Barbarians At The Gate(way)

Examination of actors, tools and defenses

#whoami

Dave Lewis
@gattaca
dave@akamai.com

Akamai

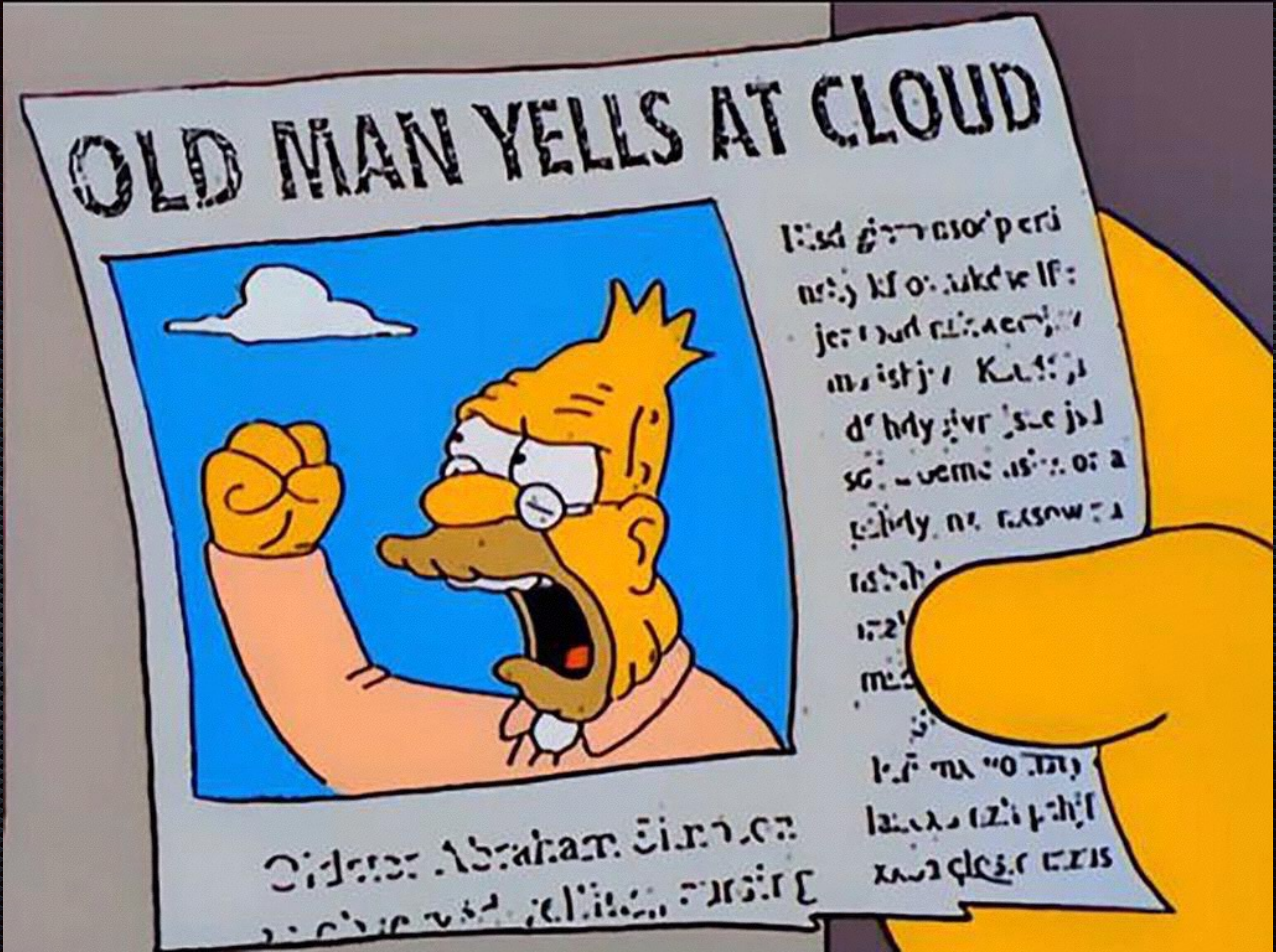
Akamai
FASTER FORWARD

Akamai

MYSTERY SOLVED!

WE FOUND HIM!

