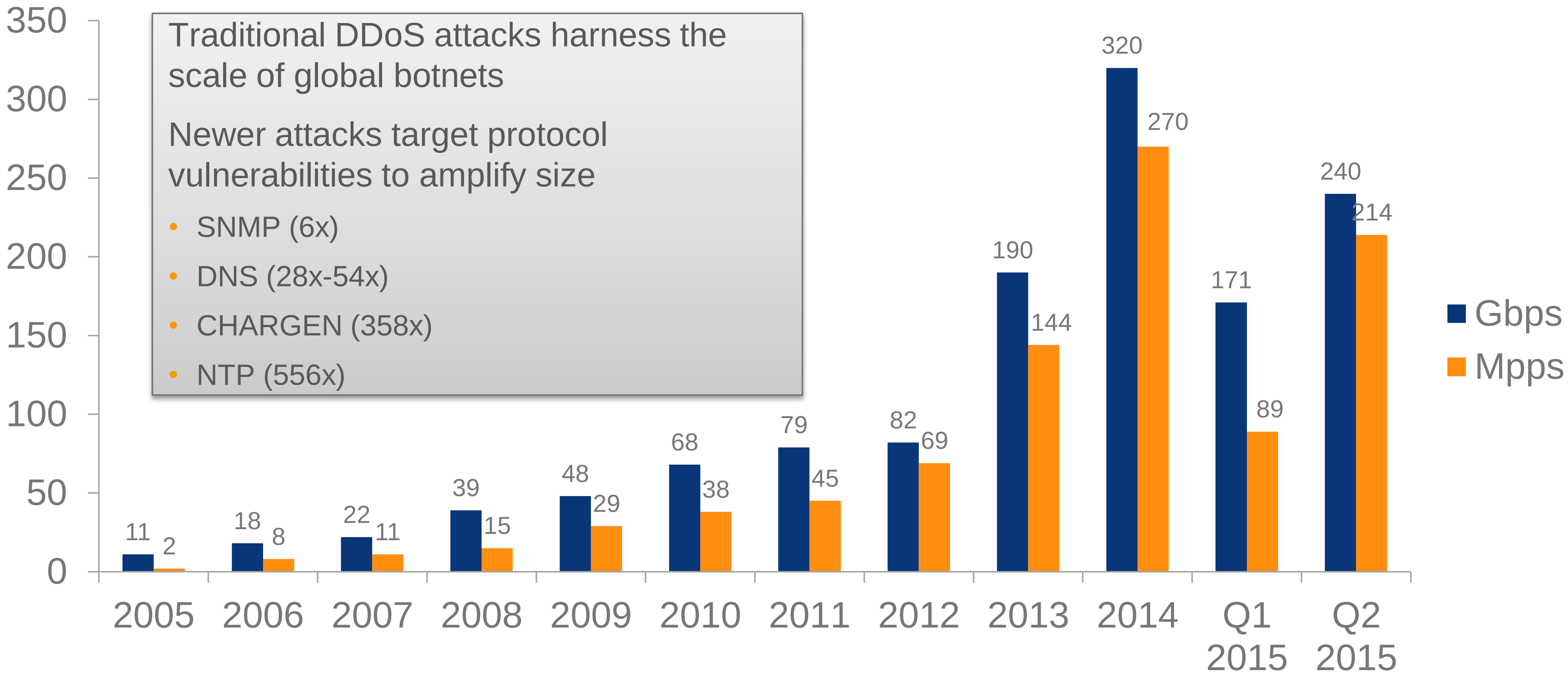
- 2 trillion hits per day
- 780 million unique IPv4 addresses seen quarterly
- 13+ trillion log lines per day
- 260+ terabytes of compressed daily logs

15 - 30% of all web traffic

The Akamai Solution – Kona Site Defender + Prolexic



In Q2 2015, DDoS attacks were less powerful, but longer and more frequent

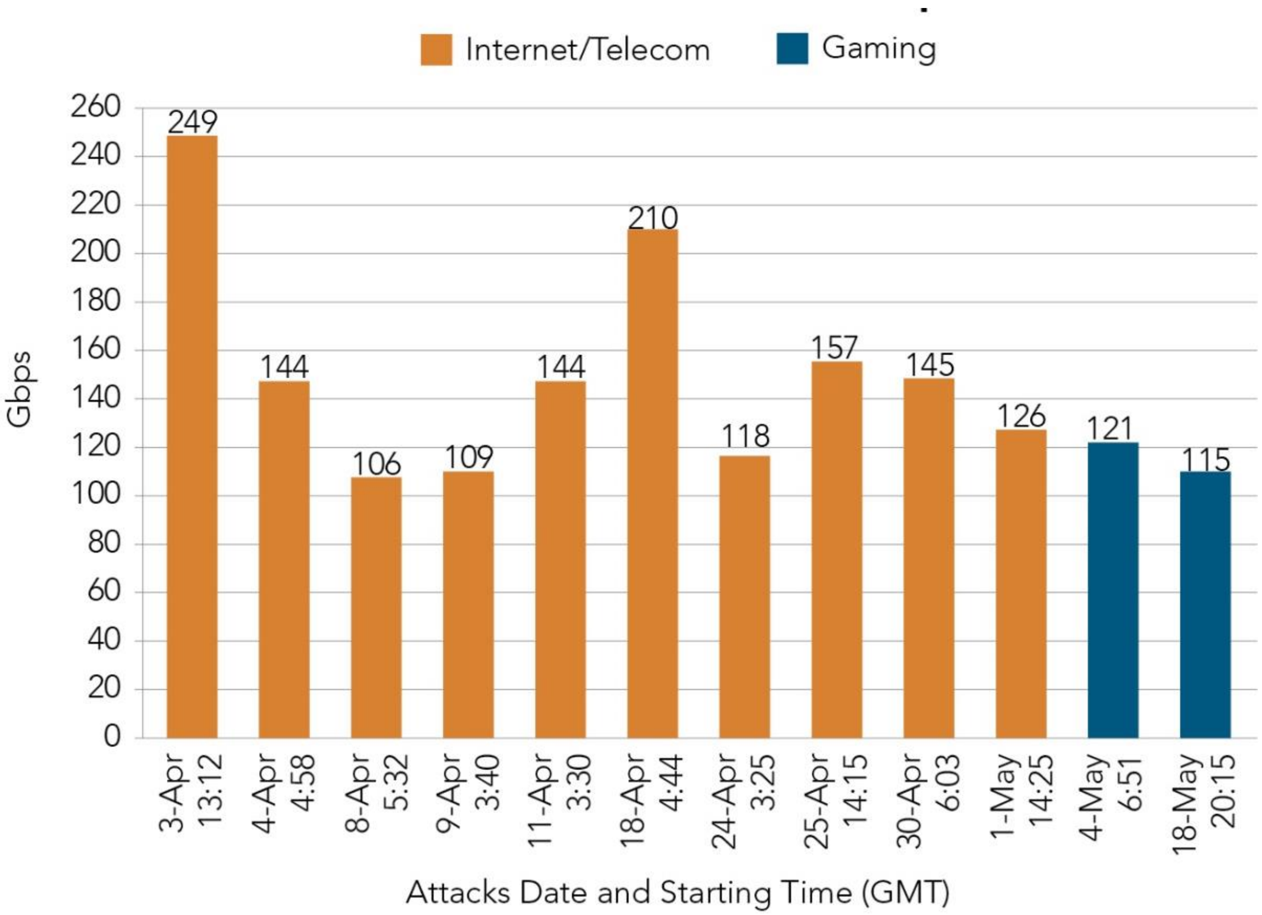


Traditional DDoS attacks harness the scale of global botnets

Newer attacks target protocol vulnerabilities to amplify size

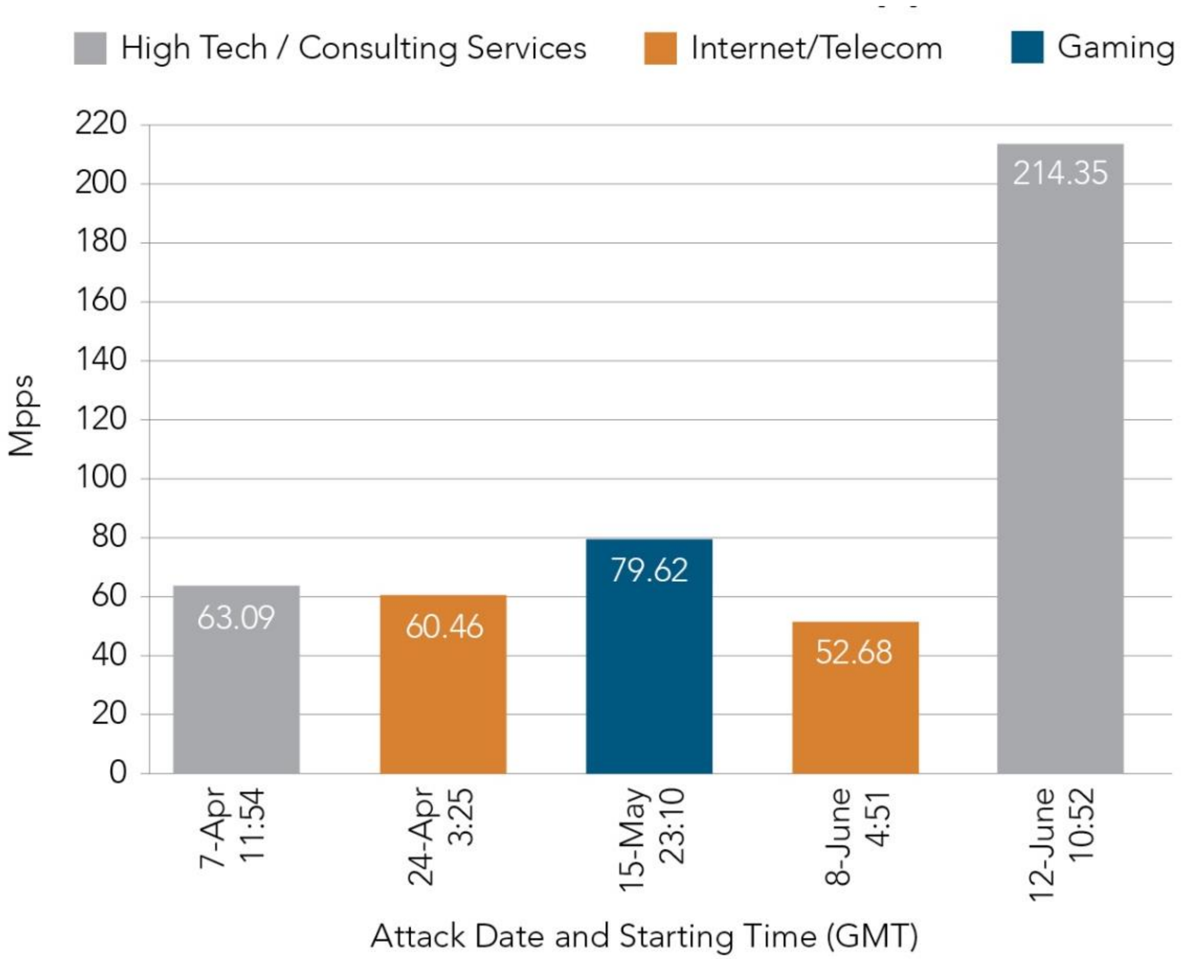
- SNMP (6x)
- DNS (28x-54x)
- CHARGEN (358x)
- NTP (556x)

DDoS Mega Attacks > 100 Gbps in Q2 2015



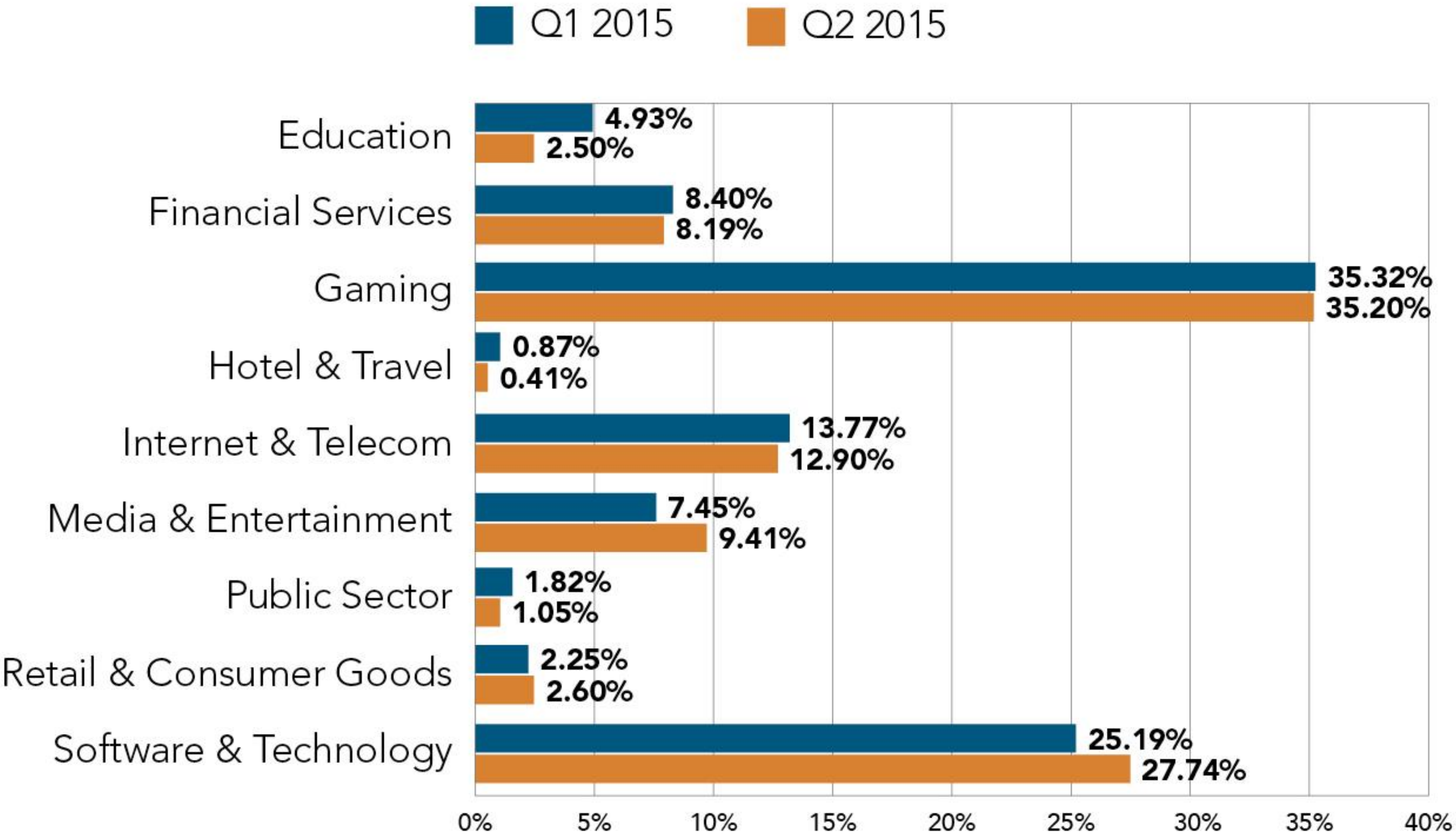
Twelve mega-attacks in Q2 2015 vs. six in Q2 2014. Most targeted Internet/Telecom. Two targeted Gaming.

