RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CCT-T08

Barbarians at the Gate(way)

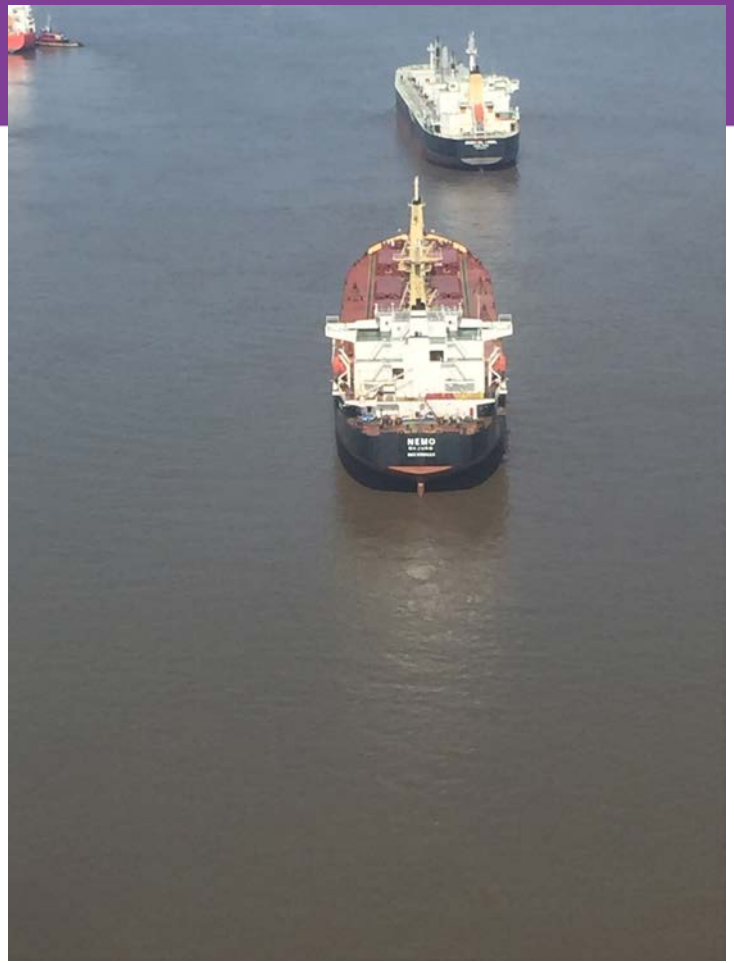
Dave Lewis
Global Security Advocate
Akamai Technologies
@gattaca

#RSAC

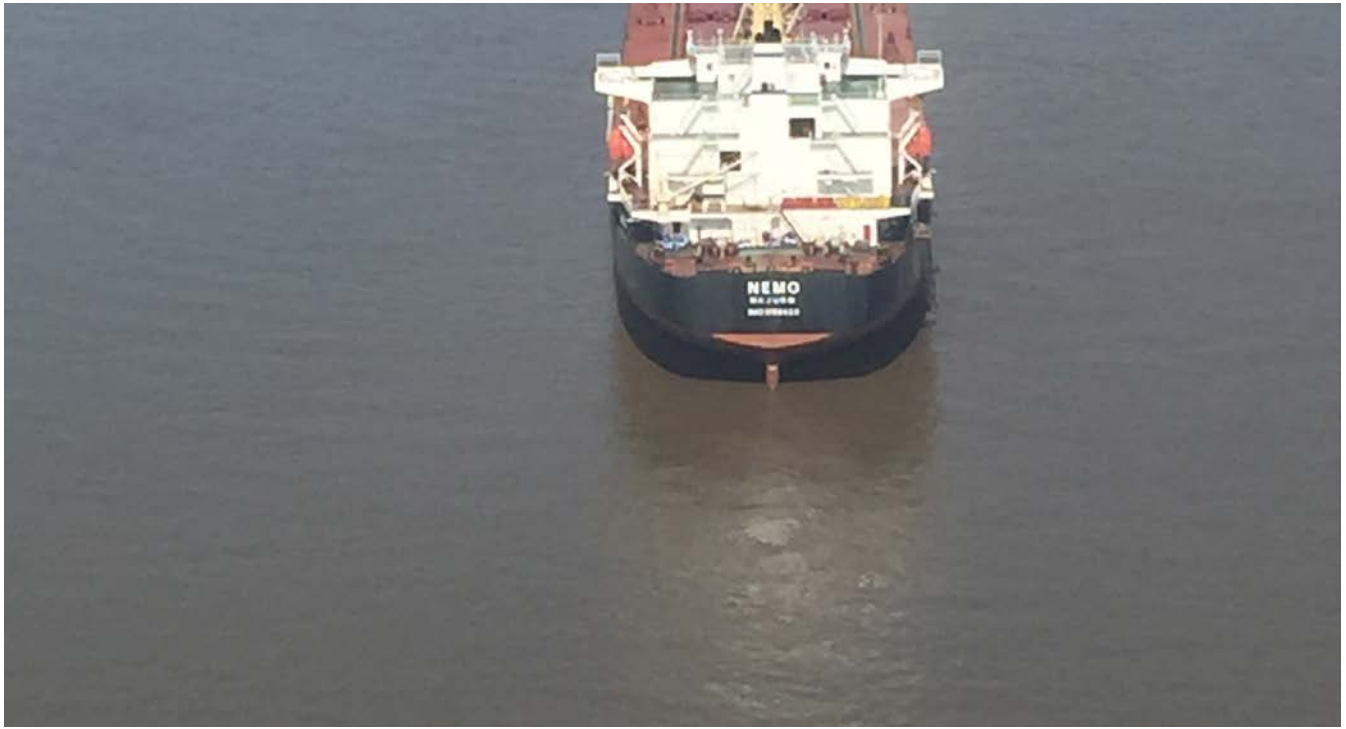
#whoami

Dave Lewis
@gattaca
dave@akamai.com

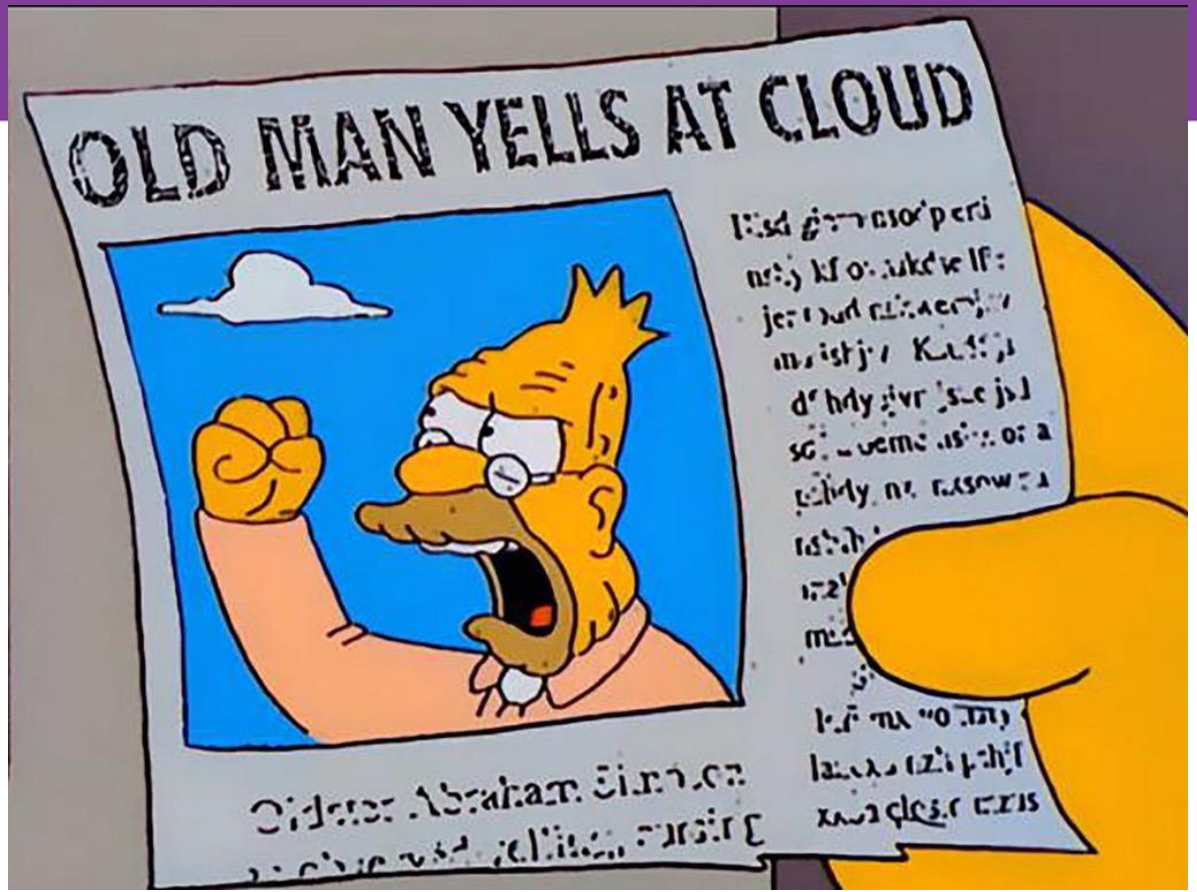

Akamai
FASTER FORWARD

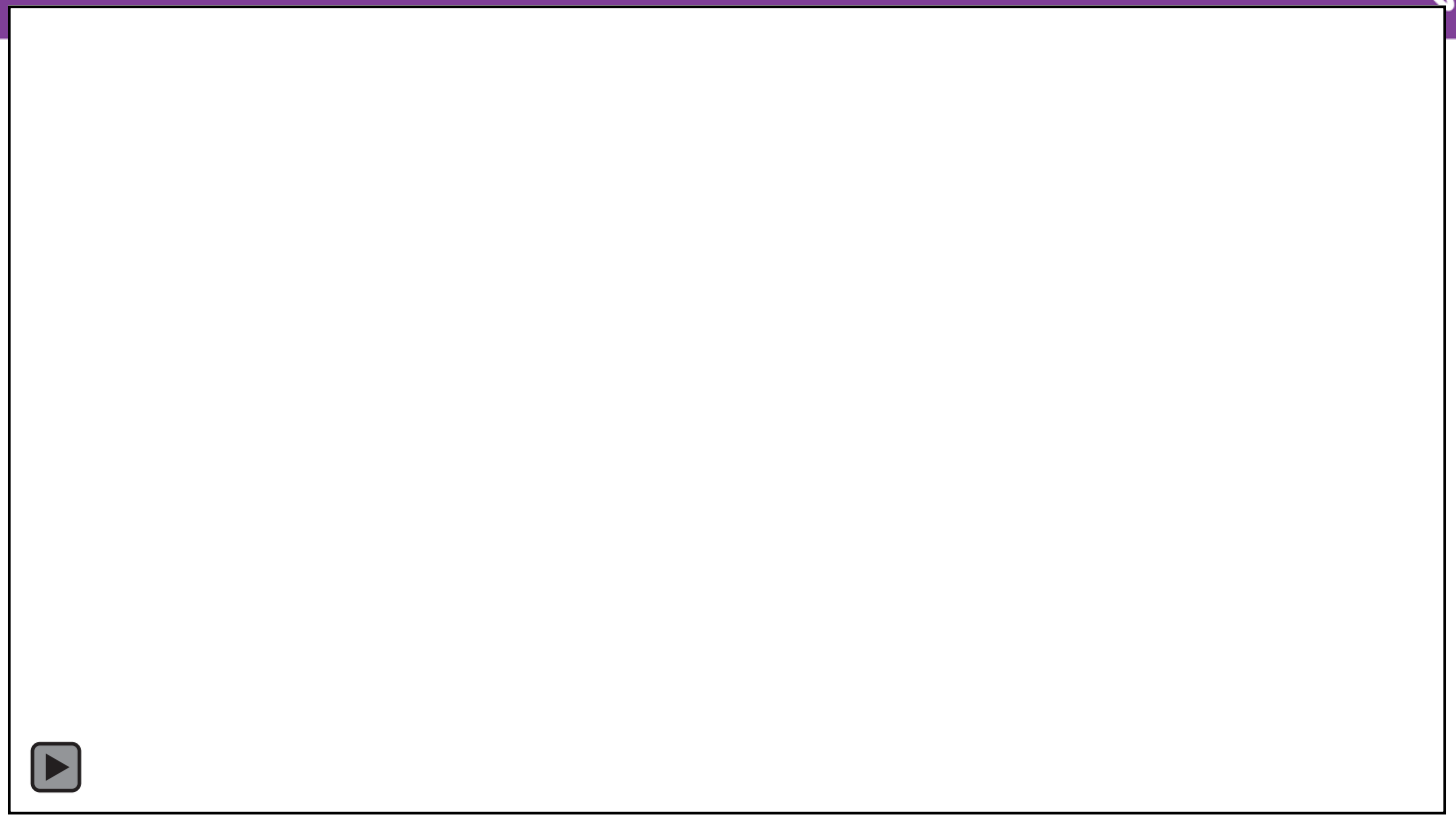

NEMO

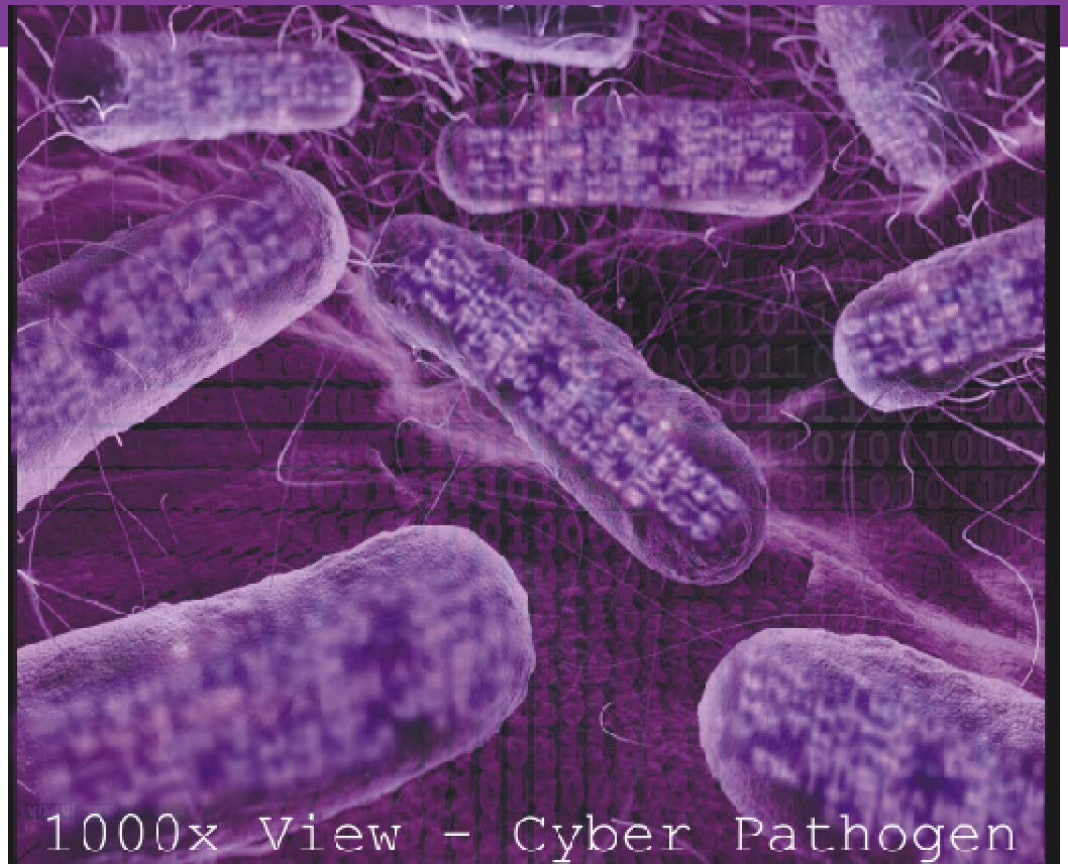
WE FOUND HIM!