NEMO
MAJURO



OLD MAN YELLS AT CLOUD

Oldster Abraham Simpson [illegible]

1000x View - Cyber Pathogen

It left me wanting…

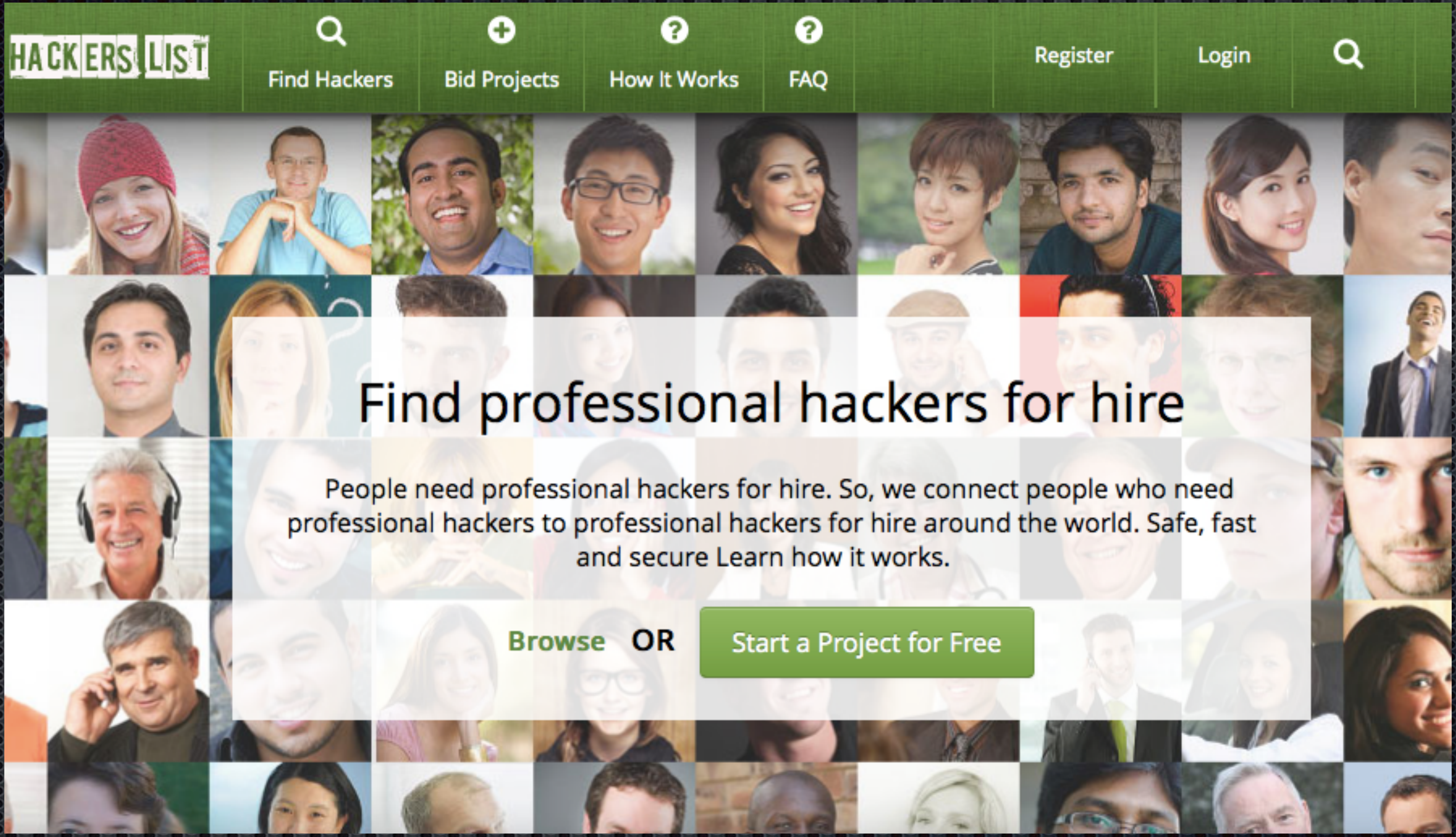
Game Plan

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

Actors: For Hire

Current(ish) prices on the Russian underground market:

- 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



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.