DDoS Mega Attacks > 50 Mpps in Q2 2015

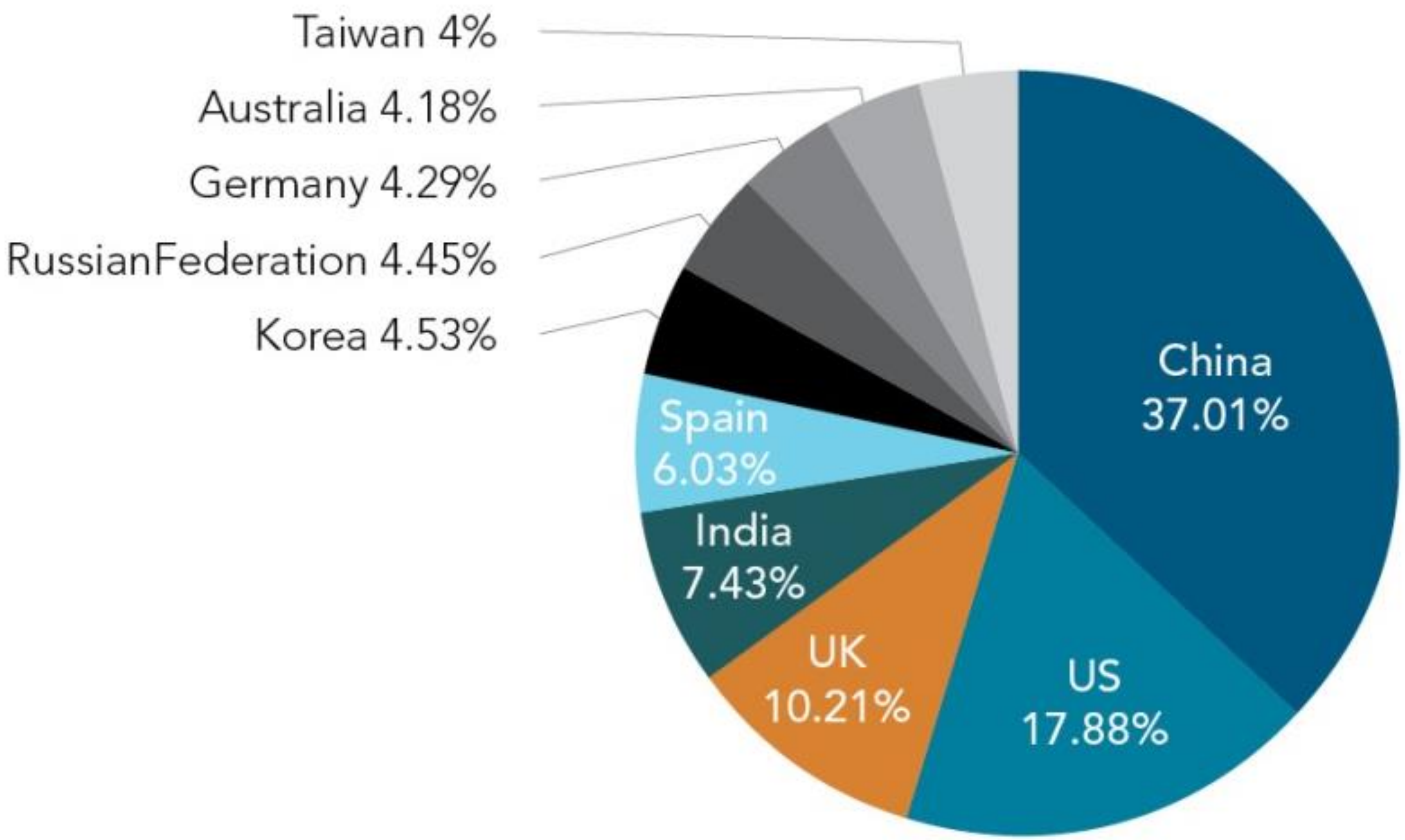


A 214 million packets per second (Mpps) DDoS attack was among the highest ever recorded. Such attacks can take out tier 1 routers, such as used by Internet service providers (ISPs).

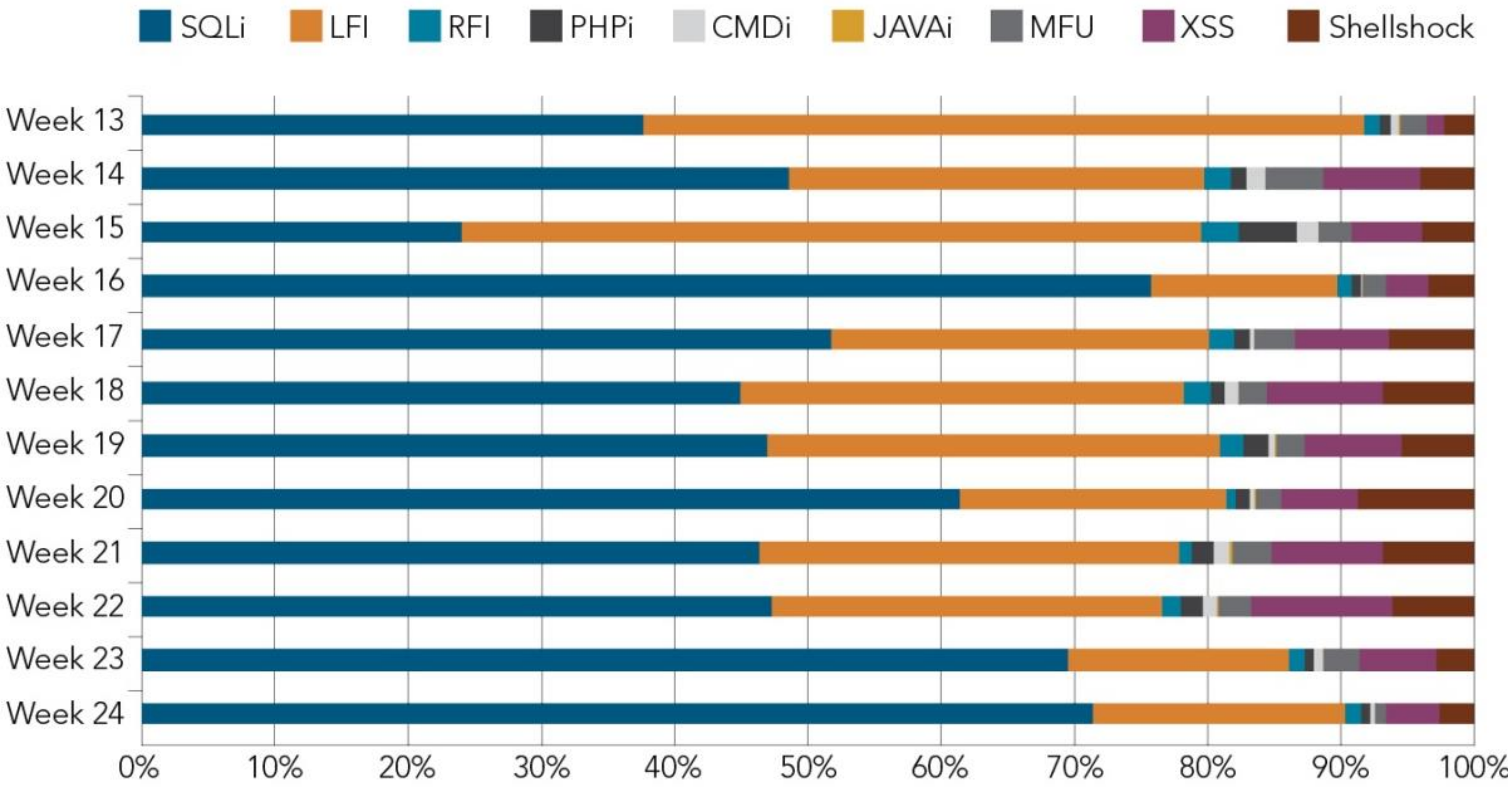
Most Commonly DDoS'ed Verticals – Q1 2015



Top 10 Source Countries for DDoS Attacks in Q2 2015

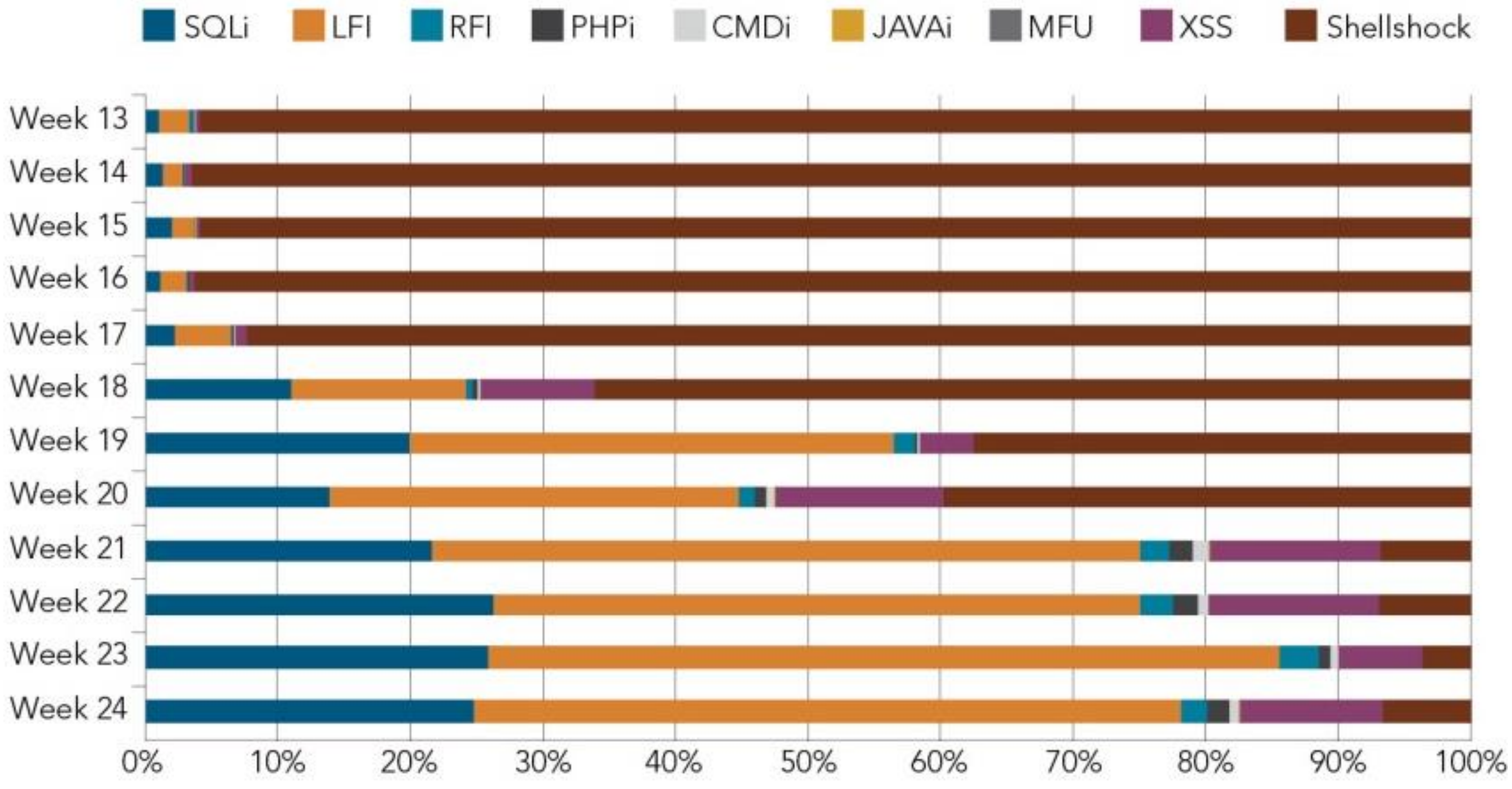


Web Application Attack Vectors, Q2 2015



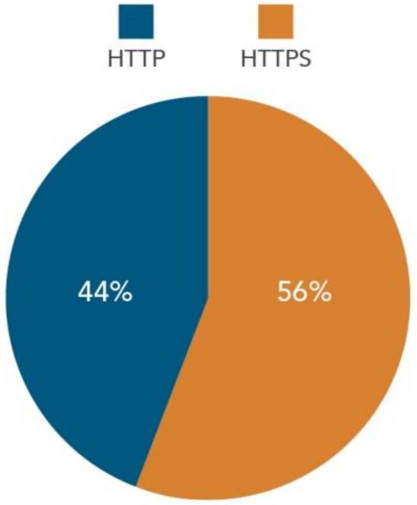
SQLi and LFI were the most prevalent attack vectors over HTTP.