NEMO


OLD MAN YELLS AT CLOUD





Akamai

Game Plan

- Actors
- Attacks
- Tools
- Trends
- Data
- Now what?

Current(ish) prices on the Russian underground

- Hacking corporate mailbox: $500
- Winlocker ransomware: $10-20
- Intelligent exploit bundle: $10-$3,000
- Hiring a DDoS attack: $30-$70/day, $1,200/month
- Botnet: $200 for 2,000 bots
- DDoS botnet: $700


HACKERS LIST
Find Hackers
Bid Projects
How It Works
FAQ
Register
Login
Find professional hackers for hire
People need professional hackers for hire. So, we connect people who need professional hackers to professional hackers for hire around the world. Safe, fast and secure Learn how it works.
Browse
OR
Start a Project for Free

Actors: Bored Kids

Akamai

https://www.flickr.com/photos/ardinhasaphotography/8484164608/sizes/l


FREE
Hugs

https://www.flickr.com/photos/sklathill/2255718951/sizes/l

Actors: Nation States

THERE ARE

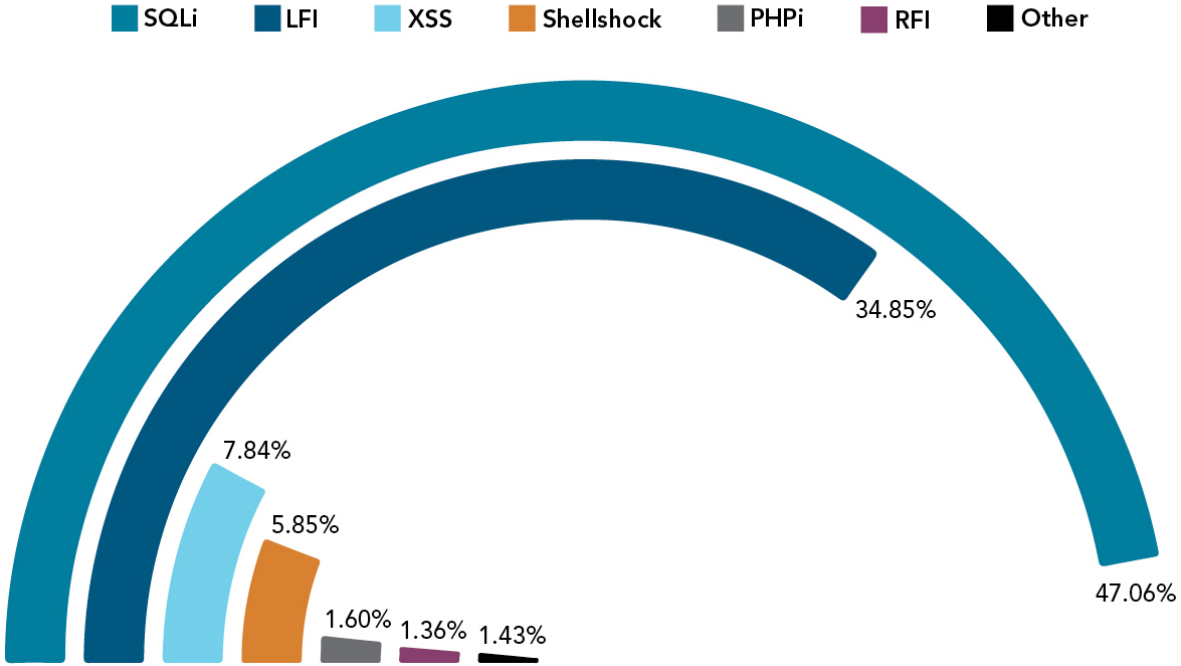
STANDARD VILLAINS

AND THERE ARE

ARCH VILLAINS

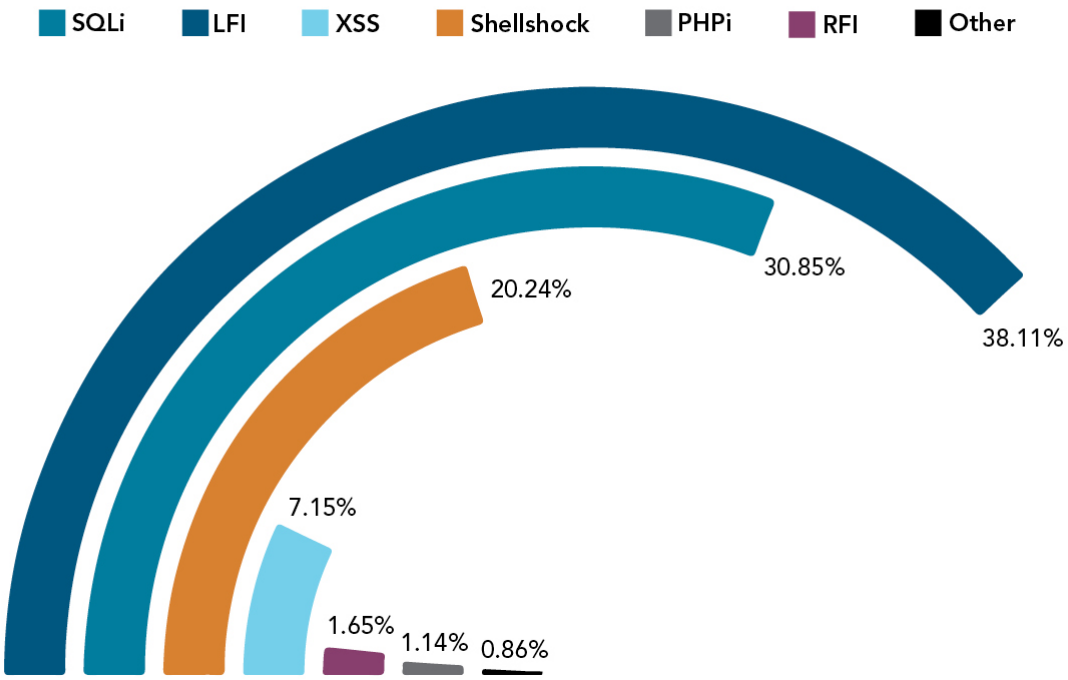
Attacks

Web Application Attack Vectors Over HTTP, Q1 2016



Akamai

Web Application Attack Vectors Over HTTPS, Q1 2016



Akamai

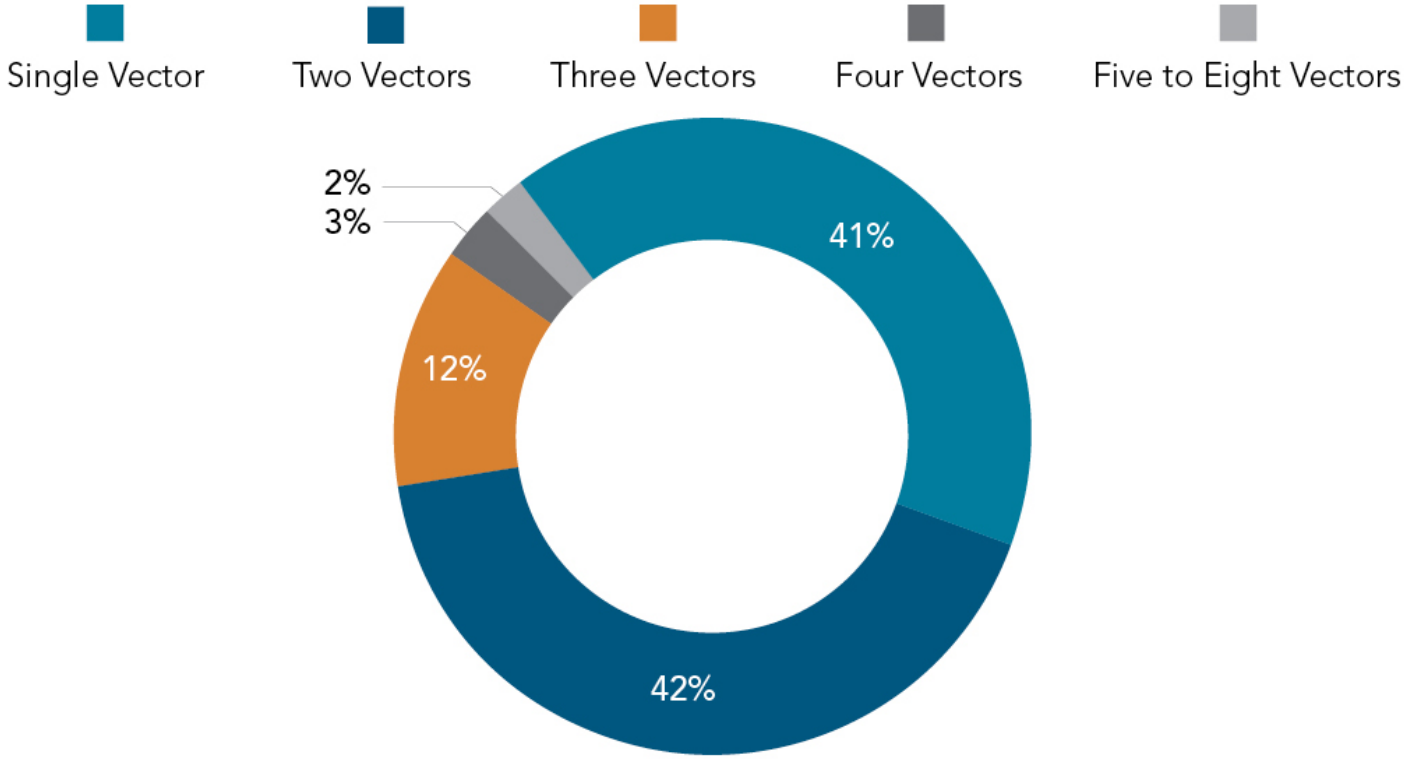
Types of Attacks

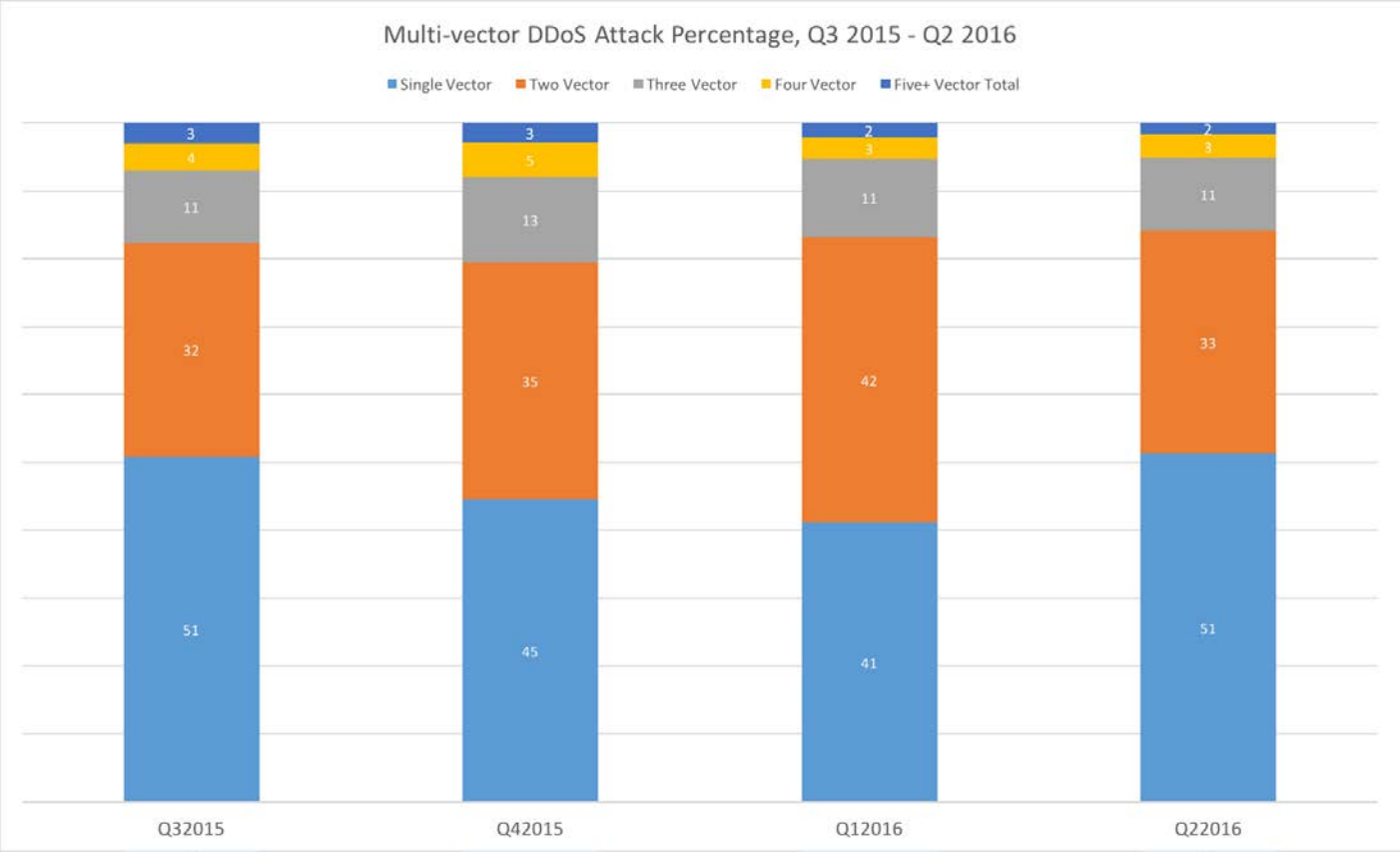
- SYN Floods
- UDP Floods
- ICMP Floods
- NTP Amplification
- HTTP Flood