Attacks Over HTTPS, Q2 2015

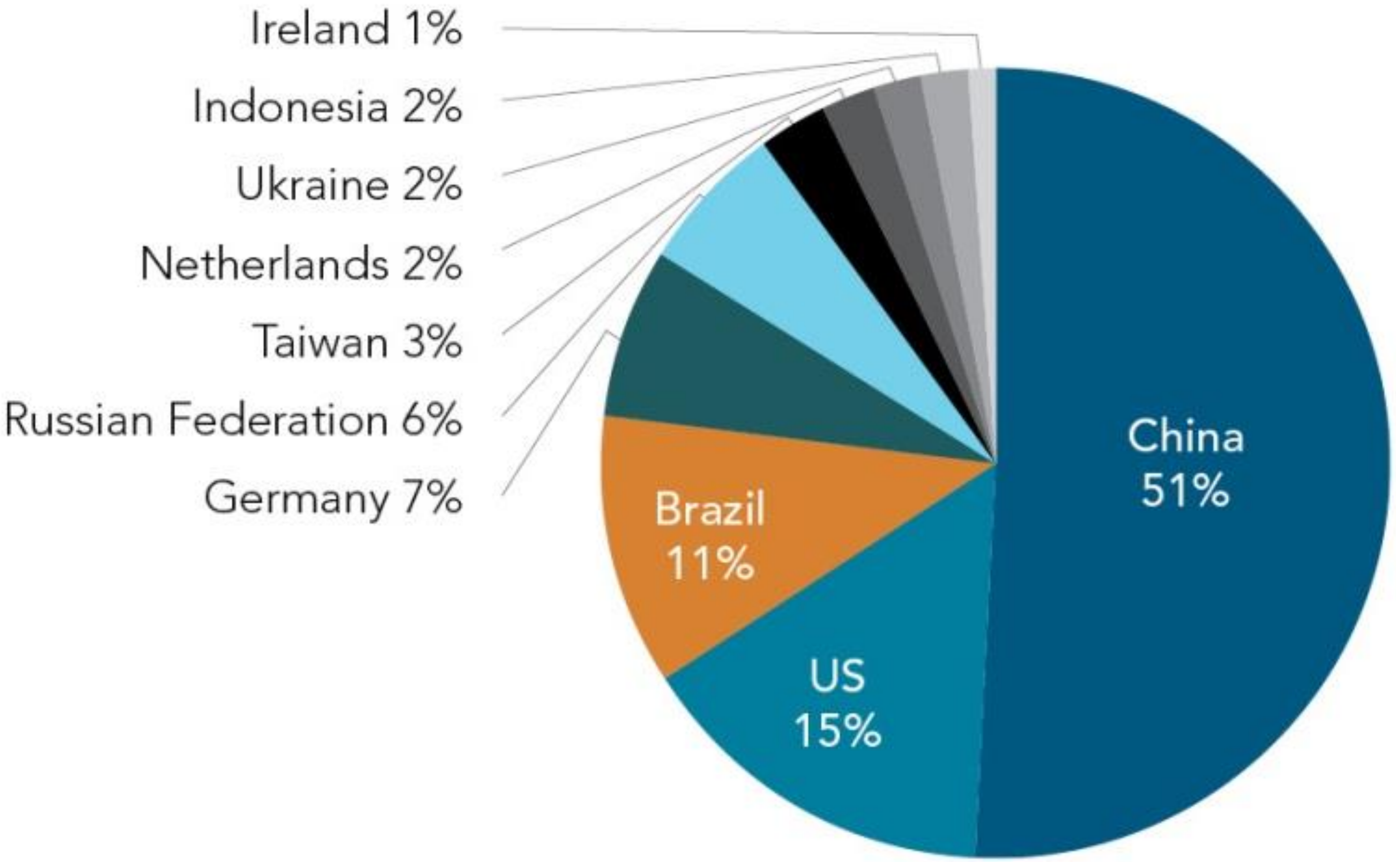


Shellshock accounted for 49% of web application attacks in Q2, largely due to a persistent, multi-week campaign against a single customer.

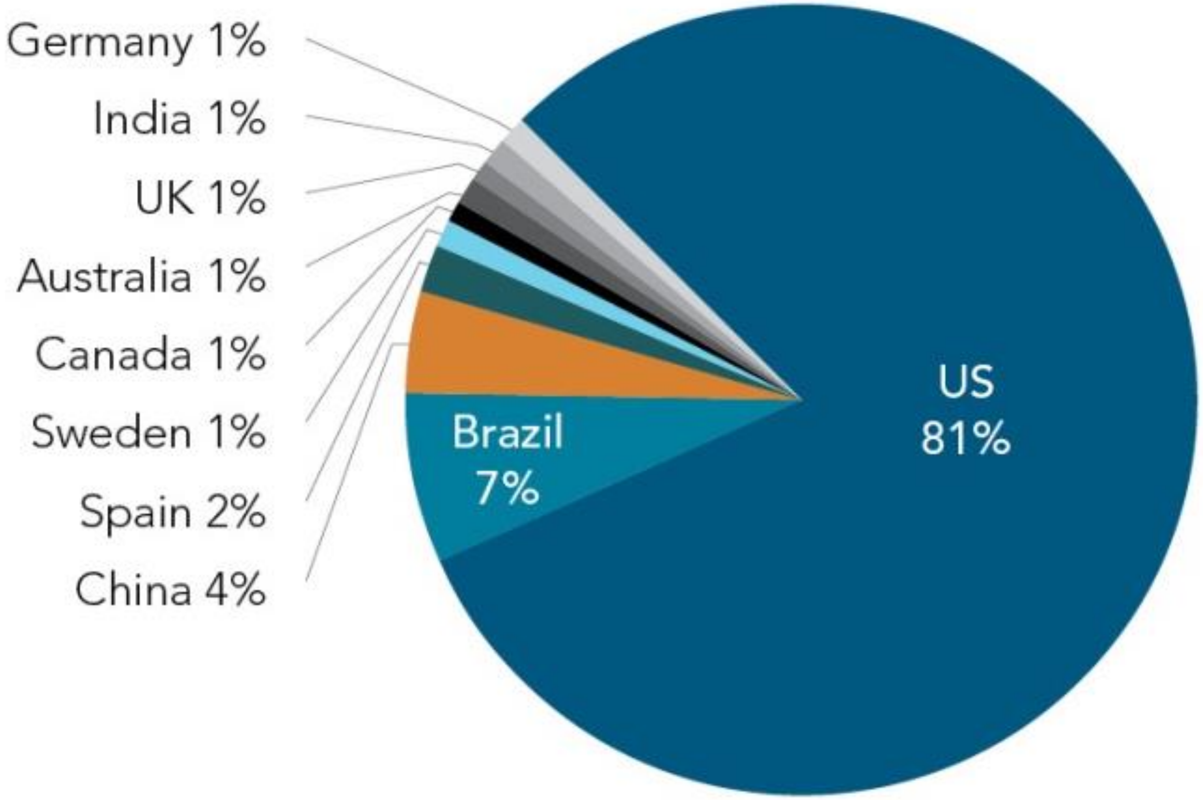
Shellshock attacks shifted the balance of attacks to HTTPS (56%). Last quarter, only 9% of attacks were over HTTPS.



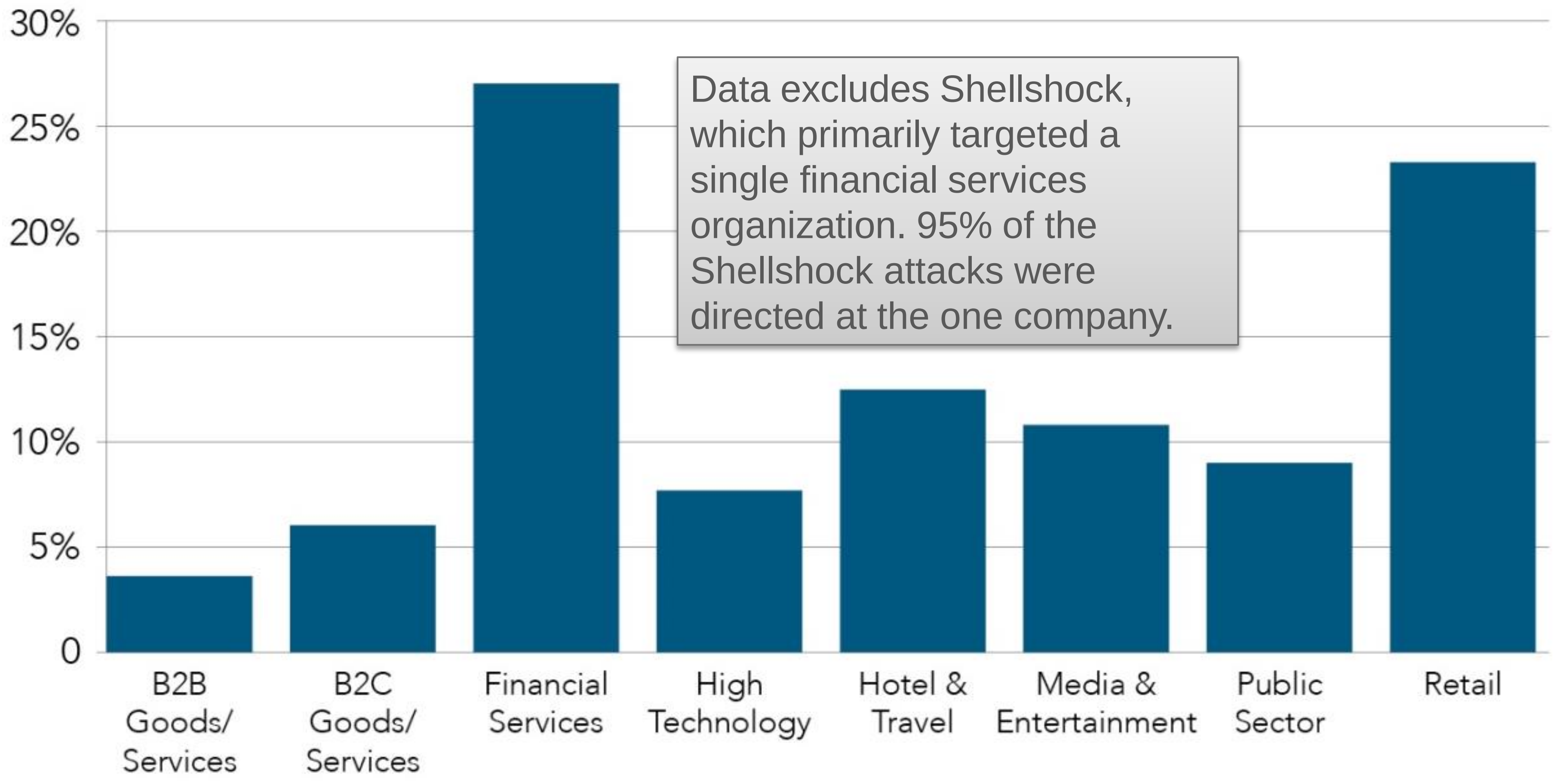
Top 10 Source Countries for Web Application Attacks, Q2 2015



Top 10 Target Countries for Web Application Attacks, Q2 2015



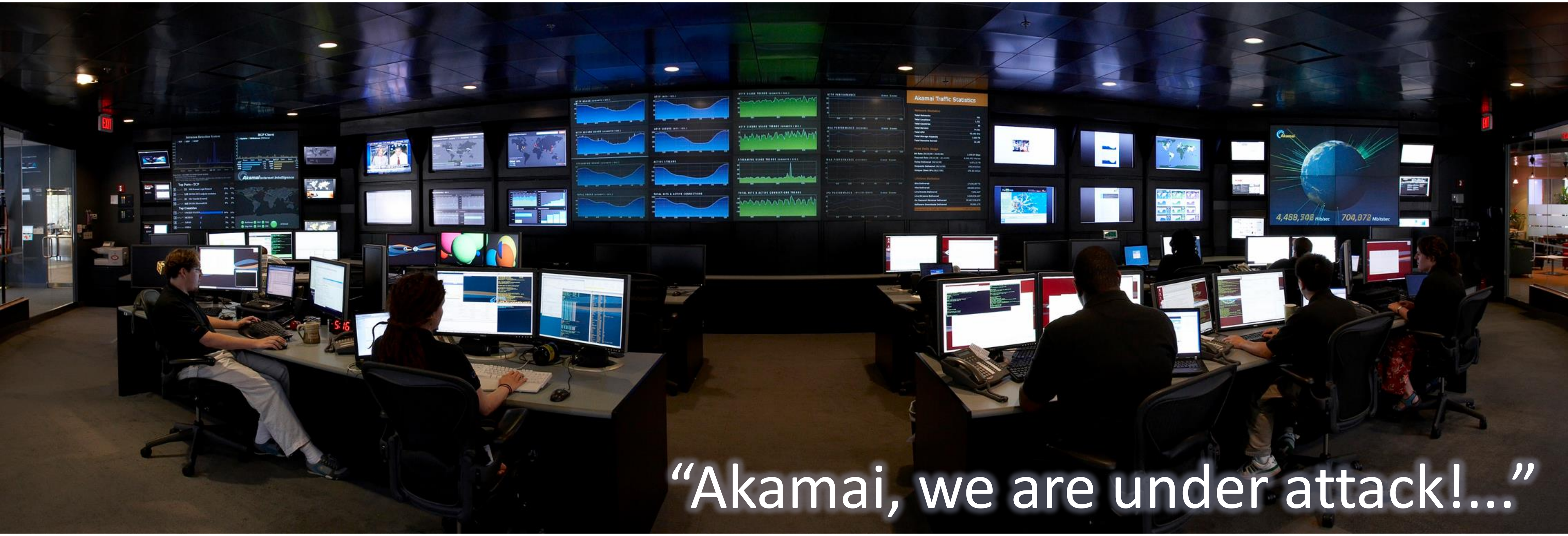
Web Application Attacks by Industry, Q2 2015



Data excludes Shellshock, which primarily targeted a single financial services organization. 95% of the Shellshock attacks were directed at the one company.