Akamai

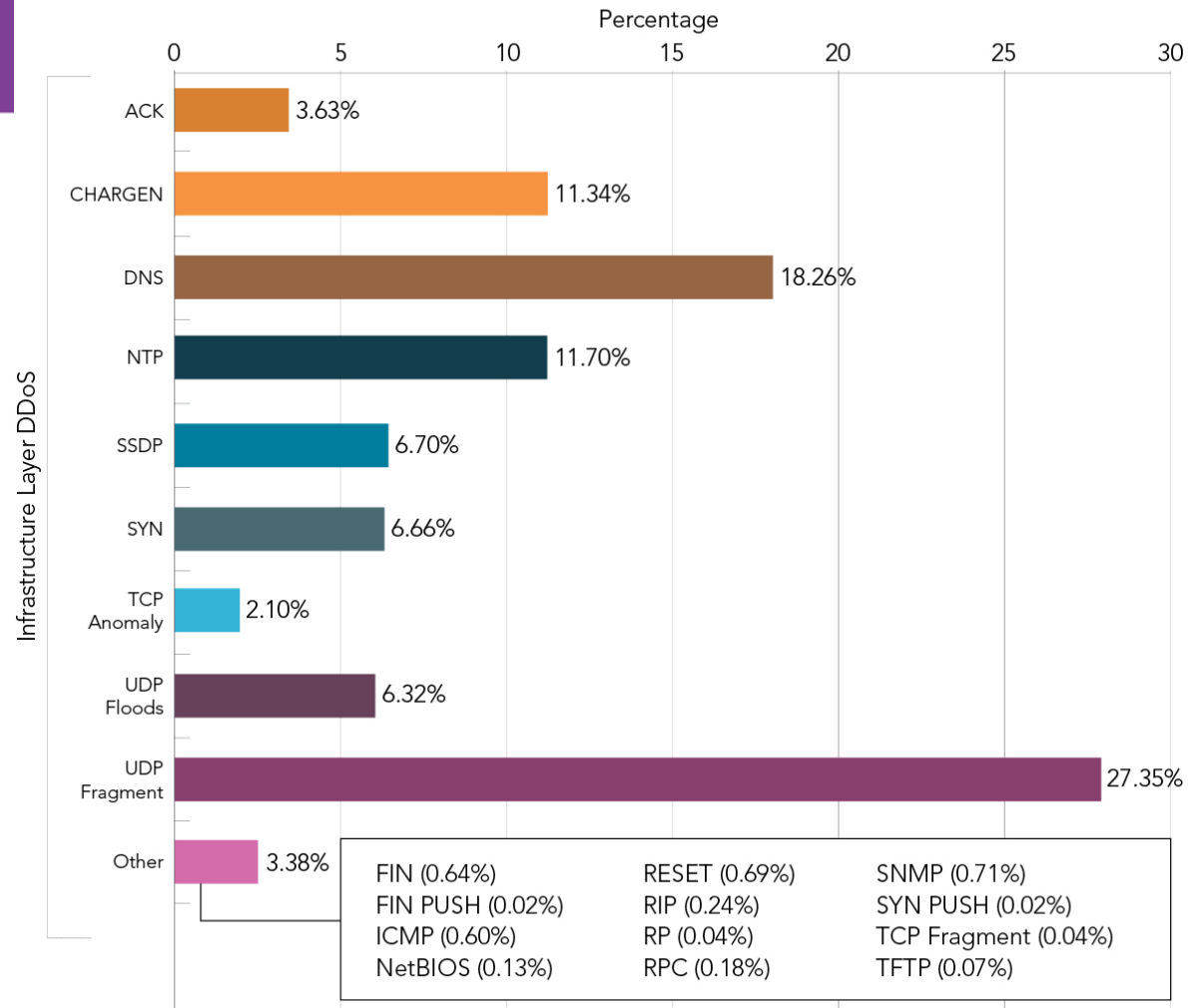
Attacks: Volumetric

Multi-Vector DDoS Attacks, Q1 2016



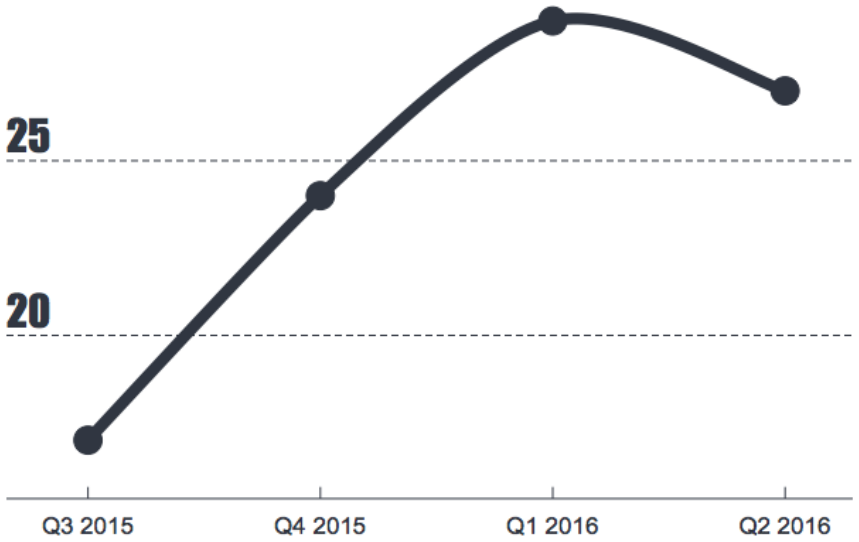

Multi-vector DDoS Attack Percentage, Q3 2015 - Q2 2016
Single Vector
Two Vector
Three Vector
Four Vector
Five+ Vector Total
3
4
11
32
51
3
5
13
35
45
2
3
11
42
41
2
3
11
33
51
Q32015
Q42015
Q12016
Q22016

DDoS Attack Vector Frequency, Q1 2016



Akamai

Average Number of DDoS Attacks Per Target



Top target organization attack count Q2 2016

373

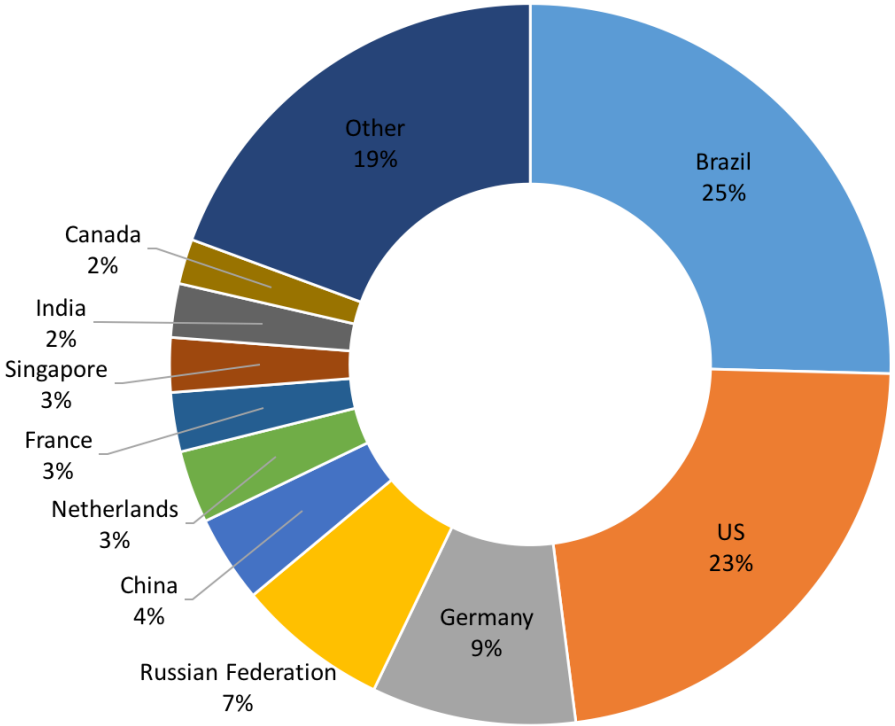
Average Number by Quarter

Q3 2015 - 17
Q4 2015 - 24
Q1 2016 - 29
Q2 2016 - 27

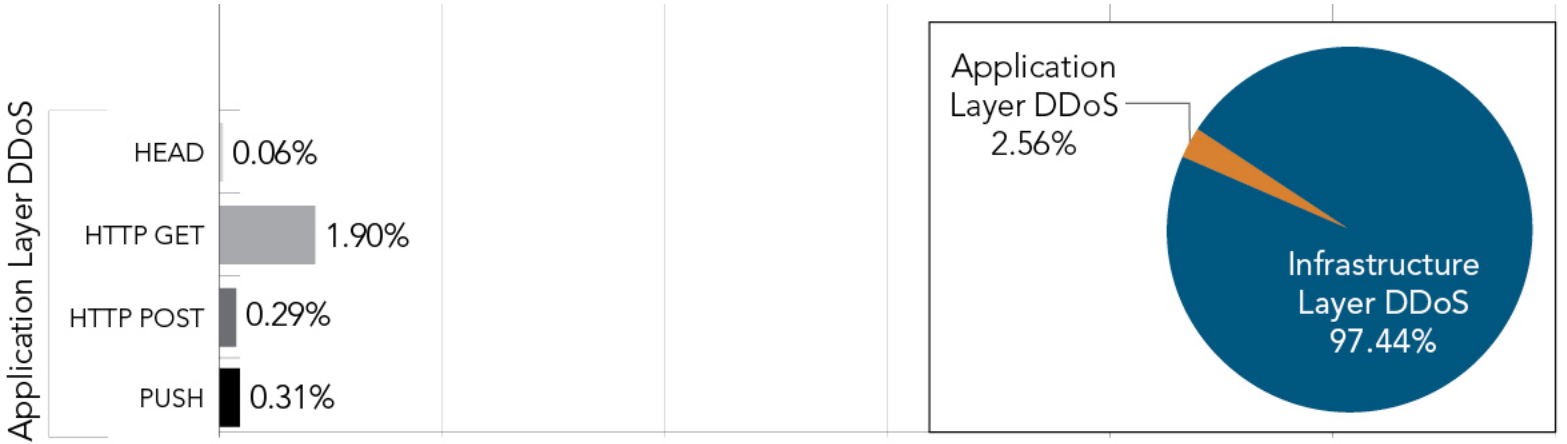
Akamai

Attacks: Application Layer

Top 10 Source Countries for Web Application Attacks, Q2 2016

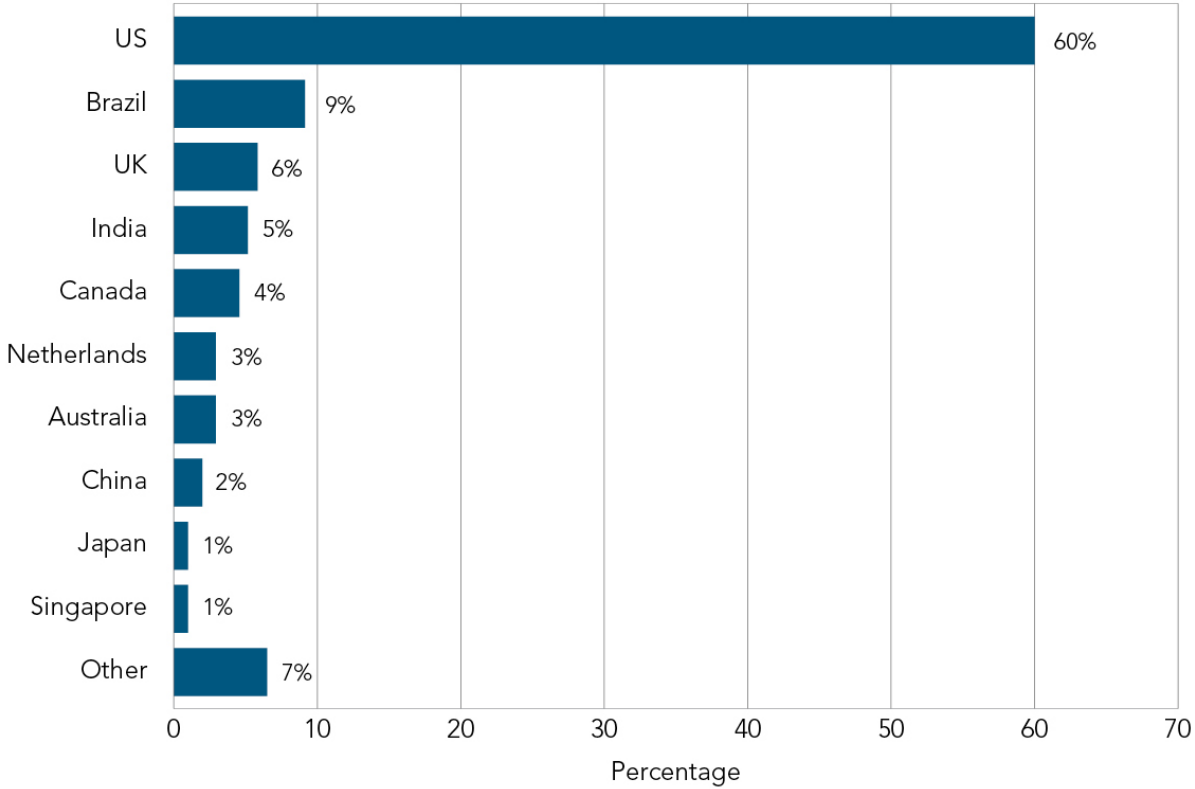


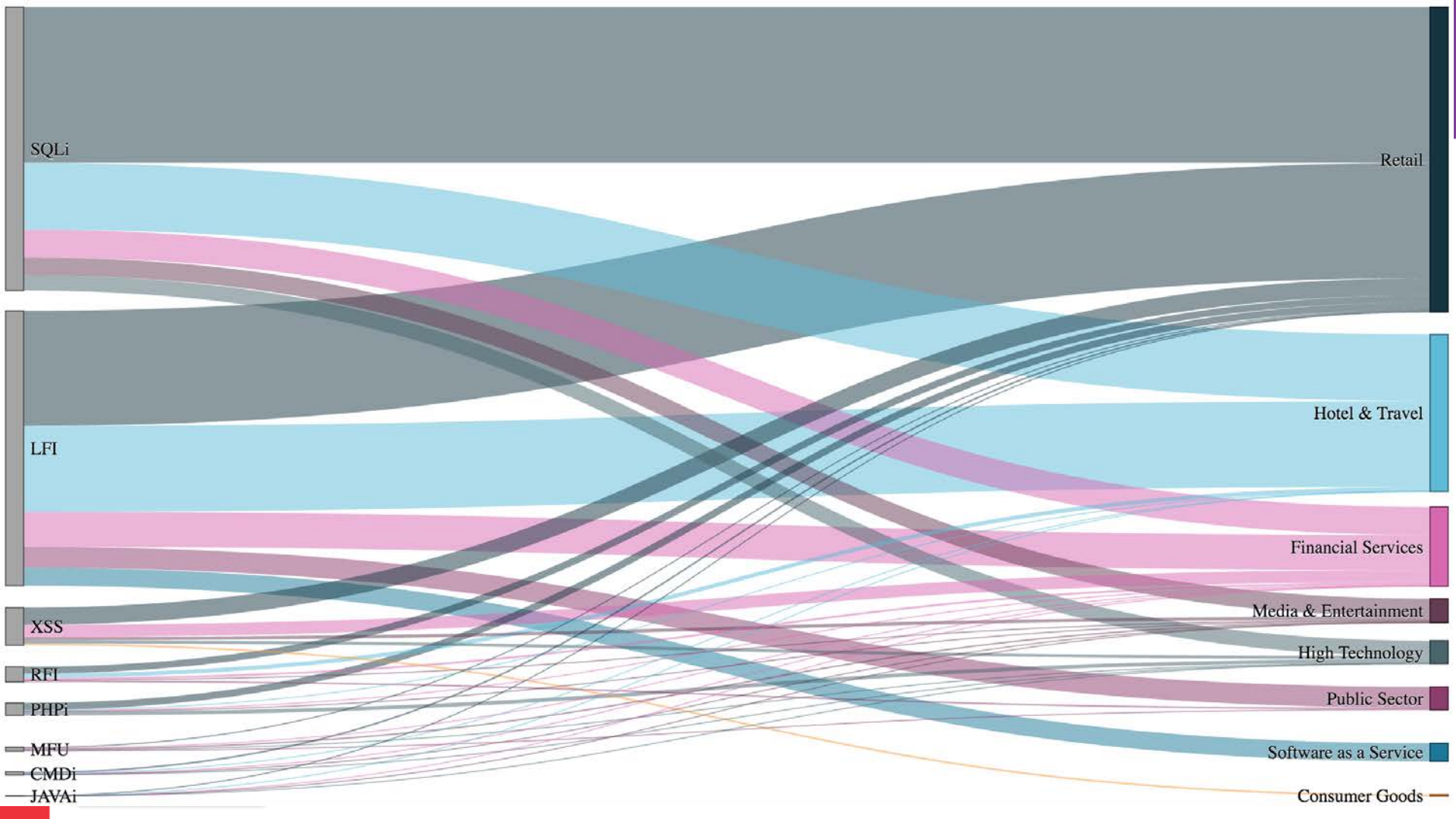
Application Layer DDoS



Akamai

Top 10 Target Countries for Web Application Attacks, Q1 2016




SQLi
LFI
XSS
RFI
PHPi
MFU
CMDi
JAVAi
Retail
Hotel & Travel
Financial Services
Media & Entertainment
High Technology
Public Sector
Software as a Service
Consumer Goods