Leveraging Big Data to Understand Attacks

The following slides are based on a real events on January 5th 2014....



“Akamai, we are under attack!...”

Ad-Hoc Attack Analysis

An attempt to exploit an old (2007) WordPress Remote File Inclusion vulnerability. The victim application was running ASP.NET

```
GET /wp-content/wordtube-button.php?wpPATH=http://www.google.com/humans.txt?
HTTP/1.1
Host: www.vulnerable.site
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
```

Attacked parameter :	wpPATH
Malicious payload:	http://www.google.com/humans.txt

What Else Did This Attacker Do On This Site?

Same attacker Sent 2122 different RFI exploit attempts

```
_PATH=http://www.go
h=http://www.google.com/huma
p?file=http://www.google.com/humans
olbar.php?dirDepth=http://www.google.com
ier=http://www.google.com/humans.txt? HTTP/1
album.php?phpbb_root_path=http://www.google.com
/lang_activity.php?phpbb_root_path=http://www.goog
/lang_admin_album.php?phpbb_root_path=http://www.go
/lang_admin_album.php?phpbb_root_path=http://www.goo
/lang_main_album.php?phpbb_root_path=http://www.googl
umspath=http://www.google.com/humans.txt? HTTP/1.0
rel=http://www.google.com/humans.txt? HTTP/1.0
s.php?gConf[dir][layouts]=http://www.google.com/human
cludePath=http://www.google.com/humans.txt? HTTP/1.0
rmExport.inc.php?includePath=http://www.google.com/
path=http://www.google.com/humans.txt? HTTP/1.0
dar.php?pathToIndex=http://www.google.com/huma
php?pathToIndex=http://www.google.com/hum
thToIndex=http://www.google.com/human
?pathToIndex=http://www.google
google.com/humans.txt?
//www.goo
```

34 different sites were attacked by the same attacker

with a total of 24,301 attacks

Welcome to Facebook – Log In, Si...
Altoro Mutual
Gmail: Email from Google
Altoro Mutual
Akamai Technologies Web Login
wired.com
Layered web browser - Google S...
Debuggex: The online visual reg...
Debuggex: The online visual reg...
PHP: Manual Quick Reference
חדשות, ידיעות מהארץ והעולם - ...עית
...Top Sites in Safari 7: A...
Apple - Start
iCloud
Twitter
Wikipedia, the free encyclopedia
Yahoo
Technology News & Computers...
Amazon.com: Online Shopping fo...
BBC - Hom...
דיסני, הבית של הסדרות, הסרטים, ה...
CNN.com International - Breakin...
Electronics, Cars, Fashion, Collec...

Was There Similar Activity Going On At The Same Time?

Attacks originated from a **botnet** containing **272** attacking machines

1696 victim applications were targeted

1,358,980 attacks were launched during the campaign

The campaign lasted for **2** weeks

Security Big Data at Akamai: Cloud Security Intelligence

20 Terabytes of daily attack data

2 Petabytes of security data stored

Up to 90 days retention

600K log lines/sec. indexed by 30 dimensions

8000 queries daily scanning terabytes of

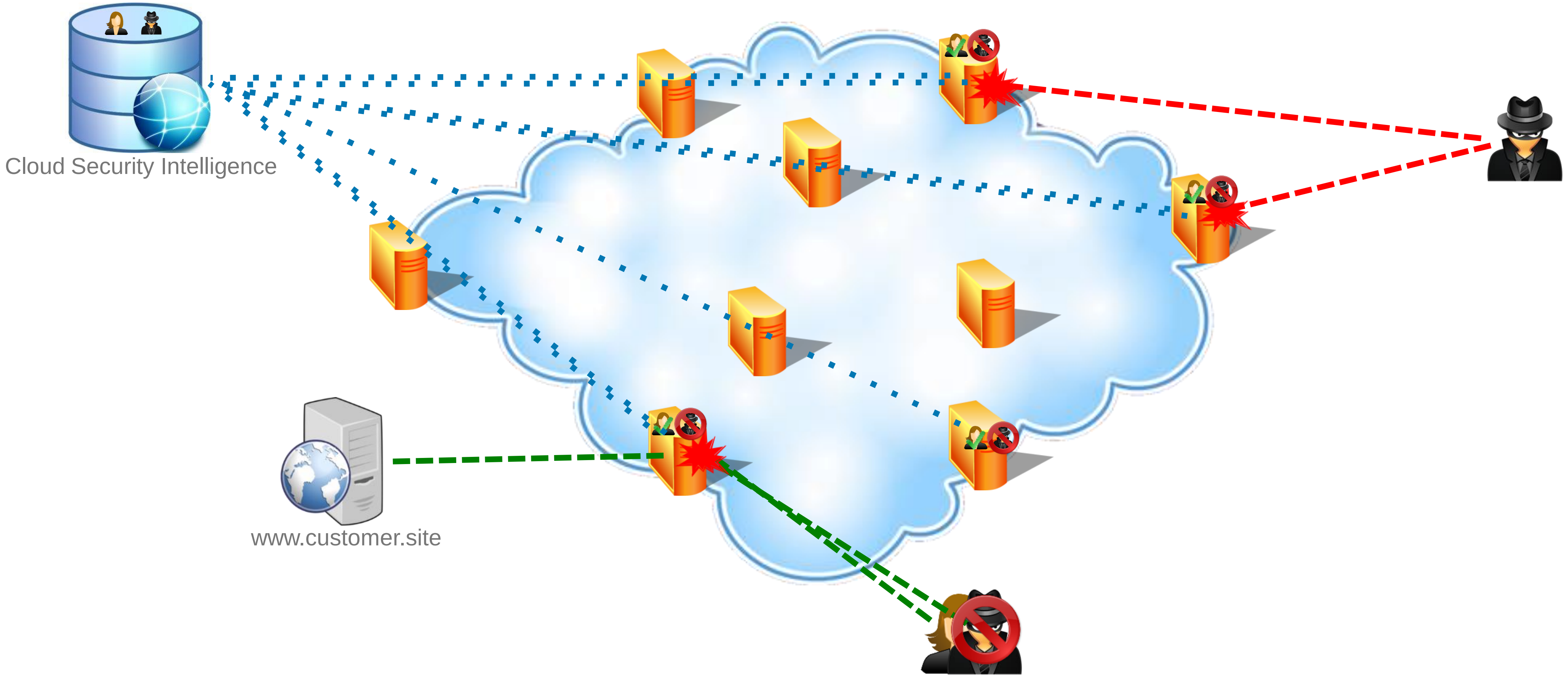
Benefits

Unrivaled Web Security visibility

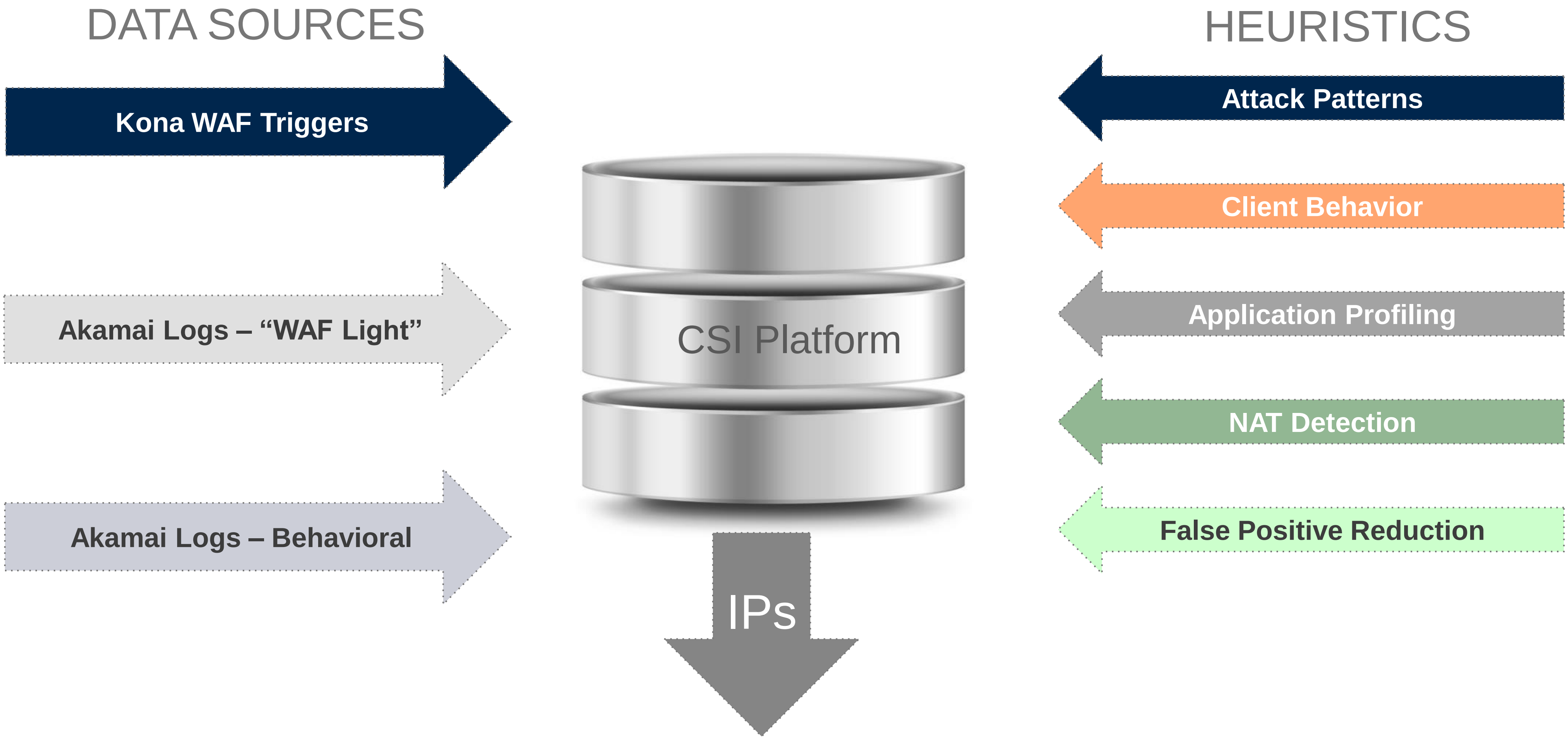
- Perform WAF accuracy analysis on any customer at any time
- Detect new attacks, including 0-day and quickly issue new protections

- A powerful web security research tool
- Improve WAF Accuracy
- Behavioral analytics platform

Behavioral Analytics & The Akamai Intelligent Platform



Proactive Security using Behavioral Analytics



DATA SOURCES

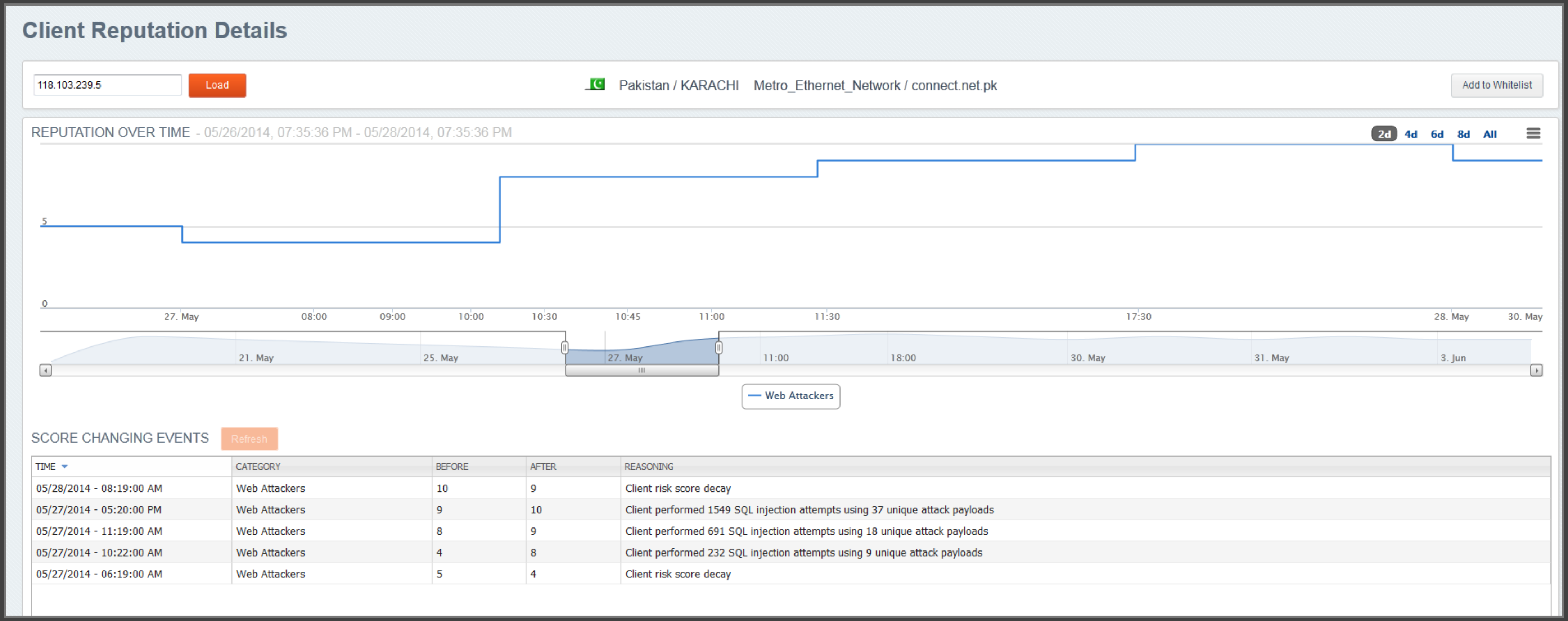
- Kona WAF Triggers
- Akamai Logs – “WAF Light”
- Akamai Logs – Behavioral

CSI Platform

IPs

HEURISTICS

- Attack Patterns
- Client Behavior
- Application Profiling
- NAT Detection
- False Positive Reduction



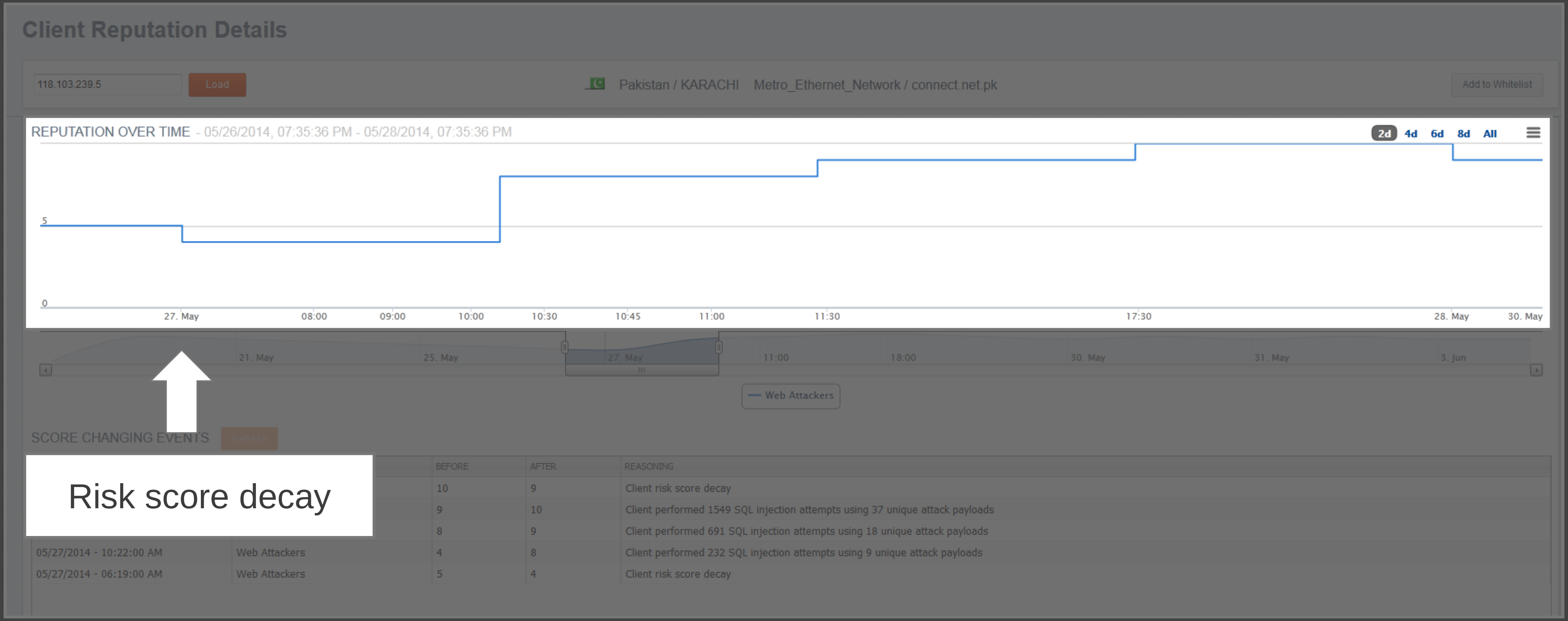
Client Reputation Details

118.103.239.5

Pakistan / KARACHI Metro_Ethernet_Network / connect.net.pk

SCORE CHANGING EVENTS

TIME	CATEGORY	BEFORE	AFTER	REASONING
05/28/2014 - 08:19:00 AM	Web Attackers	10	9	Client risk score decay
05/27/2014 - 05:20:00 PM	Web Attackers	9	10	Client performed 1549 SQL injection attempts using 37 unique attack payloads
05/27/2014 - 11:19:00 AM	Web Attackers	8	9	Client performed 691 SQL injection attempts using 18 unique attack payloads
05/27/2014 - 10:22:00 AM	Web Attackers	4	8	Client performed 232 SQL injection attempts using 9 unique attack payloads
05/27/2014 - 06:19:00 AM	Web Attackers	5	4	Client risk score decay



Client Reputation Details

118.103.239.5 Load

Pakistan / KARACHI Metro_Ethernet_Network / connect.net.pk

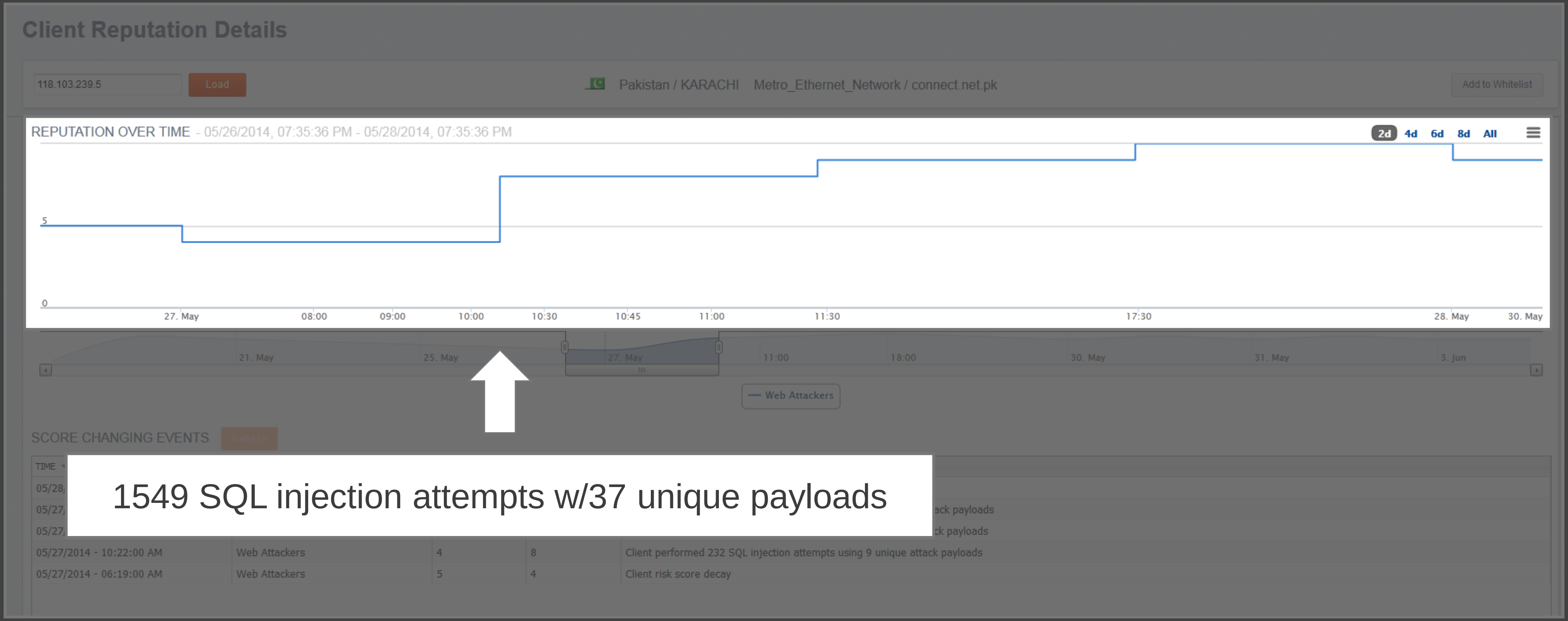
Add to Whitelist

REPUTATION OVER TIME - 05/26/2014, 07:35:36 PM - 05/28/2014, 07:35:36 PM

SCORE CHANGING EVENTS Refresh

Risk score decay

		BEFORE	AFTER	REASONING
		10	9	Client risk score decay
		9	10	Client performed 1549 SQL injection attempts using 37 unique attack payloads
		8	9	Client performed 691 SQL injection attempts using 18 unique attack payloads
05/27/2014 - 10:22:00 AM	Web Attackers	4	8	Client performed 232 SQL injection attempts using 9 unique attack payloads
05/27/2014 - 06:19:00 AM	Web Attackers	5	4	Client risk score decay



Client Reputation Details

118.103.239.5 Load

Pakistan / KARACHI Metro_Ethernet_Network / connect.net.pk

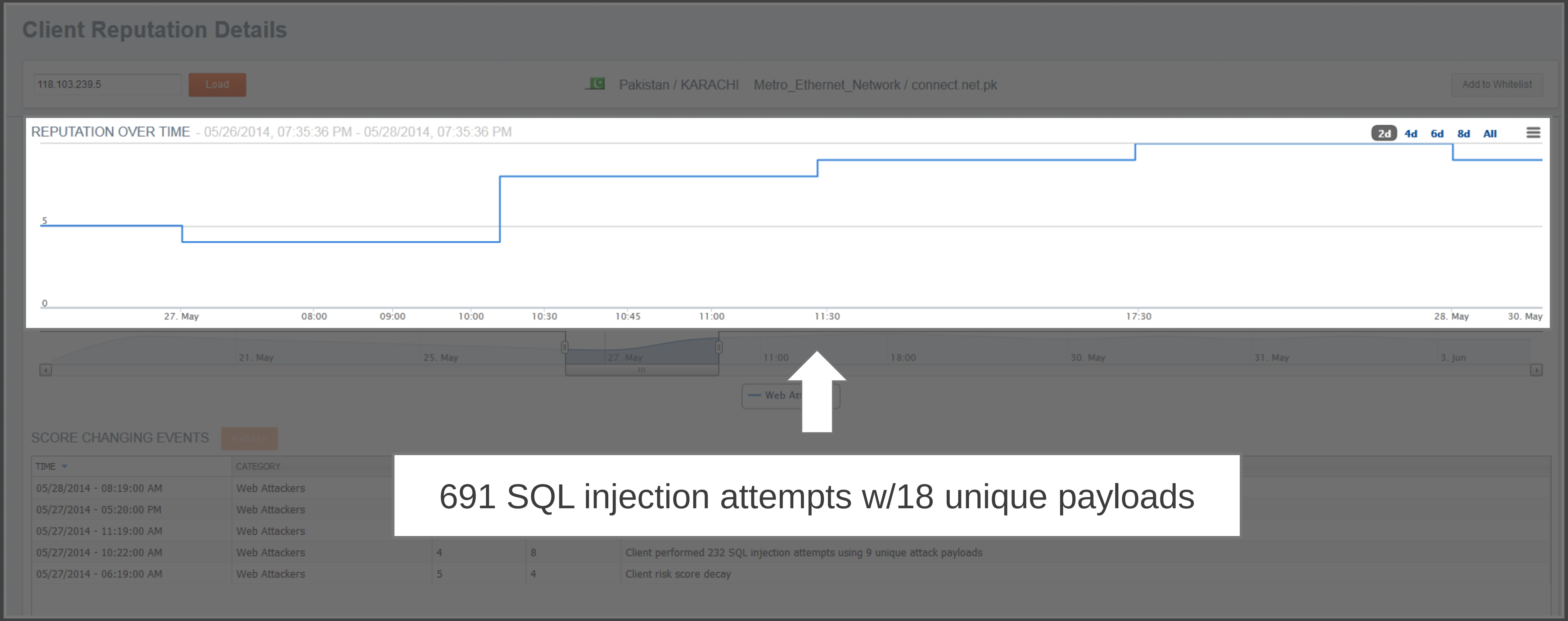
Add to Whitelist

REPUTATION OVER TIME - 05/26/2014, 07:35:36 PM - 05/28/2014, 07:35:36 PM

SCORE CHANGING EVENTS Refresh

TIME				
05/28,				
05/27,				ack payloads
05/27,				ck payloads
05/27/2014 - 10:22:00 AM	Web Attackers	4	8	Client performed 232 SQL injection attempts using 9 unique attack payloads
05/27/2014 - 06:19:00 AM	Web Attackers	5	4	Client risk score decay