Attacks: Extortion

DD4BC

- Began by targeting sites with ransom demands
- Failure to pay lead to increased $$$ to stop the attack
- Earlier attacks focused on businesses that would avoid reporting the attacks to law enforcement.
- Once research published they relocated their campaigns to APAC

-----Original Message-----
From: DD4BC Team [mailto:dd4bc@[redacted]]
Sent: June-25-15 11:48 AM
To: XXXXX
Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:

http://www.[redacted].com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks/

http://[redacted]:com/bitalo.html

http://[redacted]/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info

Or just google "DD4BC" and you will find more info.

So, it's your turn!

All your servers are going under DDoS attack unless you pay 30 Bitcoin.

- DD4BC continues to inform victims that they will launch a DDoS attack of 400-500 Gbps against them.
- To date, DD4BC attack campaigns mitigated by Akamai have not exceeded 50 Gbps in size.
- That's up from the high of 15-20 Gbps observed

January 14, 2016

'Key member' of DD4BC arrested in international crackdown

Share this article:

The cyber-extortionist gang DD4BC has reportedly suffered a blow as one of the group's key members was arrested and another detained this week in a worldwide crackdown.

International police say they are closing in on suspects believed to be behind cyber-crime rascals DD4BC. One 'main target' of the cyber-gang has been arrested with another kept in detention in a global campaign to take down the group.

One arrested and one detained in DD4BC investigation

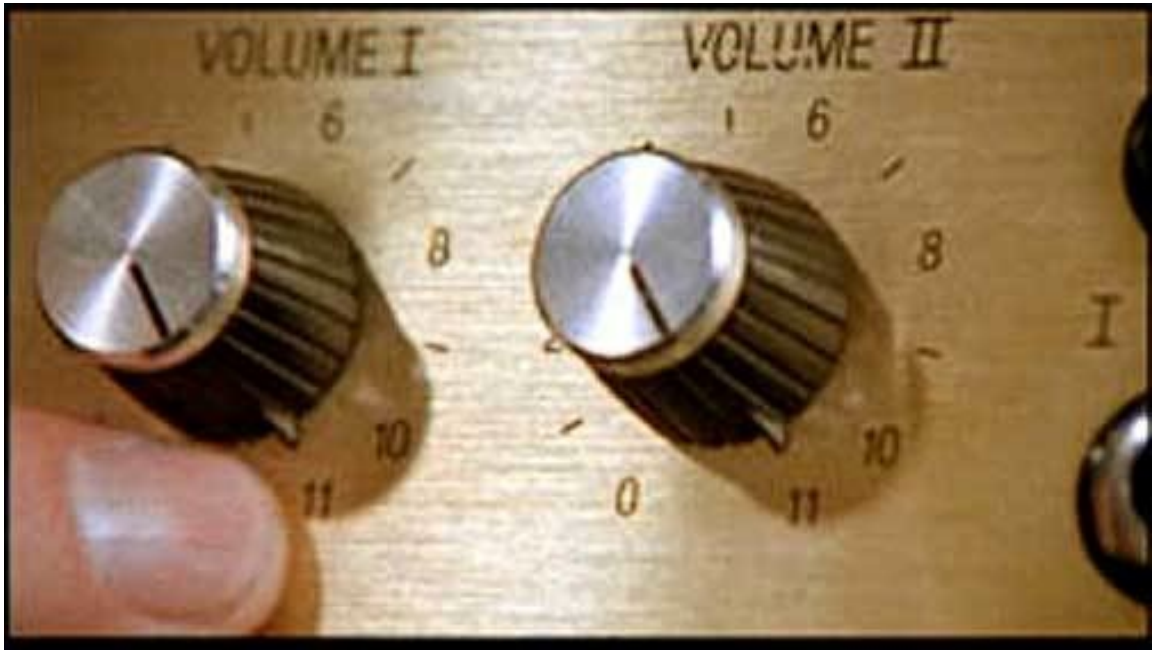
Police working under Operation Pleiades, named for the seven sisters of Greek myth, busted in on the suspects earlier this week. According to Europol, this particular taskforce, initiated by Austria, was supported by law enforcement agencies from all over the world including Japan, France, Australia, Romania, Switzerland and the USA.

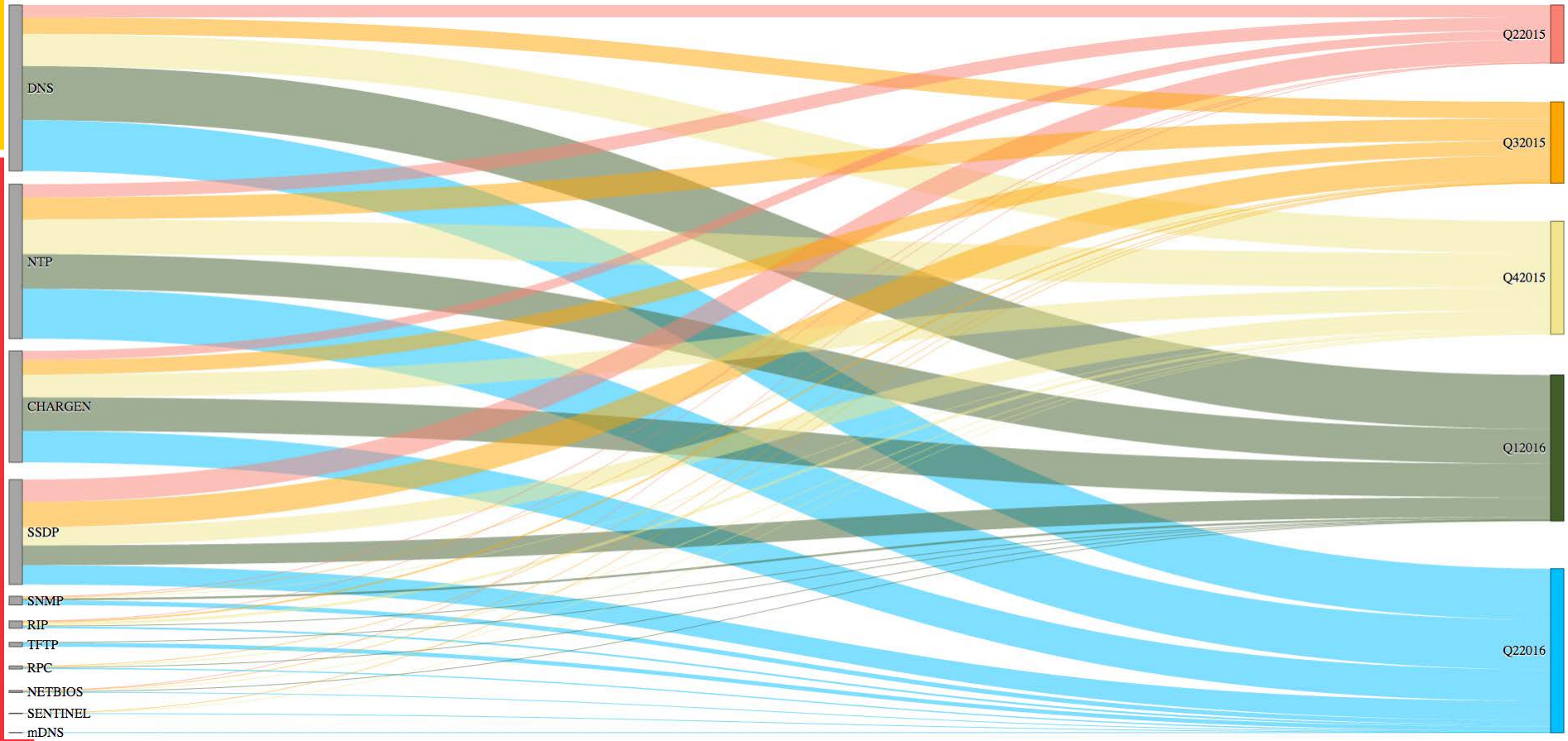
Alleged top members of DD4BC were identified by the UK's Metropolitan Police Cyber Crime Unit as living in Bosnia Herzegovina.

DD4BC, Armada Collective, and the Rise of Cyber Extortion

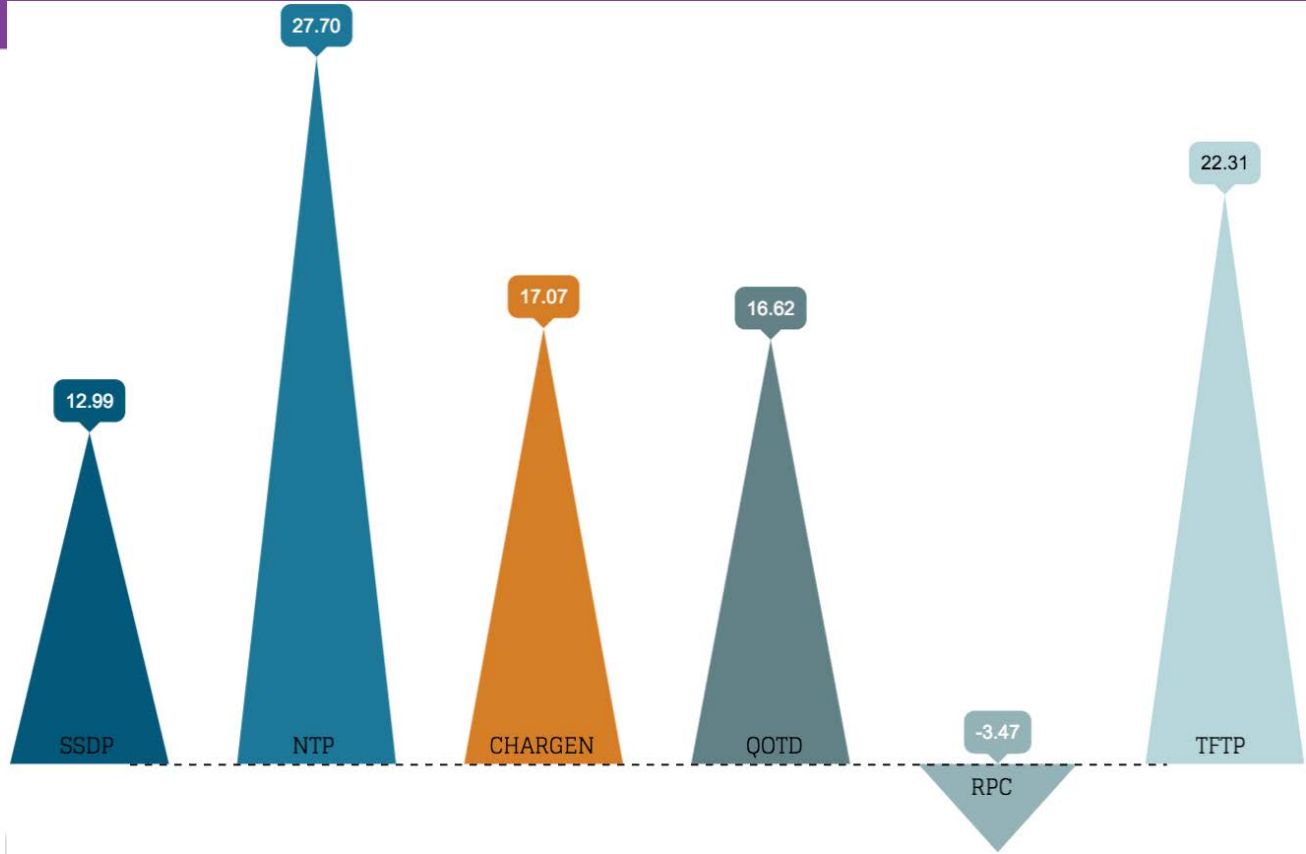
DD4BC, a group that named itself after its extortion method of choice — DDoS "4" Bitcoin — has attacked over 140 companies since its emergence in 2014. Other groups, inspired by their success, are

Attacks: Amplification



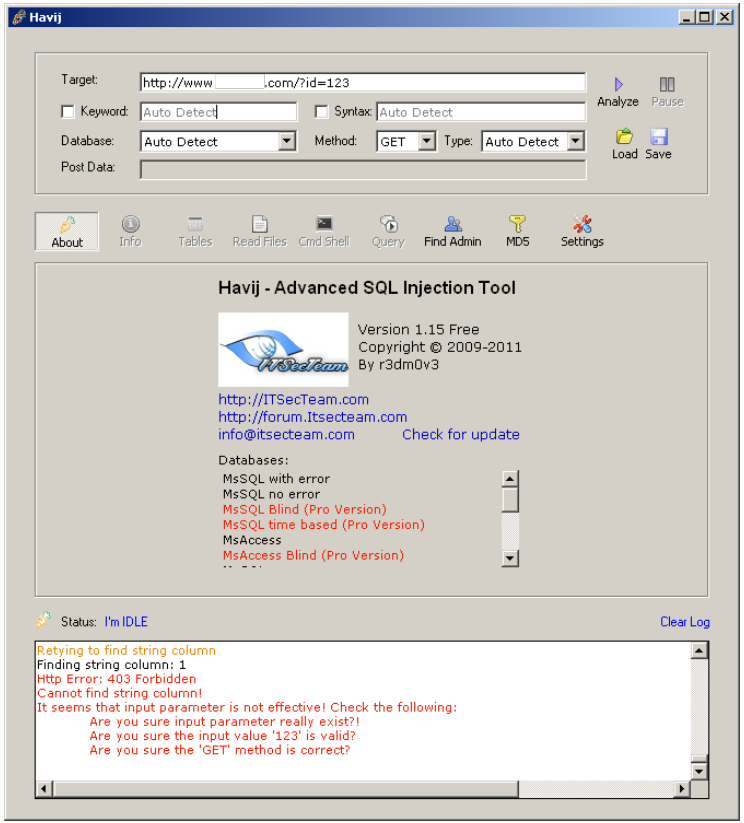

DNS
NTP
CHARGEN
SSDP
SNMP
RIP
TFTP
RPC
NETBIOS
SENTINEL
mDNS
Q22015
Q32015
Q42015
Q12016
Q22016

Akamai

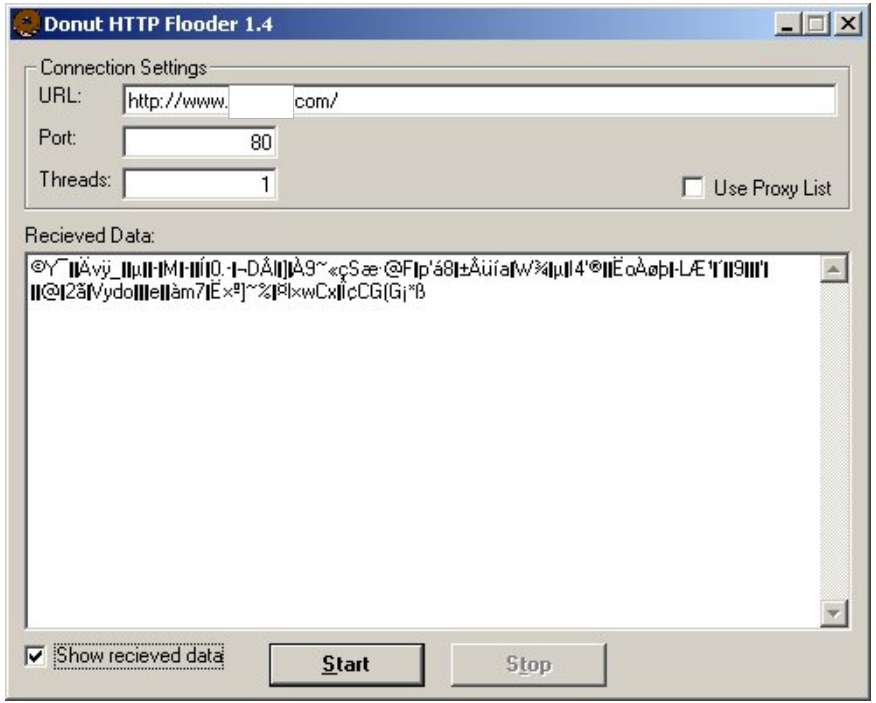

27.70
22.31
17.07
16.62
12.99
-3.47
SSDP
NTP
CHARGEN
QOTD
RPC
TFTP

Tools

Tools: Havij


Havij
Target:
http://www.com/?id=123
Keyword:
Auto Detect
Syntax:
Auto Detect
Database:
Auto Detect
Method:
GET
Type:
Auto Detect
Post Data:
Analyze
Pause
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.15 Free
Copyright © 2009-2011
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Databases:
MsSQL with error
MsSQL no error
MsSQL Blind (Pro Version)
MsSQL time based (Pro Version)
MsAccess
MsAccess Blind (Pro Version)
Status: I'm IDLE
Clear Log
Retying to find string column
Finding string column: 1
Http Error: 403 Forbidden
Cannot find string column!
It seems that input parameter is not effective! Check the following:
Are you sure input parameter really exist?!
Are you sure the input value '123' is valid?
Are you sure the 'GET' method is correct?

Tools: Donut


Donut HTTP Flooder 1.4
Connection Settings
URL:
http://www.
com/
Port:
80
Threads:
1
Use Proxy List
Recieved Data:
Show recieved data
Start
Stop

Tools: Donut (con't)

GET / HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-powerpoint, application/vnd.ms-excel, */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)

Host: www.foo.bar

Connection: Close

Tools: HULK

Tools: HULK (con't)

GET /?NJB=VURZQ HTTP/1.1

Accept-Encoding: identity

Host: www.foo.bar

Keep-Alive: 112

User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

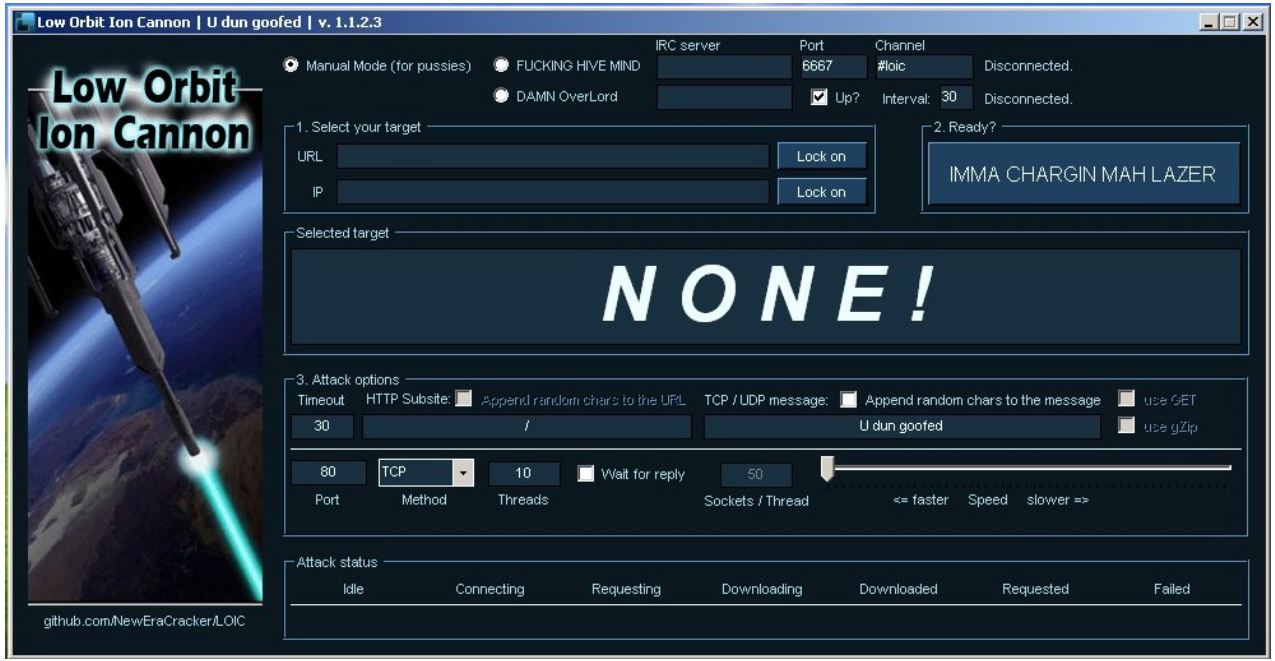
Connection: close

Referer: http://www.foo.bar

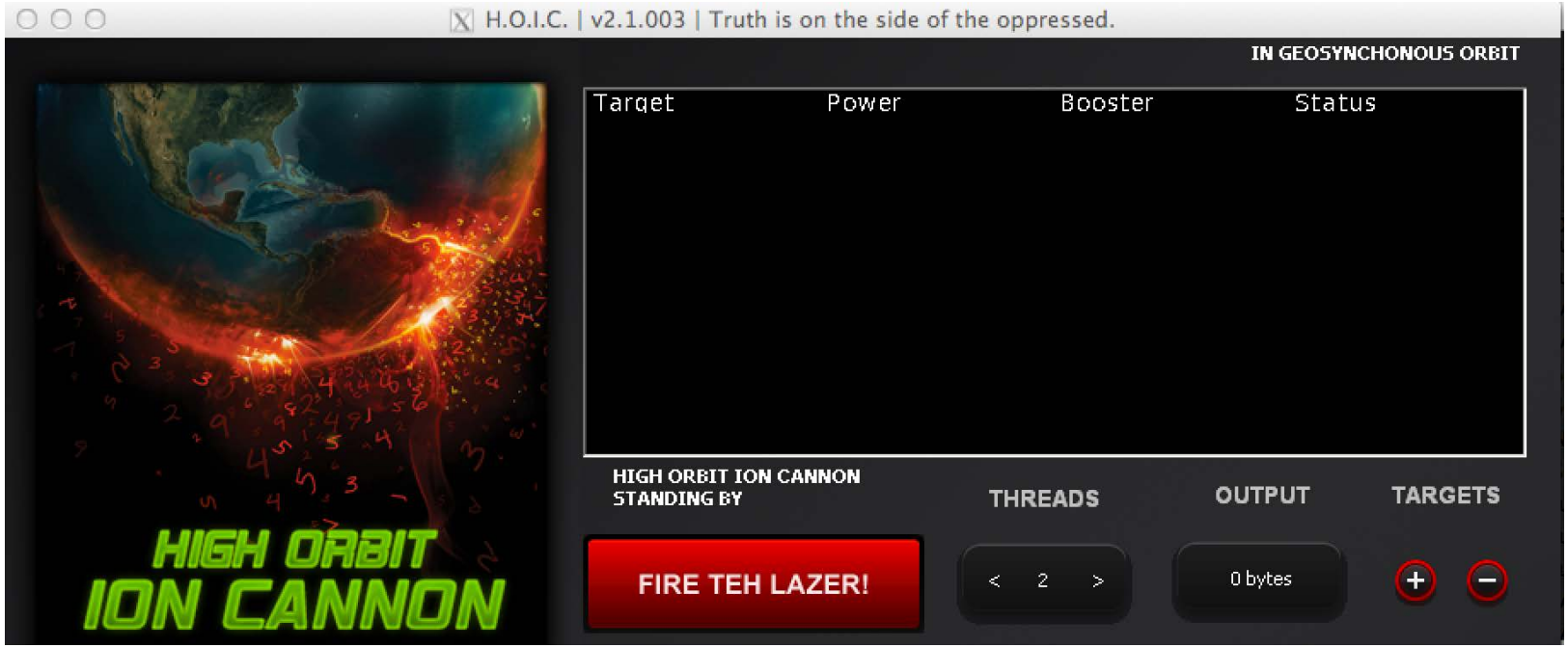
Cache-Control: no-cache

Akamai

Tools: LOIC


Low Orbit Ion Cannon | U dun goofed | v. 1.1.2.3
Low Orbit Ion Cannon
github.com/NewEraCracker/LOIC
Manual Mode (for pussies)
FUCKING HIVE MIND
DAMN OverLord
IRC server
Port
6667
Channel
#loic
Disconnected.
Up?
Interval:
30
Disconnected.
1. Select your target
URL
Lock on
IP
Lock on
2. Ready?
IMMA CHARGIN MAH LAZER
Selected target
NONE!
3. Attack options
Timeout
30
HTTP Subsite:
Append random chars to the URL
/
TCP / UDP message:
Append random chars to the message
U dun goofed
use GET
use gZip
80
Port
TCP
Method
10
Threads
Wait for reply
50
Sockets / Thread
<= faster
Speed
slower =>
Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested
Failed

Tools: HOIC


H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.
IN GEOSYNCHONOUS ORBIT
Target
Power
Booster
Status
HIGH ORBIT ION CANNON
HIGH ORBIT ION CANNON
STANDING BY
THREADS
OUTPUT
TARGETS
FIRE TEH LAZER!
< 2 >
0 bytes

Tools: Brobot

Brobot is a PHP trojan that allows an attacker to take control of a victim's compromised hosted Web server and use it to launch DDOS attacks.

Tools: Mirai

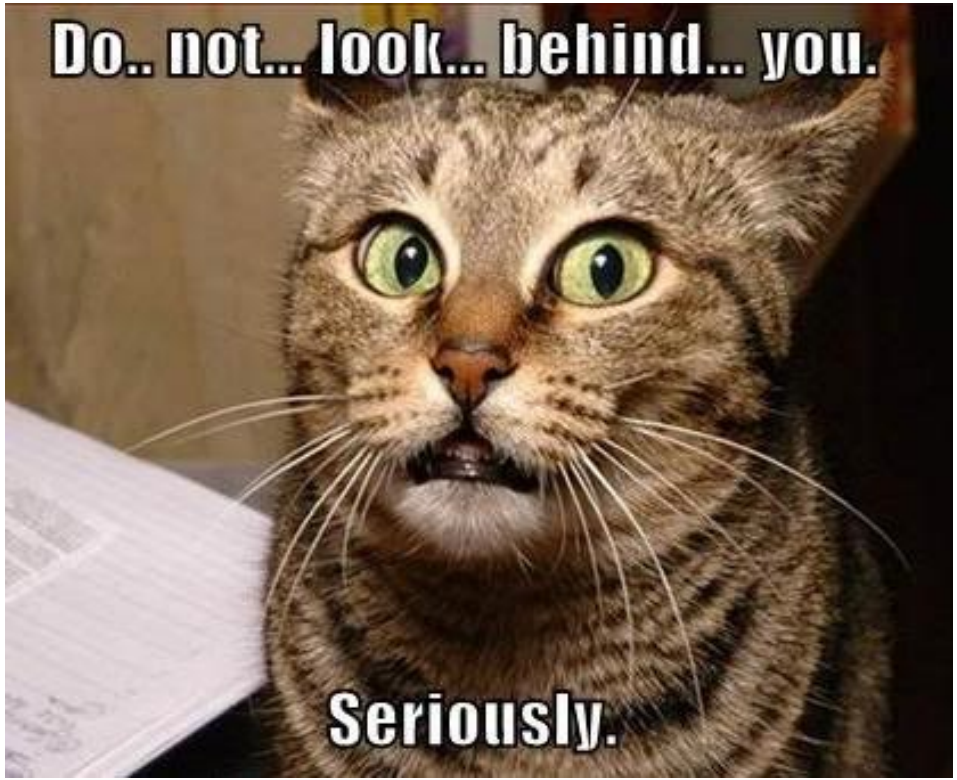
```
var loggedIn bool
var userInfo AccountInfo
if loggedIn, userInfo = database.TryLogin(username, password); !loggedIn {
    this.conn.Write([]byte("\r\033[32;1mпроизошла неизвестная ошибка\r\n"))
    this.conn.Write([]byte("\033[31mнажмите любую клавишу для выхода. (any key)\033[0m"))
    buf := make([]byte, 1)
    this.conn.Read(buf)
    return
}

this.conn.Write([]byte("\r\n\033[0m"))
this.conn.Write([]byte("[+] DDOS | Succesfully hijacked connection\r\n"))
time.Sleep(250 * time.Millisecond)
this.conn.Write([]byte("[+] DDOS | Masking connection from utmp+wtmp...\r\n"))
time.Sleep(500 * time.Millisecond)
this.conn.Write([]byte("[+] DDOS | Hiding from netstat...\r\n"))
time.Sleep(150 * time.Millisecond)
this.conn.Write([]byte("[+] DDOS | Removing all traces of LD_PRELOAD...\r\n"))
for i := 0; i < 4; i++ {
```