1549 SQL injection attempts w/37 unique payloads



Client Reputation Details

118.103.239.5 Load

Pakistan / KARACHI Metro_Ethernet_Network / connect.net.pk

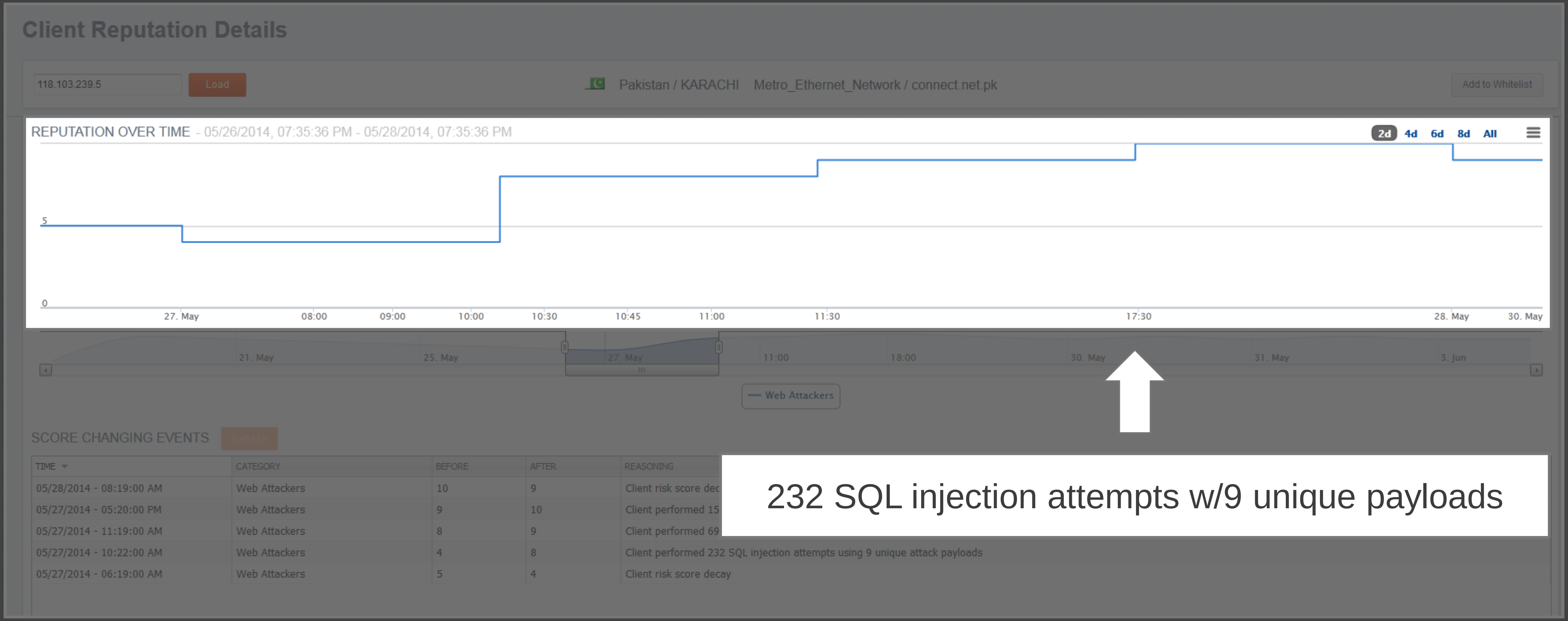
Add to Whitelist

REPUTATION OVER TIME - 05/26/2014, 07:35:36 PM - 05/28/2014, 07:35:36 PM

SCORE CHANGING EVENTS Refresh

TIME	CATEGORY			
05/28/2014 - 08:19:00 AM	Web Attackers			
05/27/2014 - 05:20:00 PM	Web Attackers			
05/27/2014 - 11:19:00 AM	Web Attackers			
05/27/2014 - 10:22:00 AM	Web Attackers	4	8	Client performed 232 SQL injection attempts using 9 unique attack payloads
05/27/2014 - 06:19:00 AM	Web Attackers	5	4	Client risk score decay

691 SQL injection attempts w/18 unique payloads



Client Reputation Details

118.103.239.5 Load

Pakistan / KARACHI Metro_Ethernet_Network / connect.net.pk

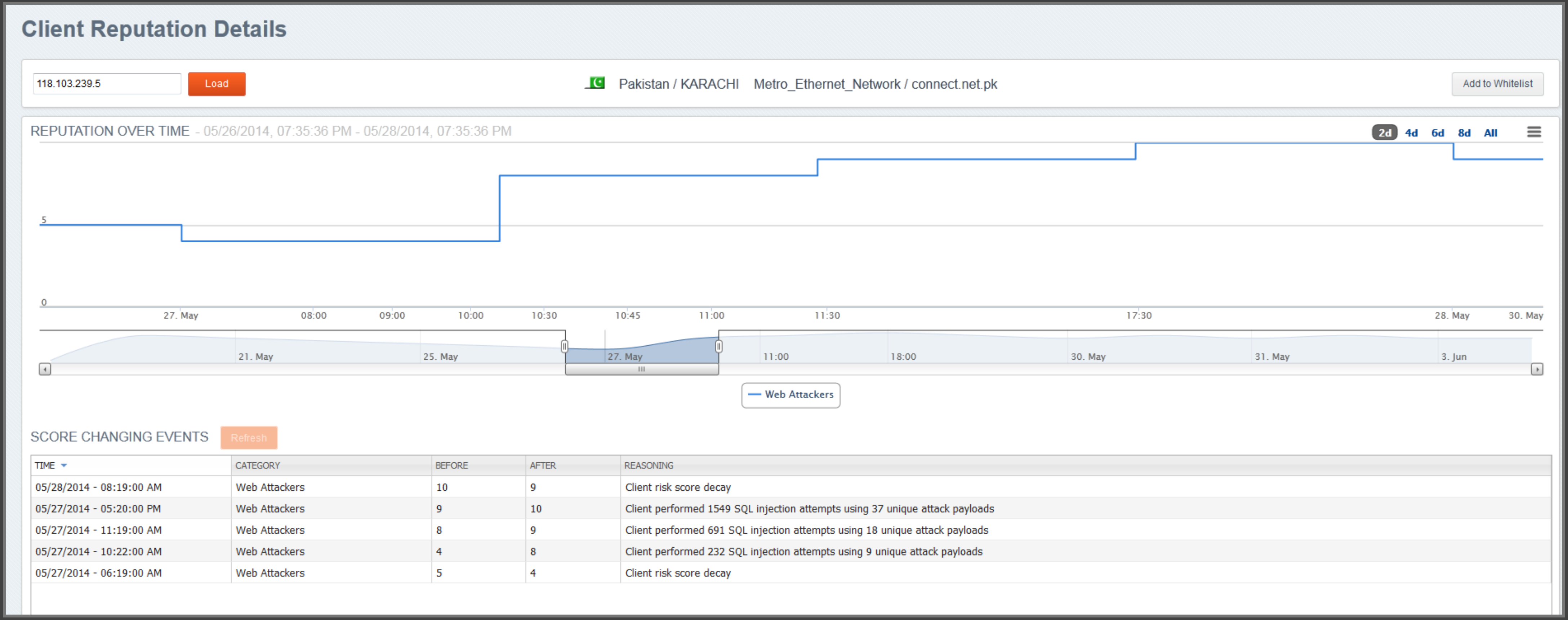
Add to Whitelist

REPUTATION OVER TIME - 05/26/2014, 07:35:36 PM - 05/28/2014, 07:35:36 PM

SCORE CHANGING EVENTS Refresh

TIME	CATEGORY	BEFORE	AFTER	REASONING
05/28/2014 - 08:19:00 AM	Web Attackers	10	9	Client risk score dec
05/27/2014 - 05:20:00 PM	Web Attackers	9	10	Client performed 15
05/27/2014 - 11:19:00 AM	Web Attackers	8	9	Client performed 69
05/27/2014 - 10:22:00 AM	Web Attackers	4	8	Client performed 232 SQL injection attempts using 9 unique attack payloads
05/27/2014 - 06:19:00 AM	Web Attackers	5	4	Client risk score decay

232 SQL injection attempts w/9 unique payloads



Client Reputation Details

118.103.239.5 | Load

Pakistan / KARACHI Metro_Ethernet_Network / connect.net.pk

SCORE CHANGING EVENTS

TIME	CATEGORY	BEFORE	AFTER	REASONING
05/28/2014 - 08:19:00 AM	Web Attackers	10	9	Client risk score decay
05/27/2014 - 05:20:00 PM	Web Attackers	9	10	Client performed 1549 SQL injection attempts using 37 unique attack payloads
05/27/2014 - 11:19:00 AM	Web Attackers	8	9	Client performed 691 SQL injection attempts using 18 unique attack payloads
05/27/2014 - 10:22:00 AM	Web Attackers	4	8	Client performed 232 SQL injection attempts using 9 unique attack payloads
05/27/2014 - 06:19:00 AM	Web Attackers	5	4	Client risk score decay

A Year in the Life of a Botnet

In January 2014 we published a blog on a global botnet:

- https://blogs.akamai.com/2014/01/analyzing-a-malicious-botnet-attack-campaign-through-the-security-big-data-prism.html

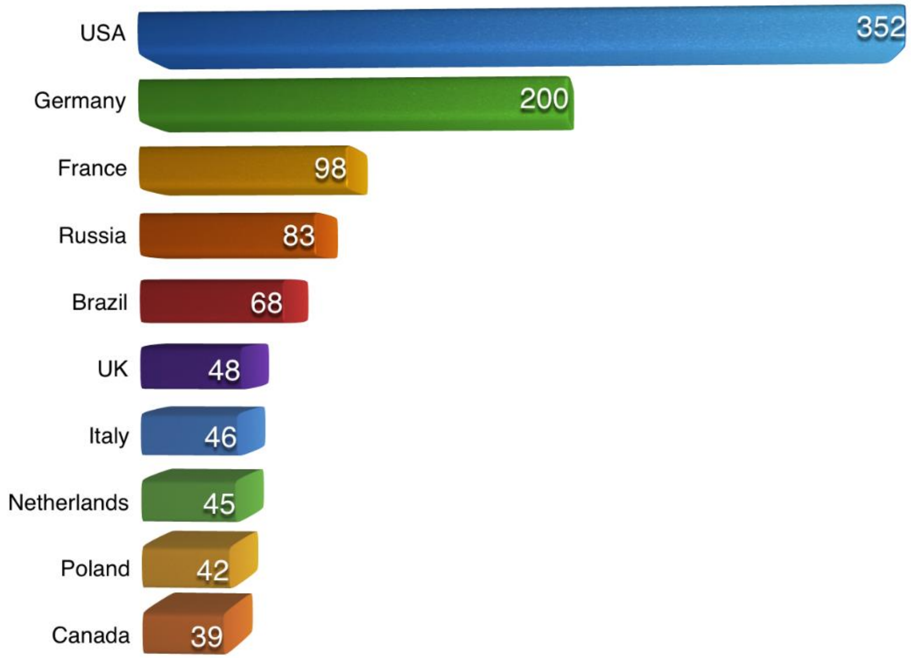
Exploiting Joomla Content Editor vulnerability to install backdoors

Began as a “single event” analysis of the exploit

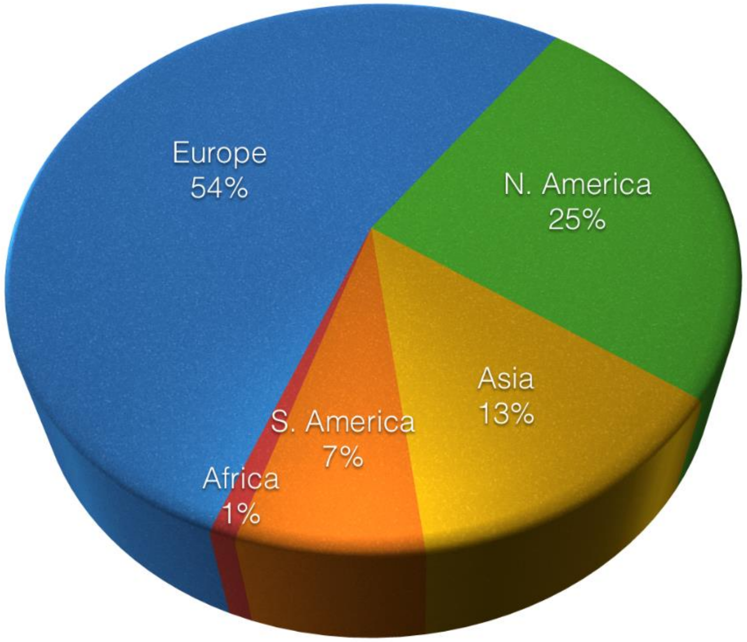
“Zoomed out” and discovered an entire botnet mining the web for vulnerable Joomla servers

A Truly Global Botnet

Botnet Machine Distribution by Country (Top 10)

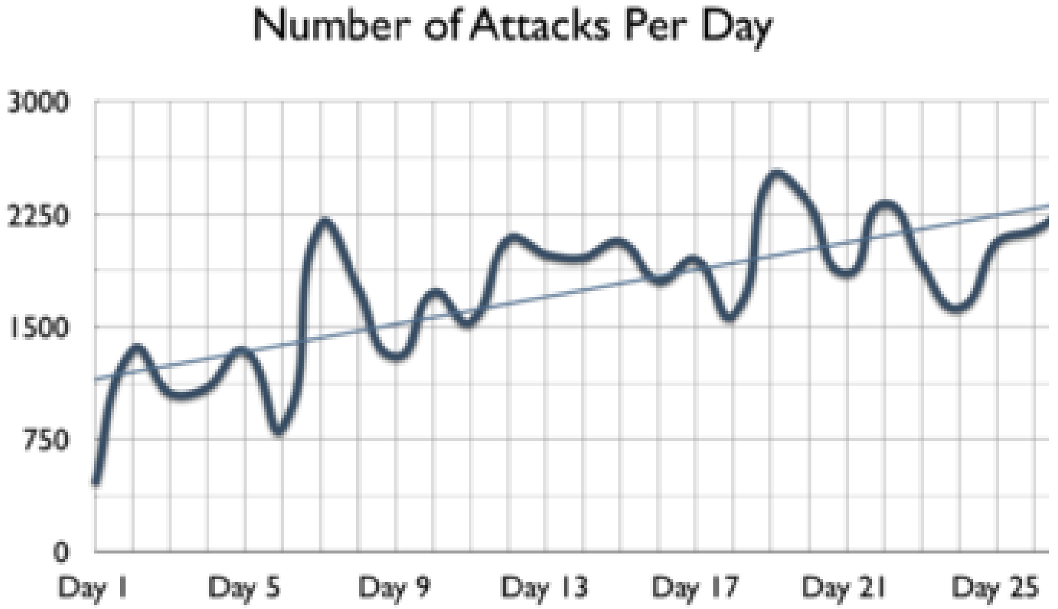


Botnet Machine Distribution by Continent

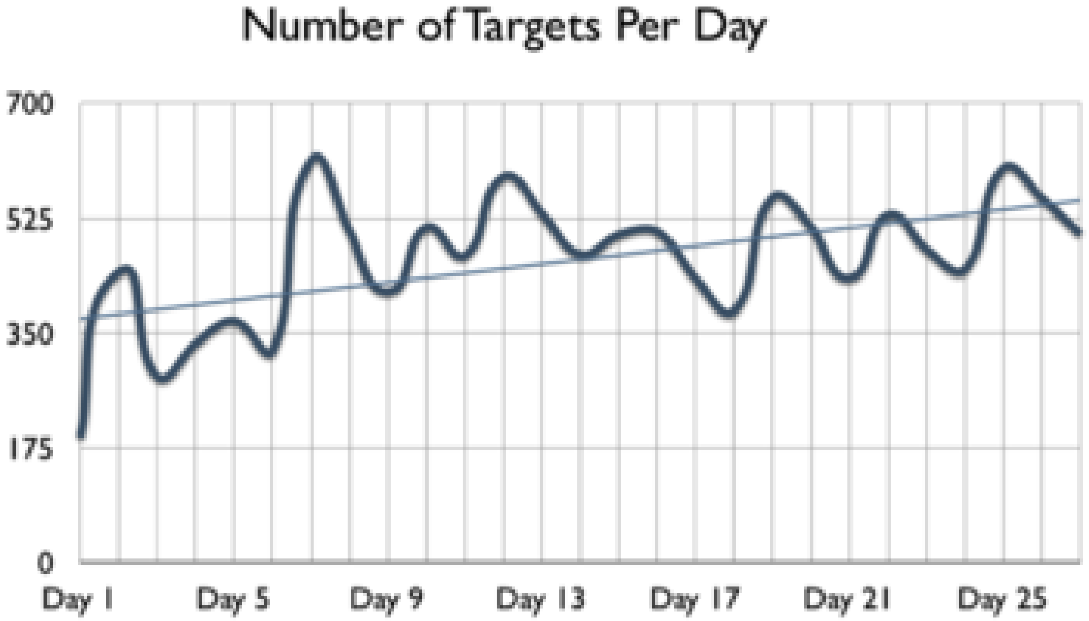


And a Very Active Botnet

- 43,000 malicious HTTP requests seen over the month
- 2008 different web applications were targeted