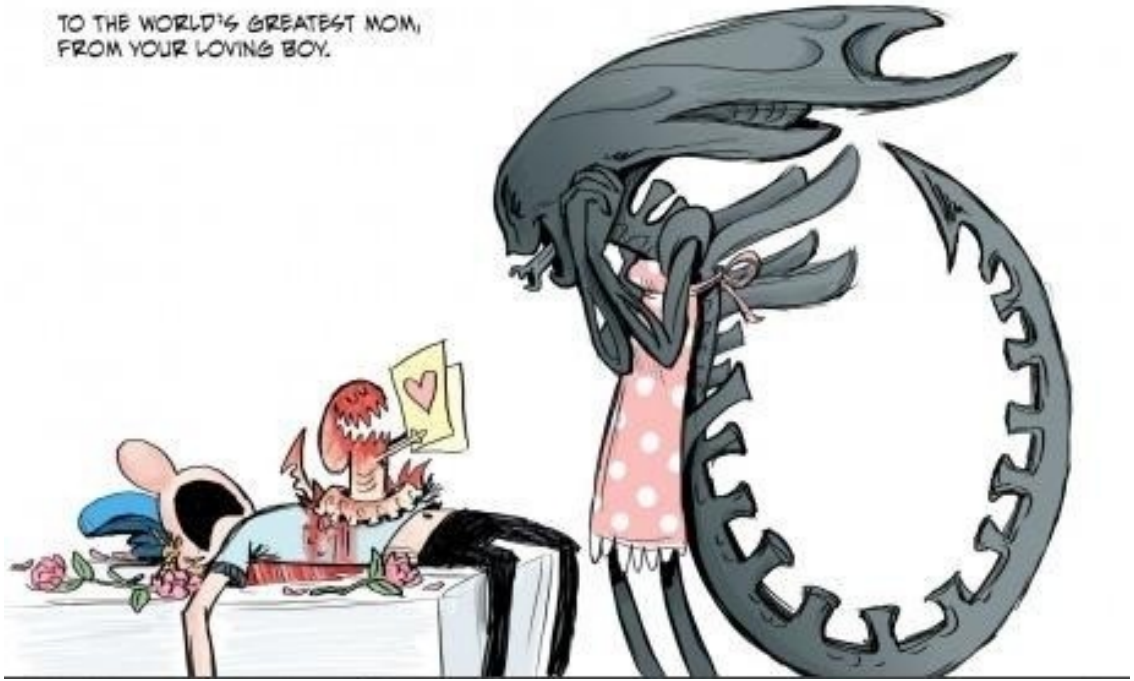
Akamai

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                      // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                          // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin    admin1234
```

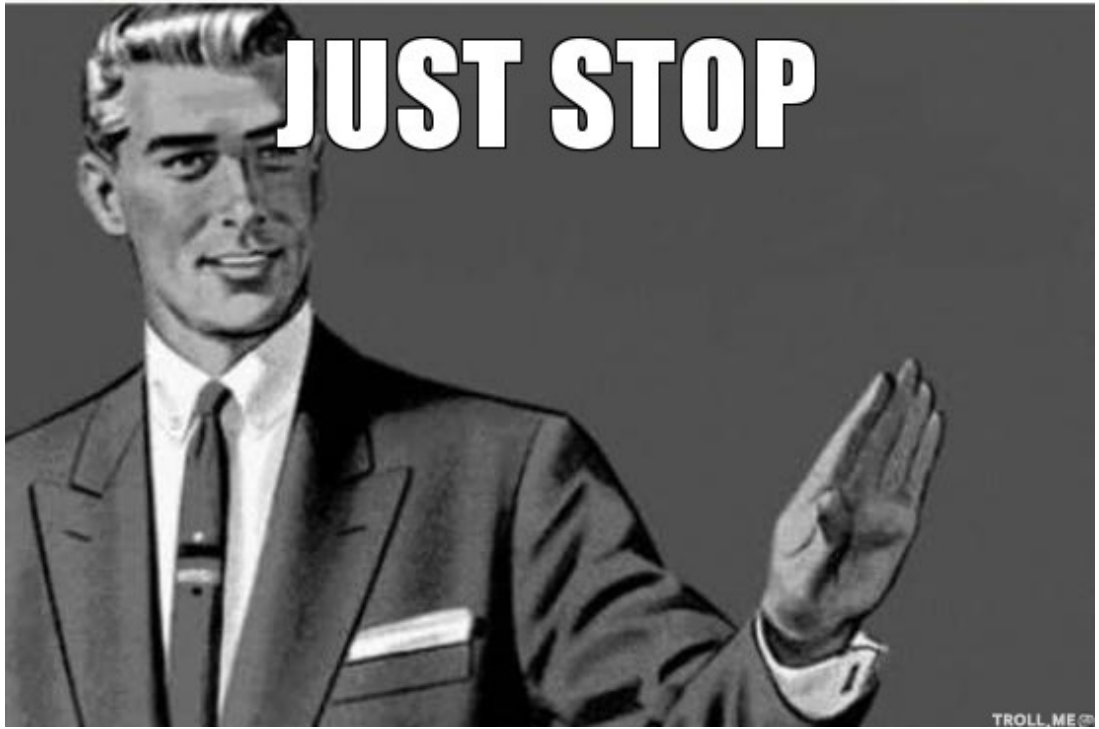
Tools: WGET



Trends



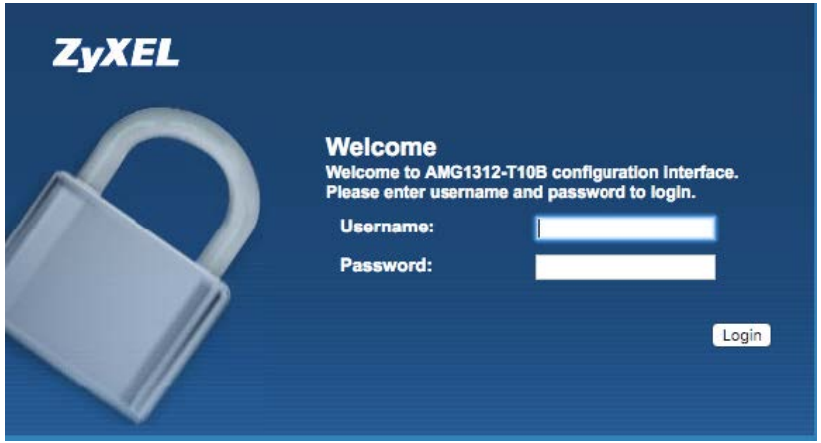
Media Grandstanding



Commoditization of DDoS

https://www.flickr.com/photos/trophygeek/7309935684/sizes/l


AA RRRRRRR RRRRRRR III SSSSS
AAAA RRRRRRRRR RRRRRRRRR III SSSSSSSSS
AAAAAA RRR RRR RRR RRR III SSS SS
AAA AAA RRR RRRR RRR RRRR III SSSS
AAA AAA RRRRRRRRR RRRRRRRRR III SSSSSS
AAAAAAAAAAA RRR RRR RRR RRR III SSSS
AAA AAA RRR RRR RRR RRR III SS SSS
AA AA RRR RRR RRR RRR III SSSSSSSS
A A RRR R RRR R III SSSSS
ARRIS Enterprises, Inc. 2015 All rights reserved
Enter password>


ZyXEL
Welcome
Welcome to AMG1312-T10B configuration interface.
Please enter username and password to login.
Username:
Password:
Login

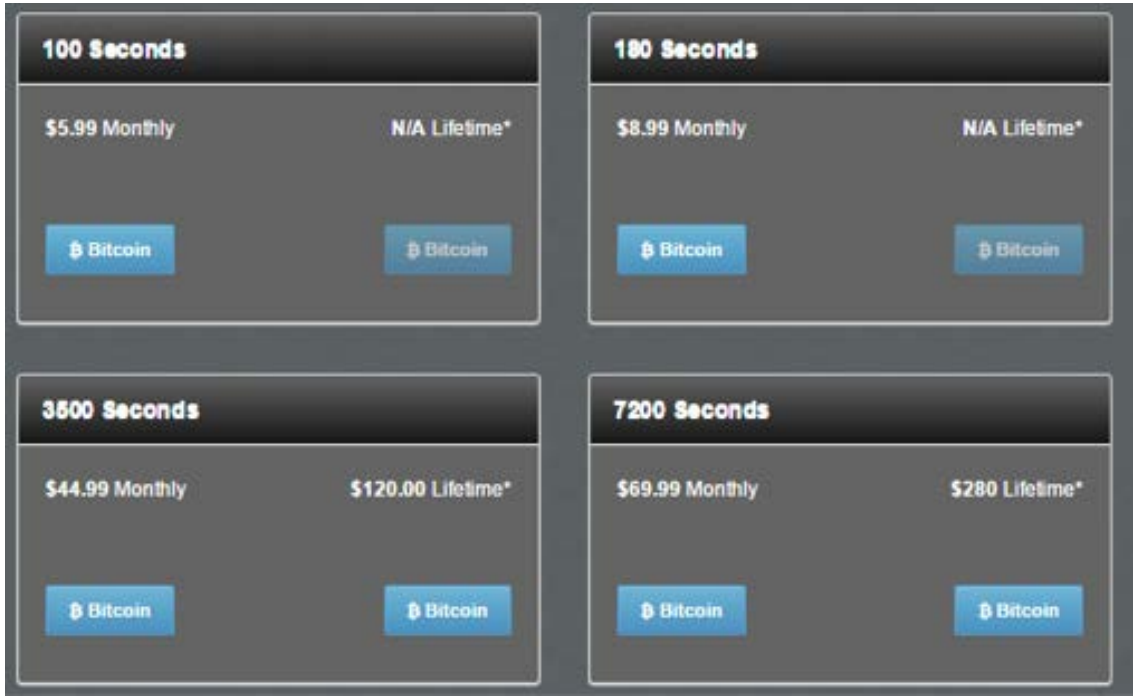
Lizard Squad launches DDoS tool that lets anyone take down online services, starting at $6 per month

December 30, 2014 8:37 AM
Emil Protalinski

557 615 96 439 70

Lizard Squad, the "hacker" group best known for attacking Microsoft's Xbox Live and Sony's PlayStation Network, has now launched a distributed denial-of-service (DDoS) attack tool. Now anyone can now take down the website or online service of their choice thanks to "Lizard Stresser," which we're not linking to for obvious reasons.

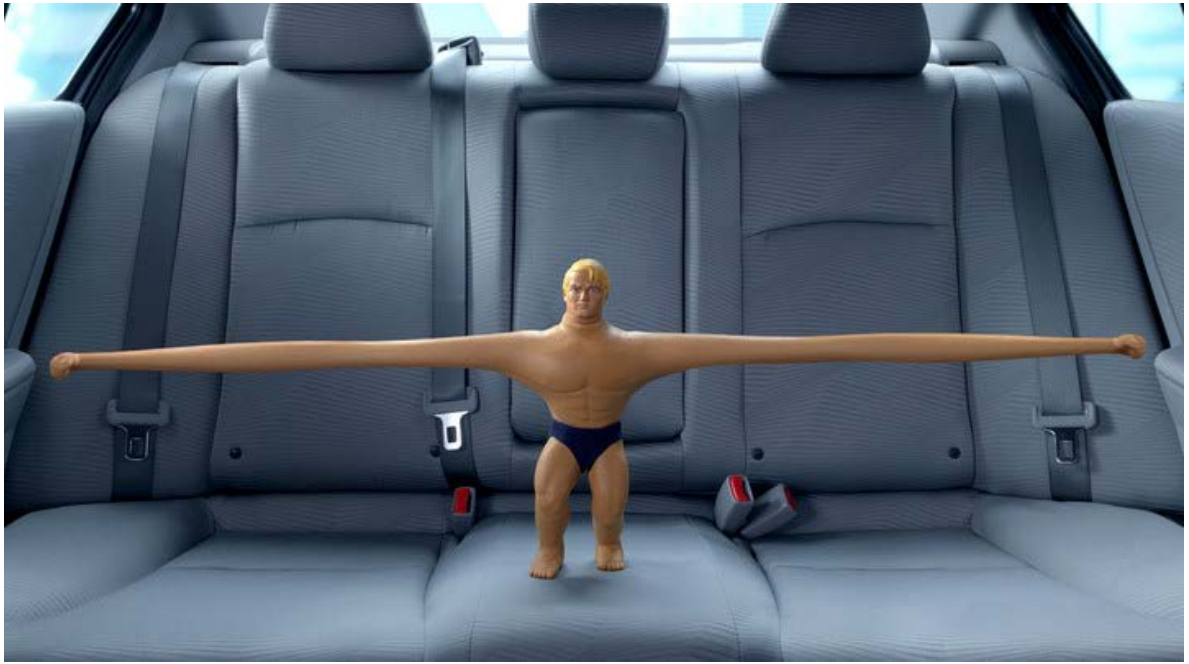
What's your fancy?



What's a Booter?

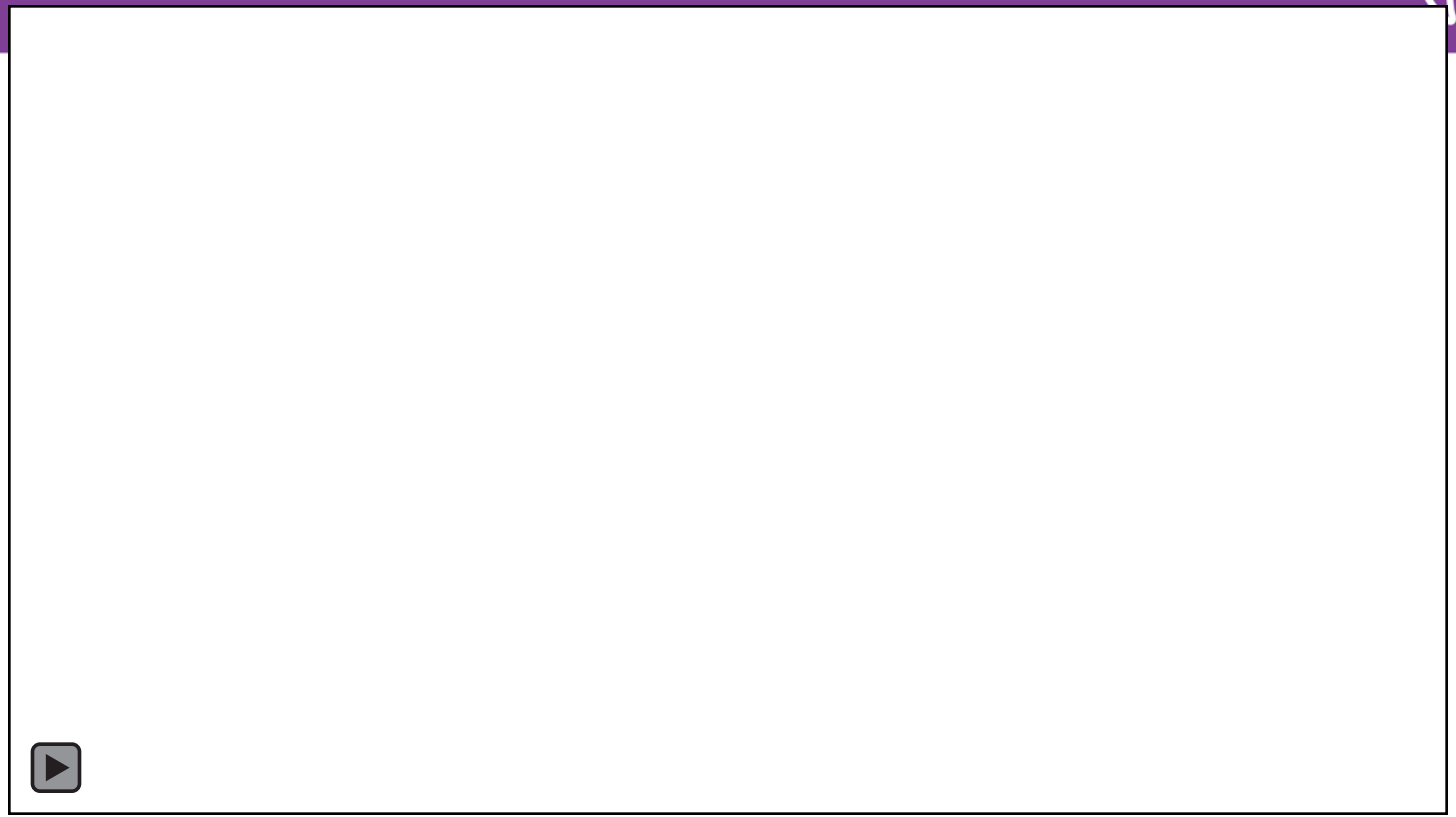
Akamai

OK, What's a Stresser?



Stressers or Booters

- xBOOT
- Flash Stresser
- Hyper Stresser
- Grim Booter
- Anonymous Stresser
- Titanium Stresser / Lizards
- Big Bang Booter…and so on.



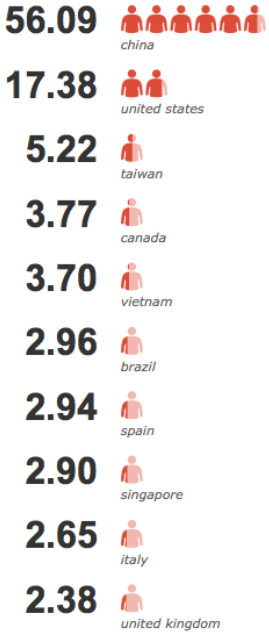
Some other highlights

- DDoS agents targeting Joomla and other SaaS apps
- A heap-based buffer overflow vulnerability in Linux systems
- Attackers using new MS SQL reflection techniques
- Data breaches fueling login attacks

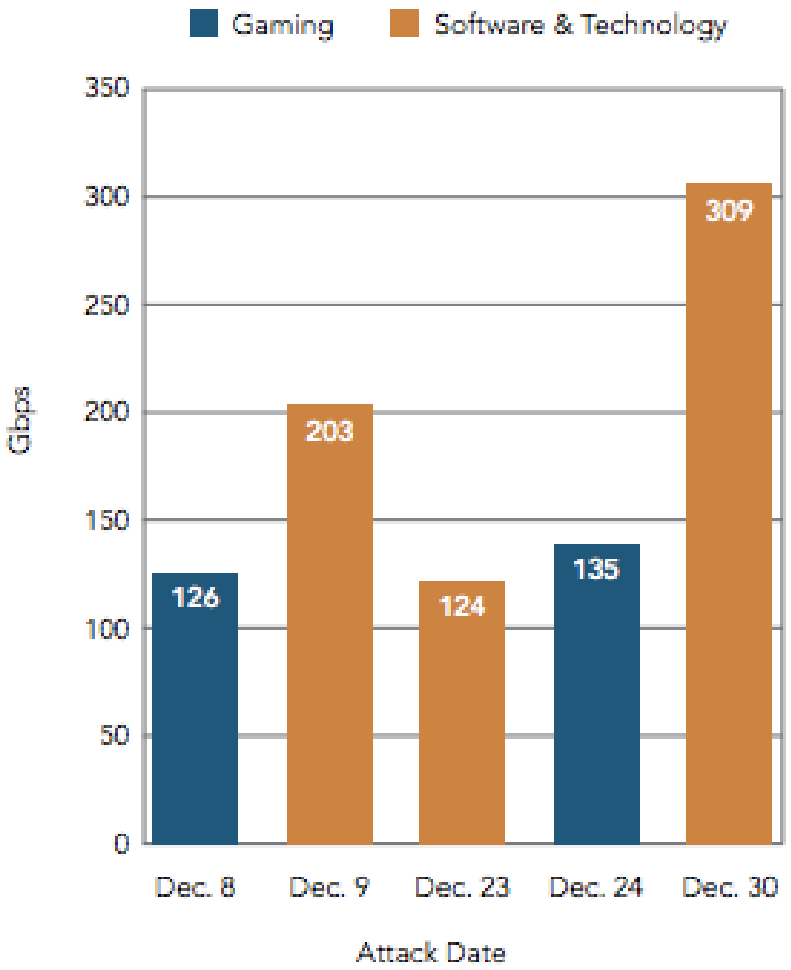
OK so, attribution?

https://www.flickr.com/photos/45909111@N00/8519280338/sizes/l

Top 10 Source Countries for DDoS Attacks, Q2 2016

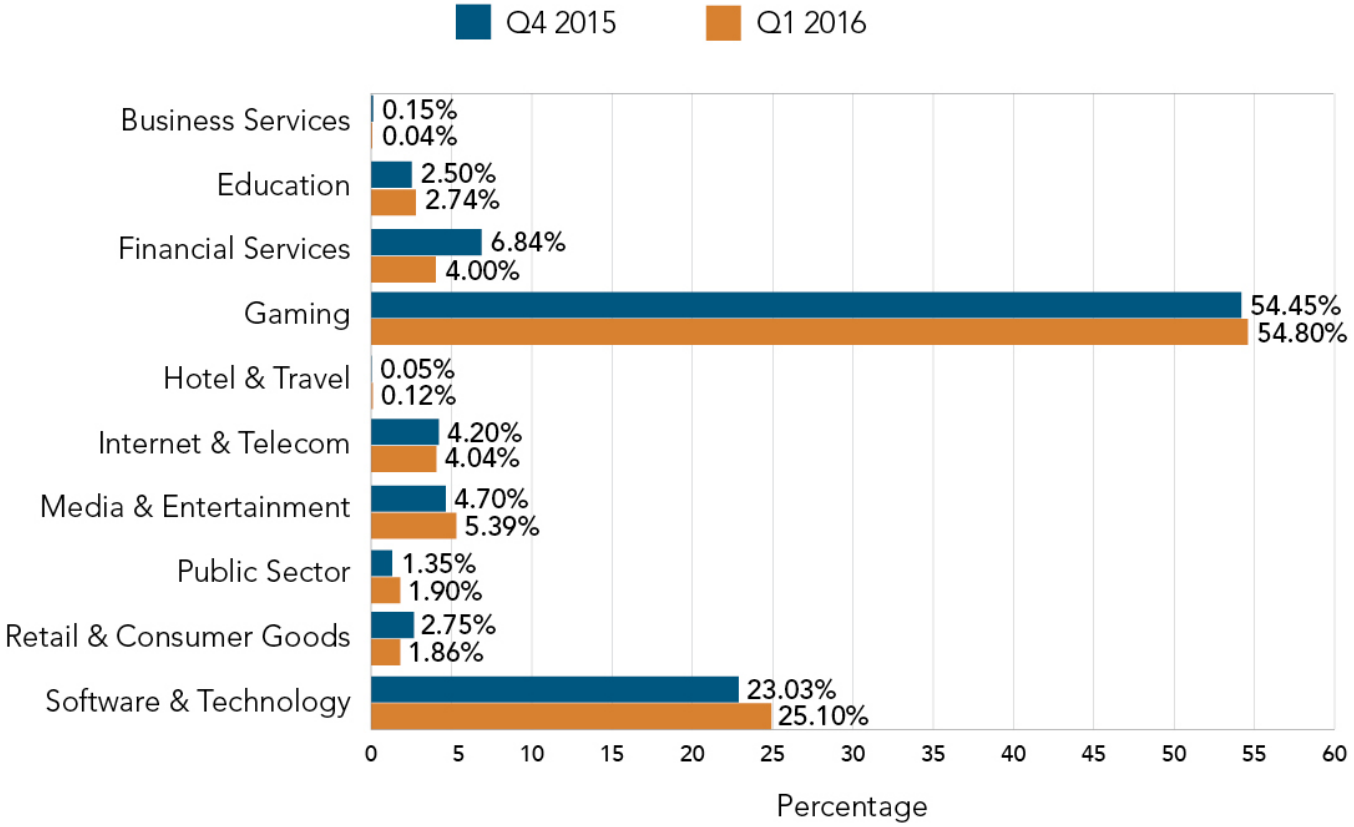


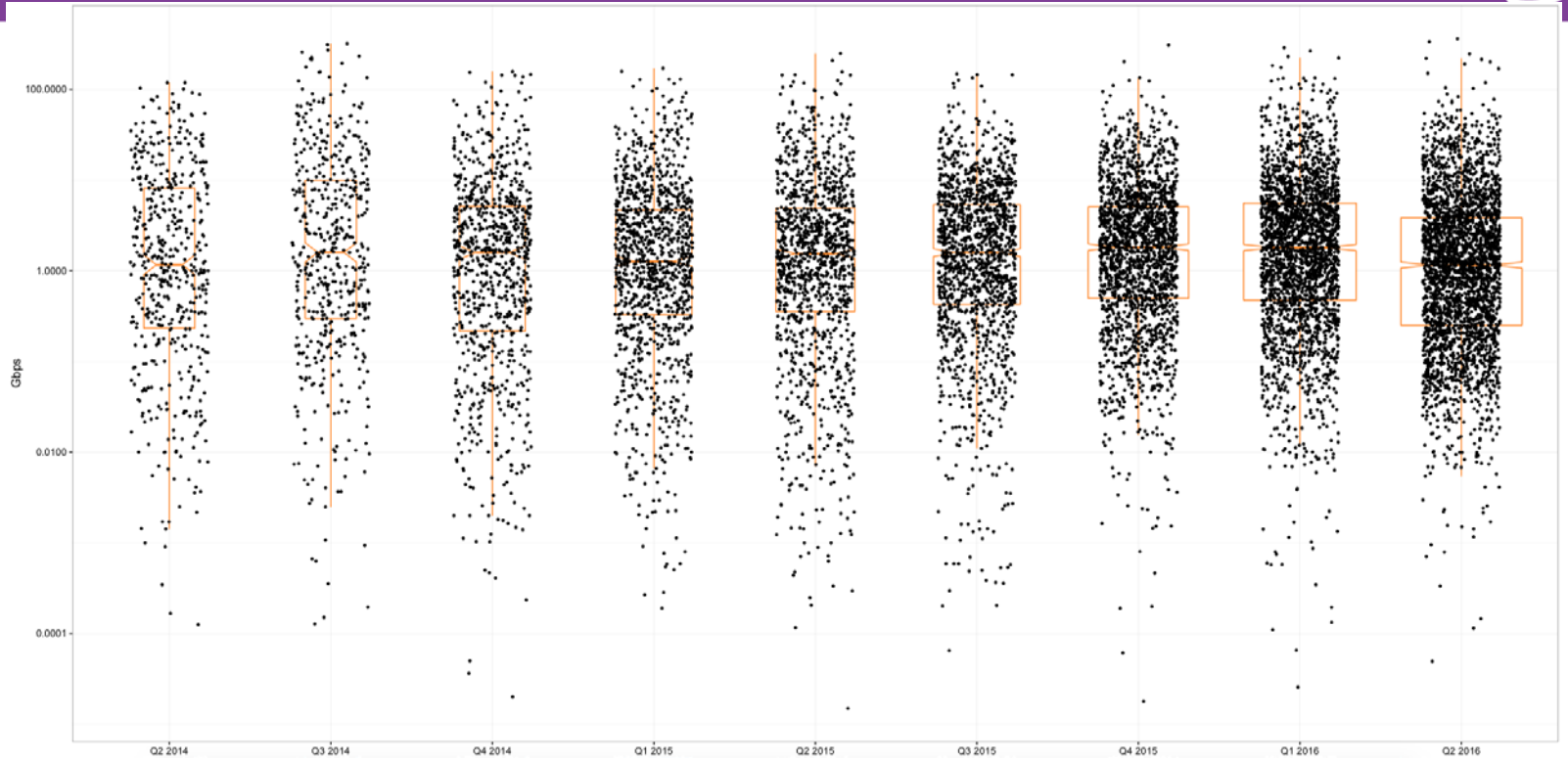
Q4 2015 DDoS Attacks > 100 Gbps



Akamai

DDoS Attack Frequency by Industry, Q1 2016




Gbps
100.0000
1.0000
0.0100
0.0001
Q2 2014
Q3 2014
Q4 2014
Q1 2015
Q2 2015
Q3 2015
Q4 2015
Q1 2016
Q2 2016

Akamai

Other Observations

- SQLi
- Local/Remote File Inclusion
- IoT botnets coming to the forefront
- PHP Injection
- Malicious File upload
- JAVA …best remote access platform ever!

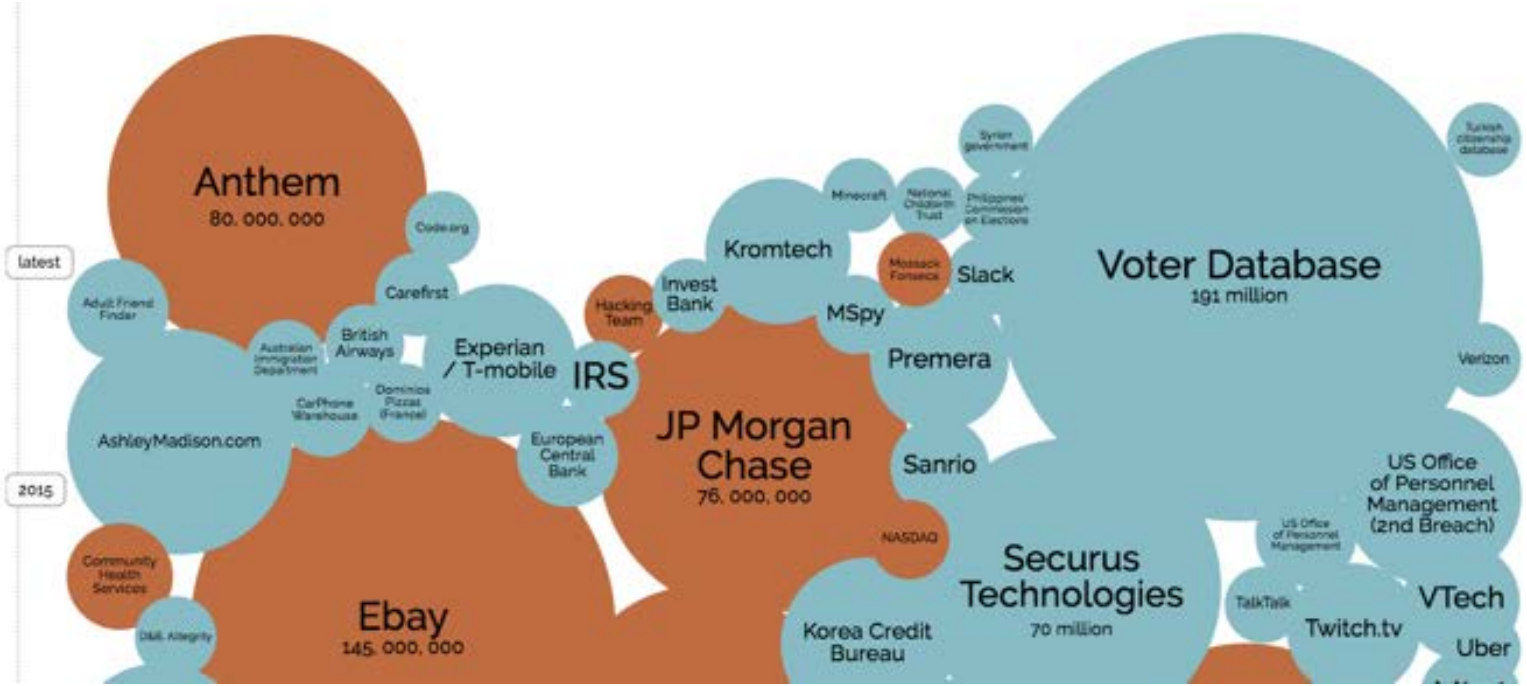
SQL Injection…still

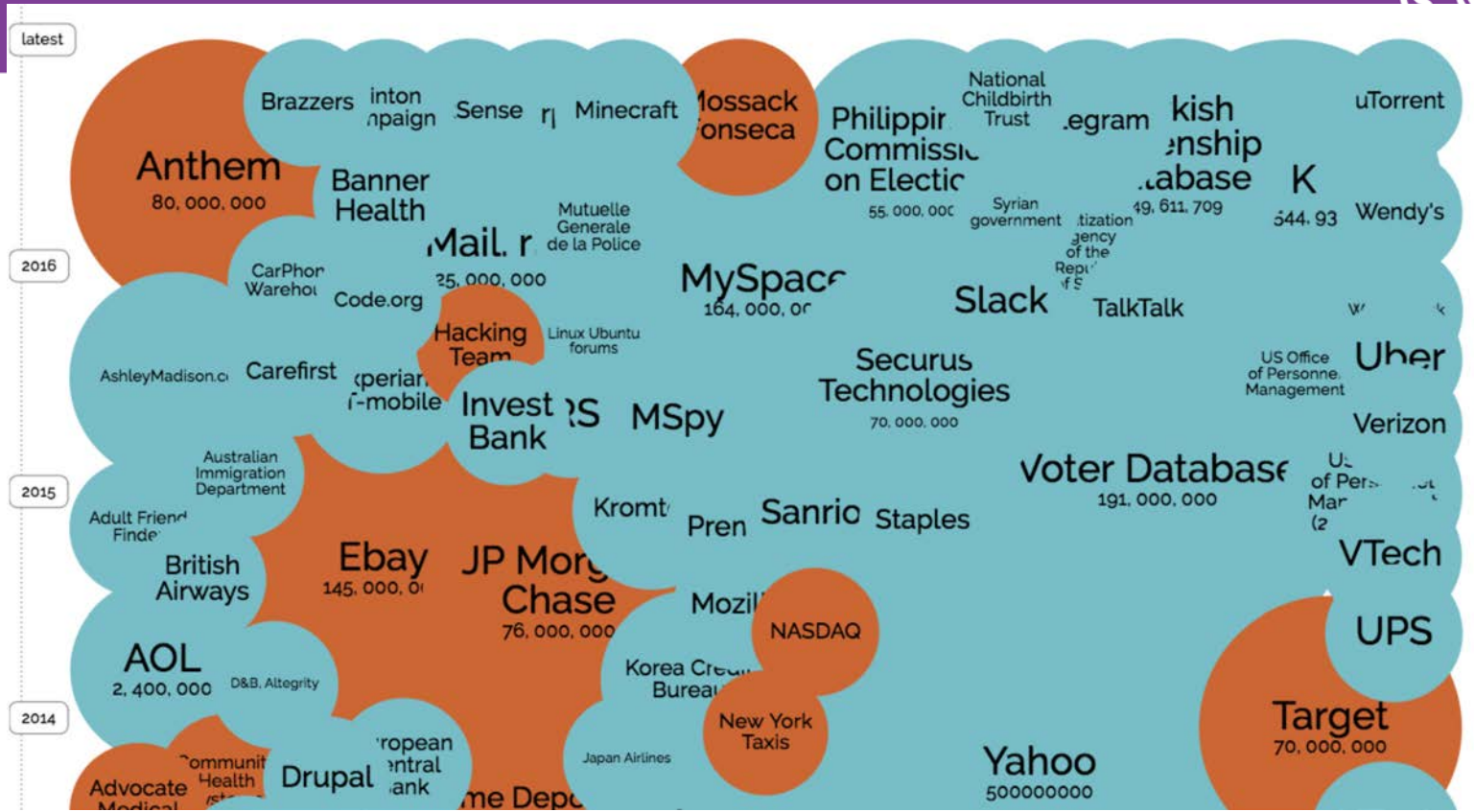
Pwned websites

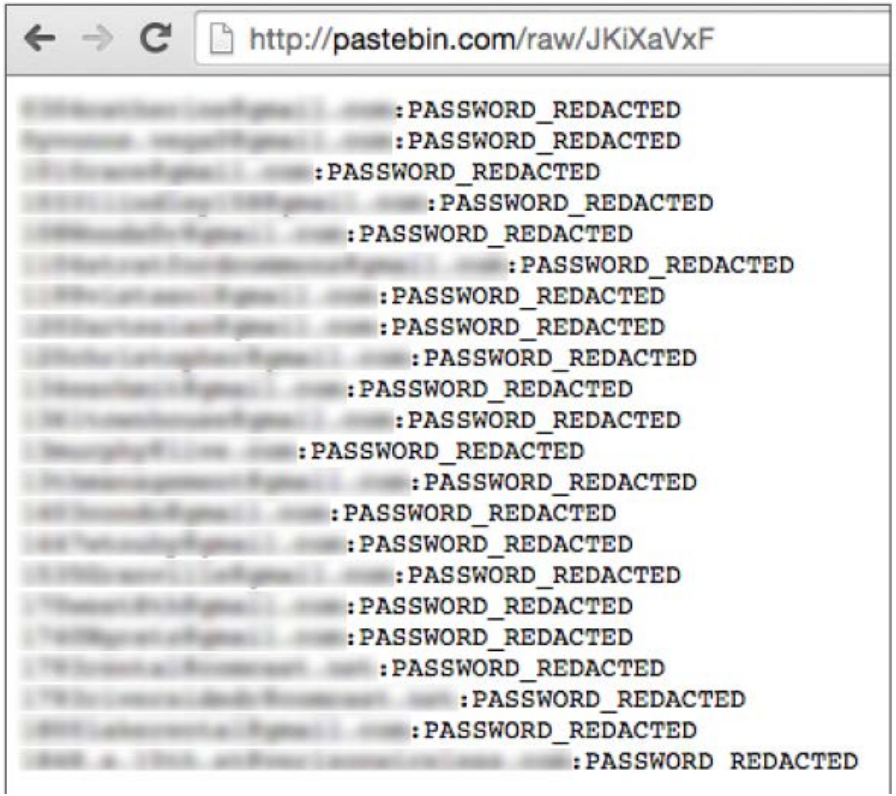
Breached websites that have been loaded into this service

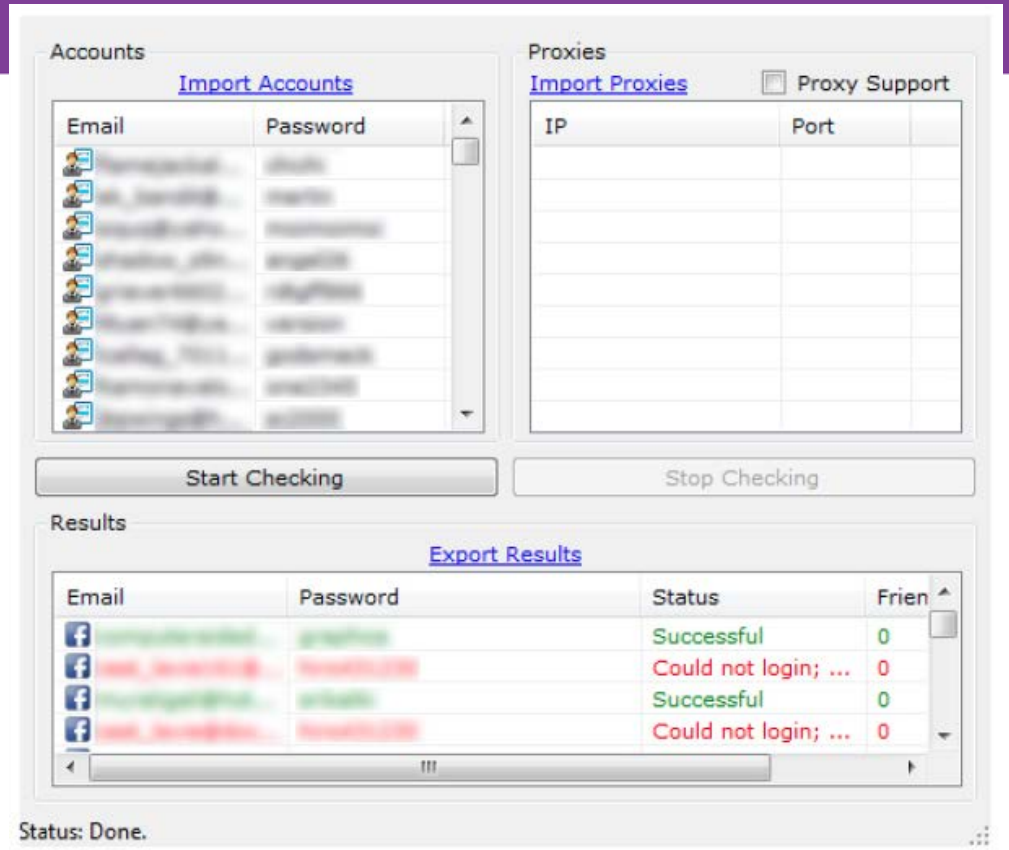
Here's an overview of the various breaches that have been consolidated into this site. Each of these has been dumped publicly and is readily available via various sites on the web. This information is also available via an RSS feed.

359,420,698	MySpace accounts	432,943	Acne.org accounts
164,611,595	LinkedIn accounts	432,552	Xbox-Scene accounts
152,445,165	Adobe accounts	422,959	Avast accounts
65,469,298	tumblr accounts	341,118	PSX-Scene accounts
40,767,652	Fling accounts	327,314	Plex accounts
30,811,934	Ashley Madison accounts	285,191	Sumo Torrent accounts
27,393,015	Mate1.com accounts	281,924	Seedpeer accounts
13,545,468	000webhost accounts	269,548	MajorGeeks accounts
13,186,088	R2Games accounts	252,751	myRepoSpace accounts
8,243,604	Gamigo accounts	252,216	Foxy Bingo accounts
8,089,103	Heroes of Newerth accounts	228,605	COMELEC (Philippines Voters) accounts
7,089,395	Lifeboat accounts	227,746	Cannabis.com accounts
5,915,013	Nexus Mods accounts		


latest
2015
Anthem
80, 000, 000
Code.org
Carefirst
Adult Friend Finder
British Airways
Australian Immigration Department
Experian / T-mobile
IRS
CarPhone Warehouse
Dominos Pizzas (France)
AshleyMadison.com
European Central Bank
Community Health Services
D&B, Allegrity
Ebay
145, 000, 000
Hacking Team
Invest Bank
Kromtech
Minecraft
National Children's Trust
Syrian government
Philippines' Commission on Elections
Mossack Fonseca
Slack
MSpy