Number of Attacks Per Day



Number of Targets Per Day

10 months later, the Botnet lives on…

In Nov. 2014, the team began a 3 month follow on analysis

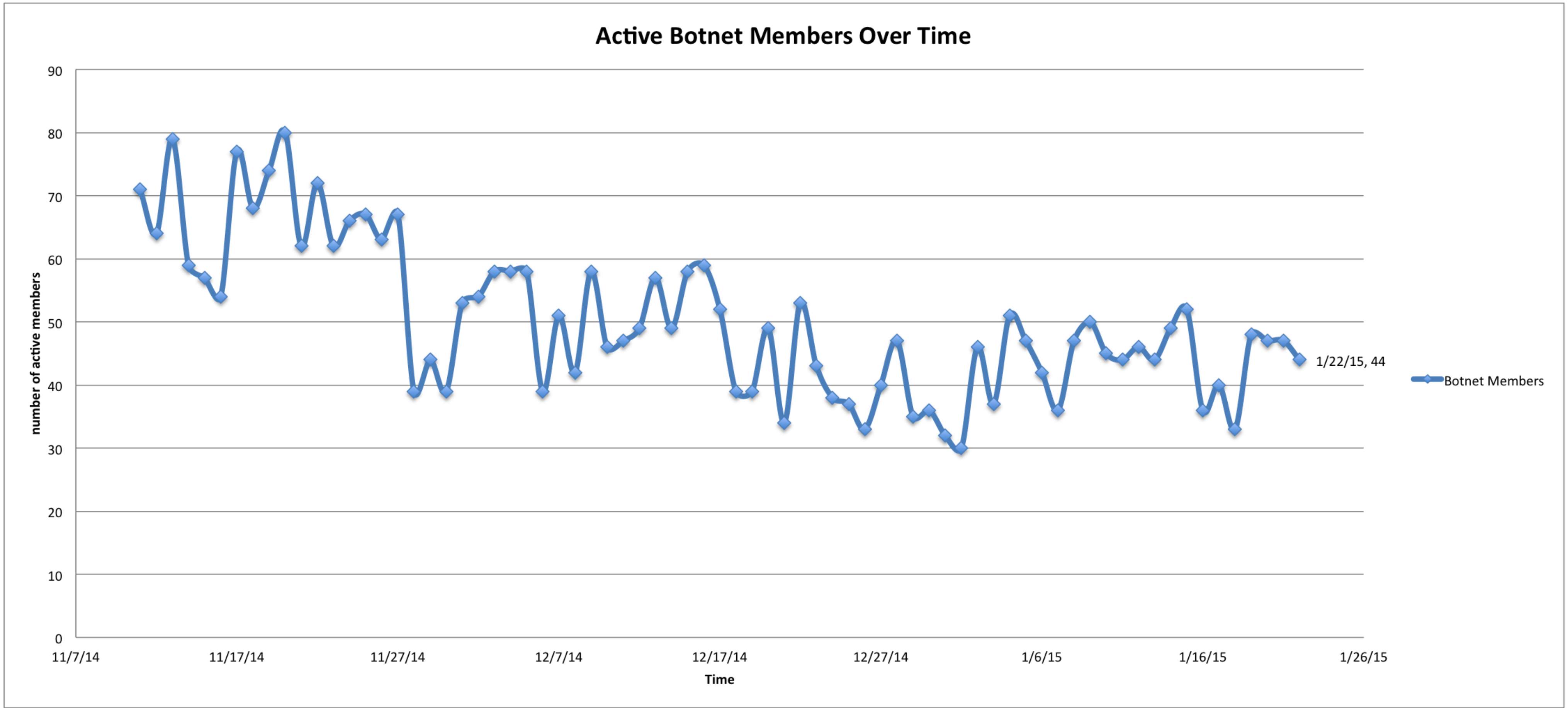
The botnet now contains 1037 members.

All members are compromised public Web servers, mostly running Joomla and WordPress CMS

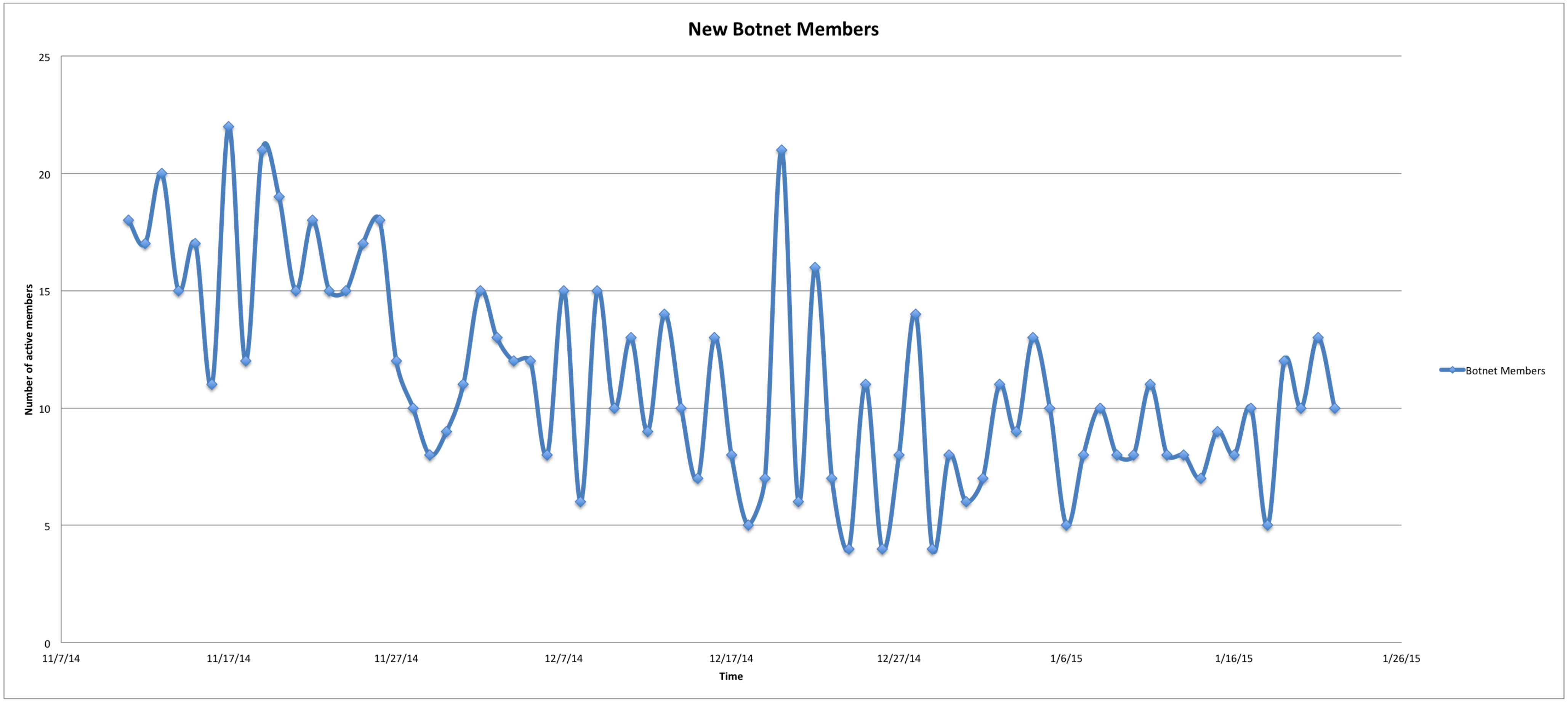
The Botnet has targeted more than 7800 applications over the period

Note – the data is only based on Akamai customers – probably targeted many more applications

Active Members Over Time



New Botnet Members Over Time



Activity Duration of Botnet Members and Evolution

On average, Joomla botnet members spurted malicious traffic over 29 days.

To compare, compromised web servers running other Web platforms, were maliciously active for 10 days on average.

- The reason for the difference between Joomla and the rest of the servers is unclear
- Likely related to the massive exploitation of the Joomla vulnerability

The Botnet evolved over time to attempt to also exploit other vulnerabilities:

- Remote File Inclusion (RFI) on the TimThumb image resizer WordPress module
- Remote Code Execution (RCE) on the Open Flash Chart library

Longevity of Members

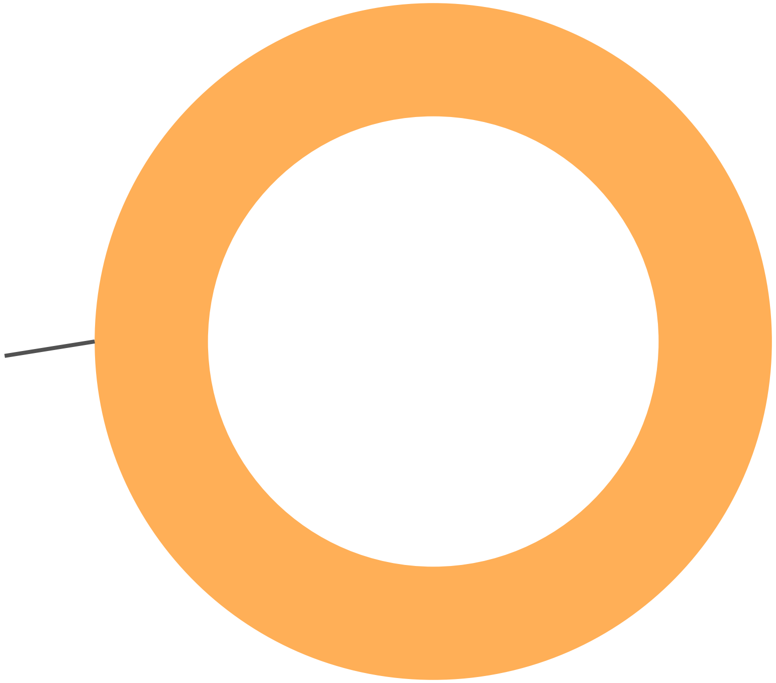
Comparing the active Botnet members from 9 months ago to now

- 43 of the botnet members were also maliciously active 9 months ago.
- 4% of botnet members have not been “cleaned up” for 9 months

Surprising, given that:

- The botnet targets a 3-year old vulnerability. Vulnerable web servers should have been upgraded with newer software ages ago
- The awareness for the usage of this vulnerability in the wild. This is not the first publication of a JCE vulnerability exploitation
- The botnet activity is visible and loud, targeting many applications across the Internet, making it easy to be detected.

Bots on the Akamai Platform



8.01 BILLION

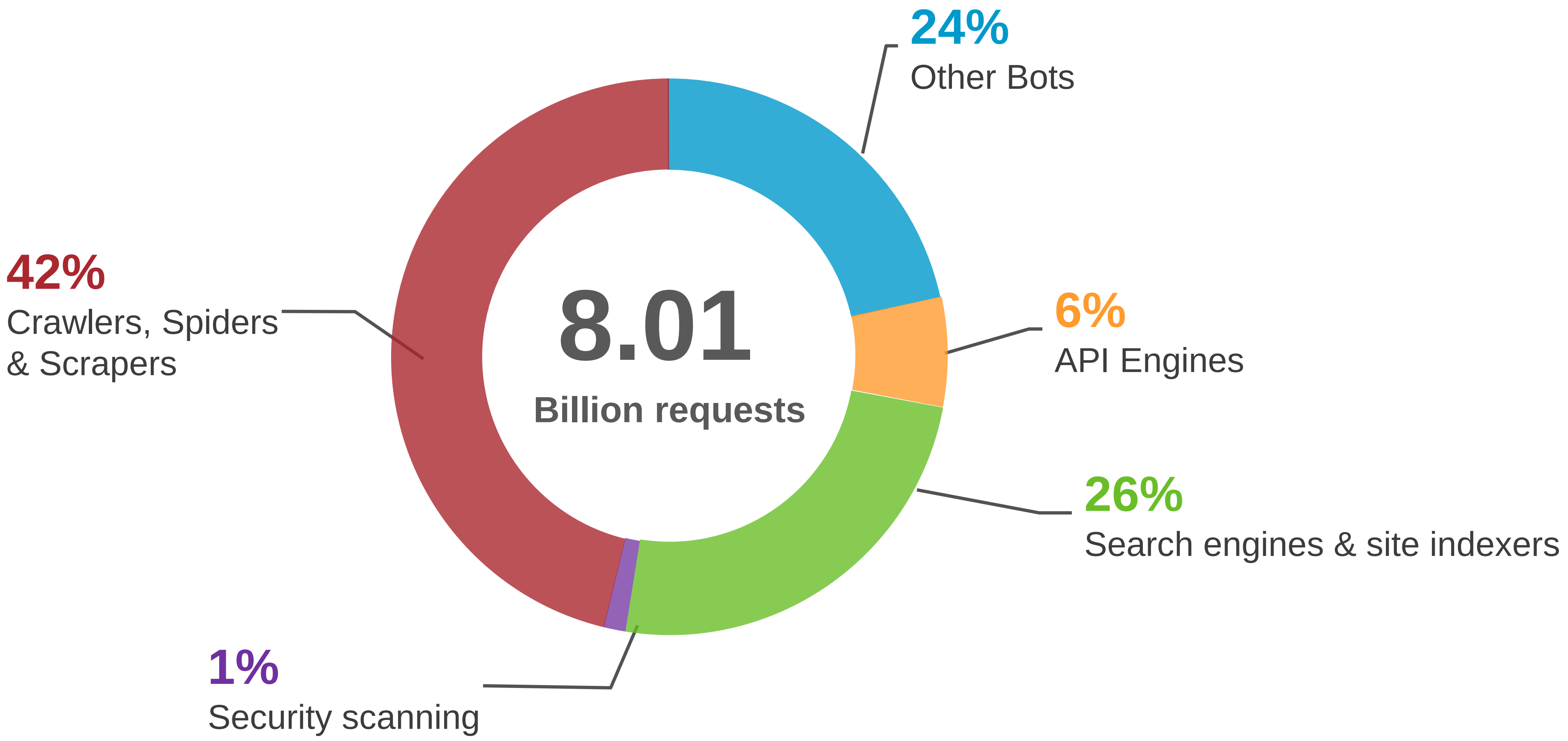
Bot requests in 24-hours

Data Collected
April 1-2, 2015

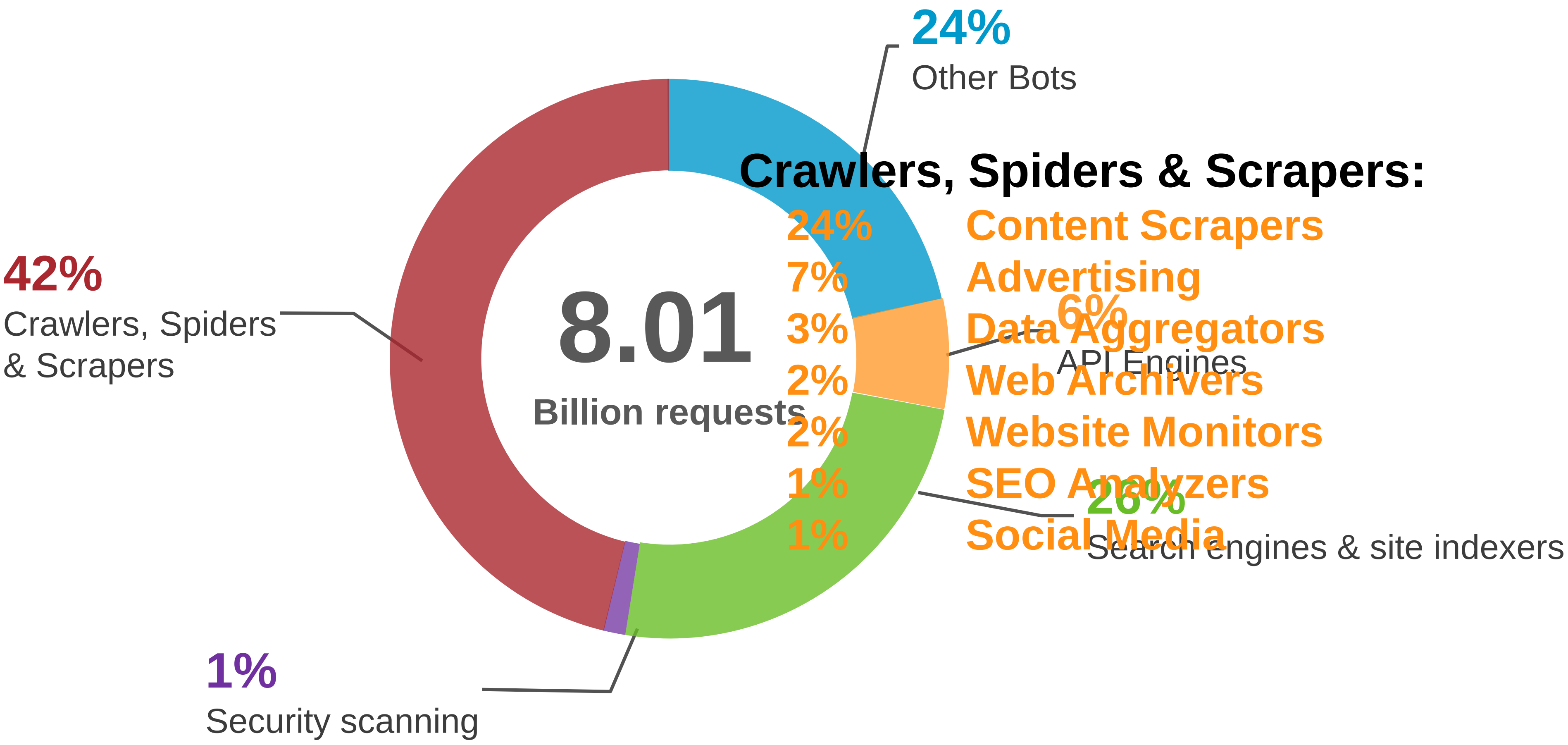
Total Requests:
85,475,034,620

Bots were 9.4% of all requests

Bots on the Akamai Platform



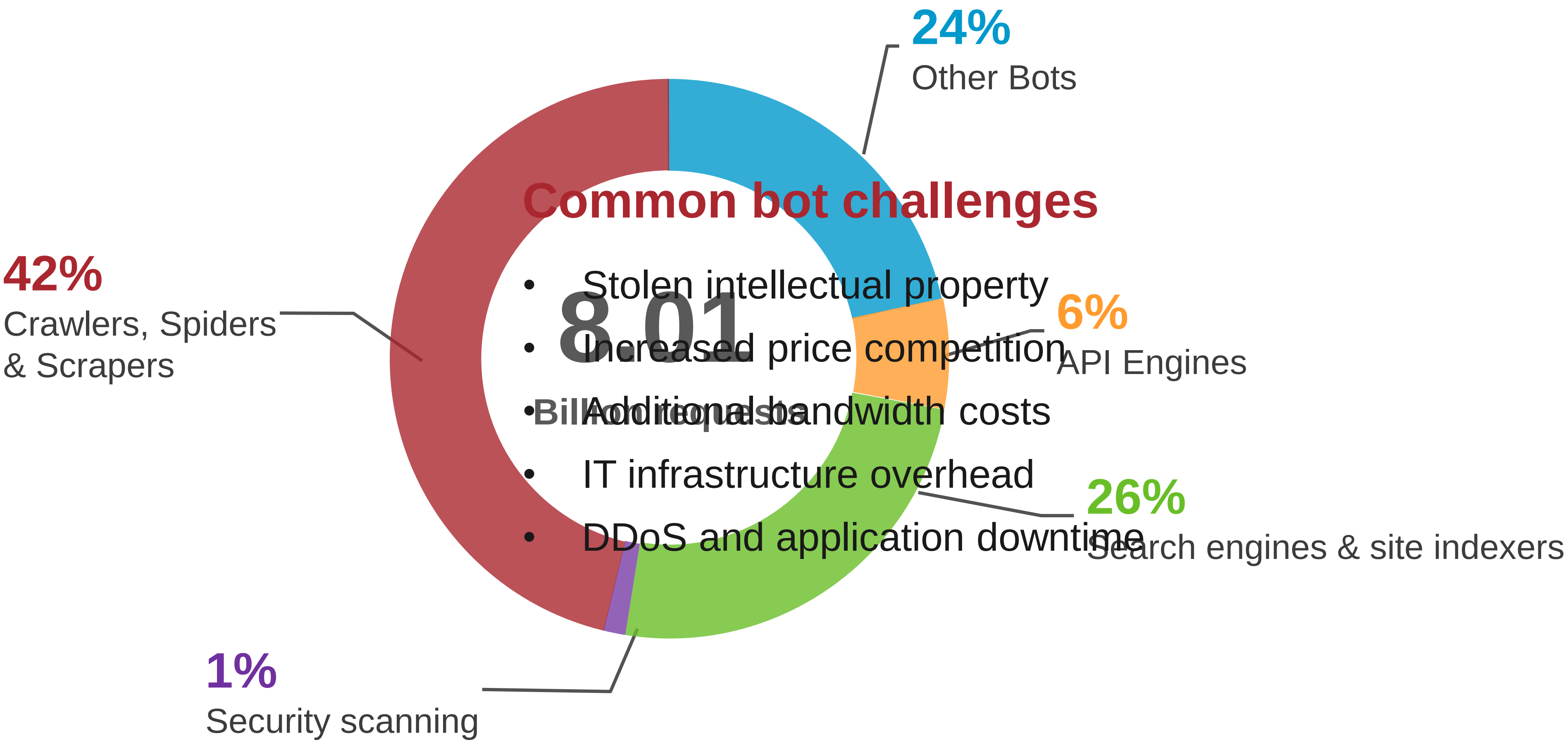
Bots on the Akamai Platform



Crawlers, Spiders & Scrapers:

24%	Content Scrapers
7%	Advertising
3%	Data Aggregators
2%	Web Archivers
2%	Website Monitors
1%	SEO Analyzers
1%	Social Media

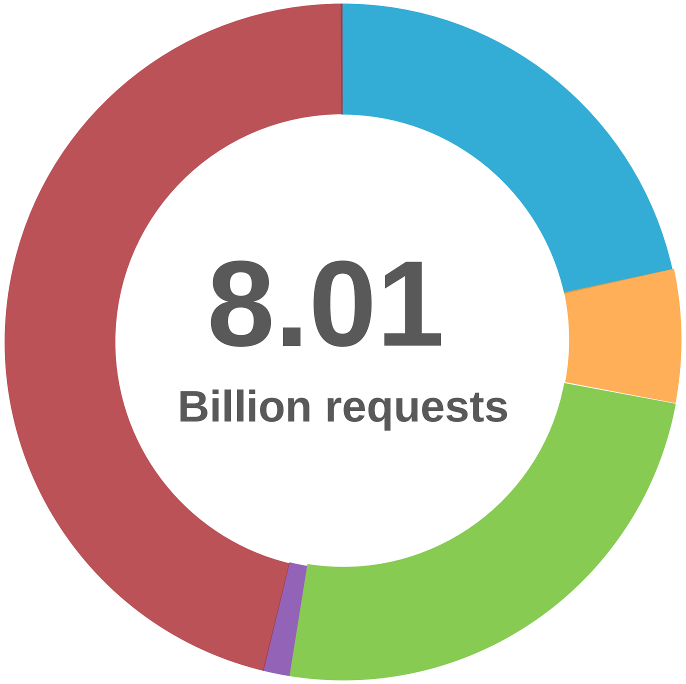
Bots – The Akamai Viewpoint



Common bot challenges

- Stolen intellectual property
- Increased price competition
- Additional bandwidth costs
- IT infrastructure overhead
- DDoS and application downtime

Bots – The Akamai Viewpoint

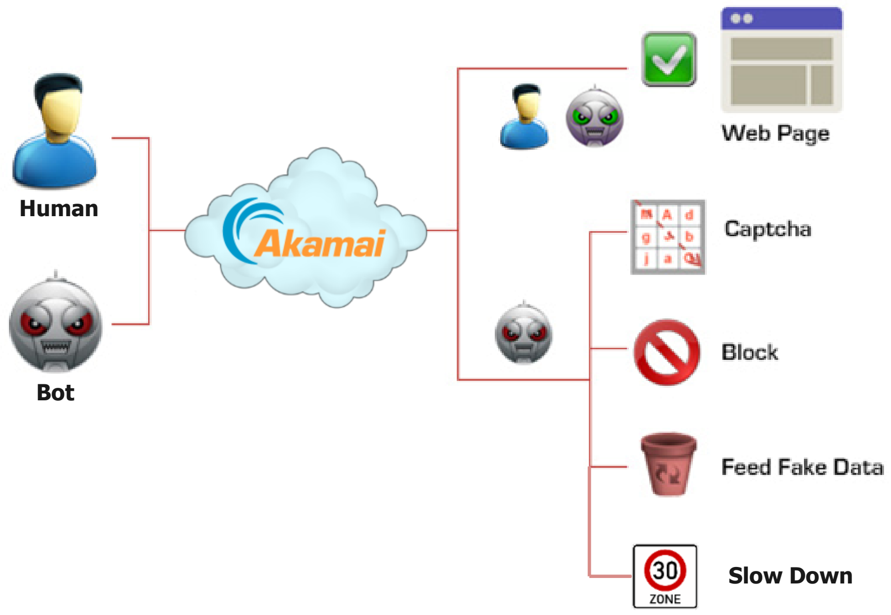


Bot management needs

- Bot detection and identification
- Advanced bot responses
- Report on bot activity and mitigations applied
- Policies to enab le business-level protection

Bot Manager Product Concept

Allow customers to manage the load on their infrastructure from Bots and protect their Web content from being scraped



- ***Detect if human or not***
- ***Manage Good and Bad Bot Traffic***
- ***Business Oriented Policies – Apply actions based on importance of the traffic to business:***
  - ***Slow it down***
  - ***Feed fake / stale data***
  - ***Challenge it***
  - ***Deny it***
  - ***Etc.***

Closing Thoughts

Bots and automation are an increasing problem for the web

Simply exposing a botnet and it’s tactics has little impact

Shutting down members of a Botnet only causes it to breed faster

Effective detection requires many techniques, but especially behavioral analytics

Effective mitigation requires a variety of responses that keep the bot unaware that they have been detected

Akamai

FASTER FORWARD

War Stories from the Cloud: Rise of the Machines

John Summers

VP Security Products