Premera
JP Morgan Chase
76, 000, 000
Sanrio
NASDAQ
Korea Credit Bureau
Securus Technologies
70 million
Voter Database
191 million
Turkish citizenship database
Verizon
US Office of Personnel Management (2nd Breach)
US Office of Personnel Management
TalkTalk
Twitch.tv
VTech
Uber


latest
2016
2015
2014
Brazzers
Minecraft
Anthem
80, 000, 000
Banner Health
Mail. r
25, 000, 000
Mutuelle Generale de la Police
CarPhon Warehou
Code.org
Hacking Team
Linux Ubuntu forums
AshleyMadison.c
Carefirst
T-mobile
Invest Bank
MSpy
MySpace
164, 000, 00
Slack
TalkTalk
Securus Technologies
70, 000, 000
US Office of Personne Management
Uber
Verizon
Australian Immigration Department
Adult Friend Finde
British Airways
Ebay
145, 000, 0
JP Morg Chase
76, 000, 000
Kromt
Pren
Sanrio
Staples
Voter Database
191, 000, 000
VTech
UPS
AOL
2, 400, 000
D&B, Altegrity
NASDAQ
New York Taxis
Japan Airlines
Yahoo
500000000
Target
70, 000, 000
Drupal
Advocate
Health
Philippir
Commissi on Electic
55, 000, 00
National Childbirth Trust
Syrian government
49, 611, 709
544, 93
Wendy's
uTorrent


http://pastebin.com/raw/JKiXaVxF
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD_REDACTED
:PASSWORD REDACTED


Accounts
Import Accounts
Email
Password
Proxies
Import Proxies
Proxy Support
IP
Port
Start Checking
Stop Checking
Results
Export Results
Email
Password
Status
Frien
Successful
0
Could not login; ...
0
Successful
0
Could not login; ...
0
Status: Done.

File Inclusions

Malicious Uploads

- KCFinder file upload vulnerability
- Open Flash Chart file upload vulnerability (CVE-2009-4140)
- appRain CMF (uploadify.php) unrestricted file upload exploit (CVE-2012-1153)
- FCKeditor file upload vulnerability (CVE-2008-6178)

Undead Army

https://www.flickr.com/photos/scabeater/3272684874/sizes/o/

So, what to do?

- I might know a vendor that could help :-)
- SQL INJECTION IS A SOLVABLE PROBLEM
- Harden systems
- Work with your ISP on mitigation strategies
- Use ACL lists to deal with known bad IPs
- IP Rate limiting
- PATCH PATCH PATCH

Akamai


NO
DATA
THIS COMIC MADE POSSIBLE THANKS TO ADAM LINGELBACH
MRLOVENSTEIN.COM


MAKE CYBER
GREAT AGAIN

Thank You RSA!

شكرا على استماعكم

Questions?
Thanks

Dave Lewis
@gattaca

dave@akamai.com