Actors: Bored Kids

AND

BORED TEENS

FREE
Hugs

THE HACKTIVISTS

Actors: Nation States

THERE ARE

STANDARD VILLAINS

AND THERE ARE

ARCH VILLAINS

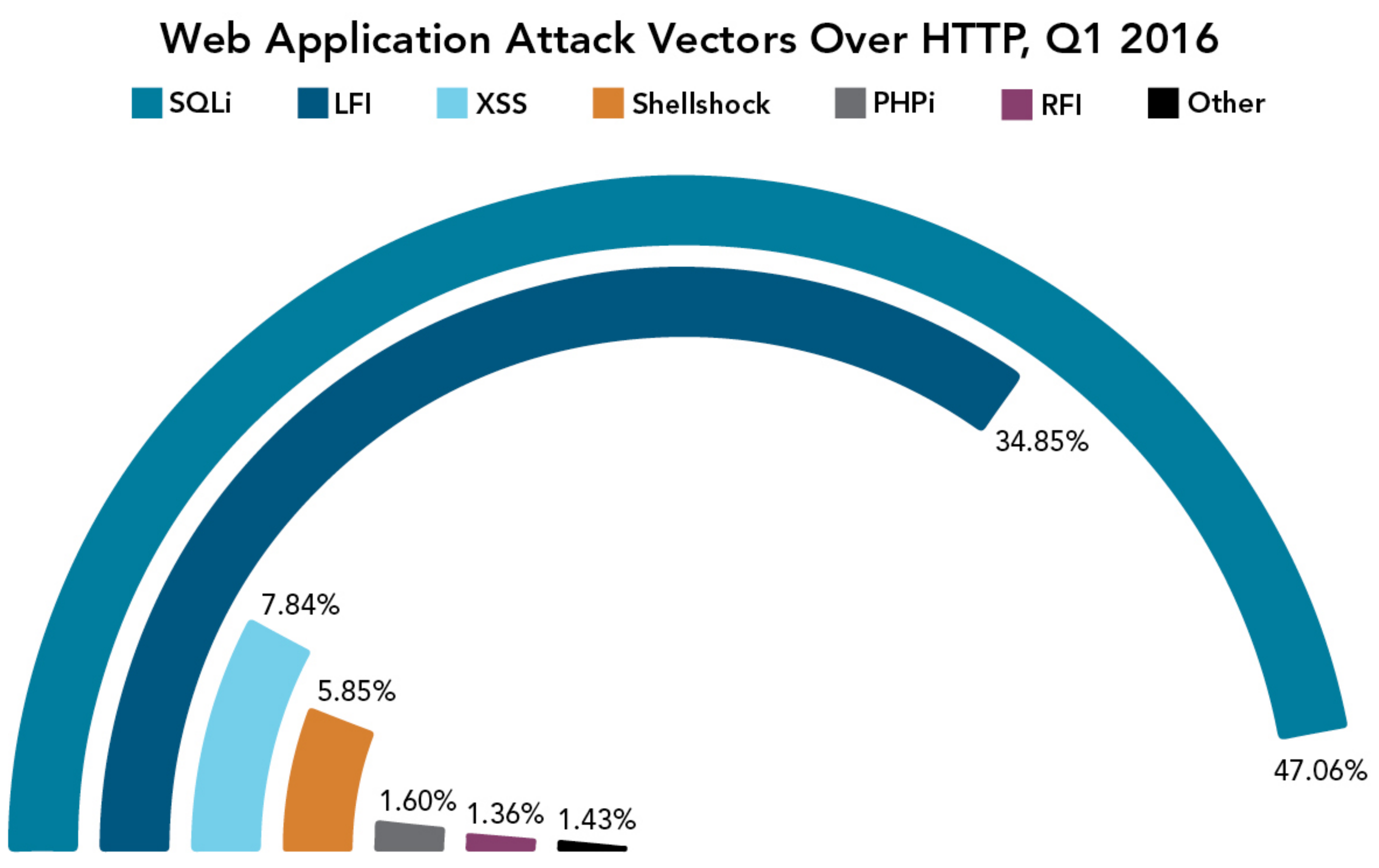
Actors: al-Qassam Cyber Fighters, QCF

QCF is an Iranian group that has been focused on attacking US and Canadian banks.

They use the Brobot botnet that attacks from compromised servers. Using server hardware and connection they can usually overwhelm scrubbers with traffic.

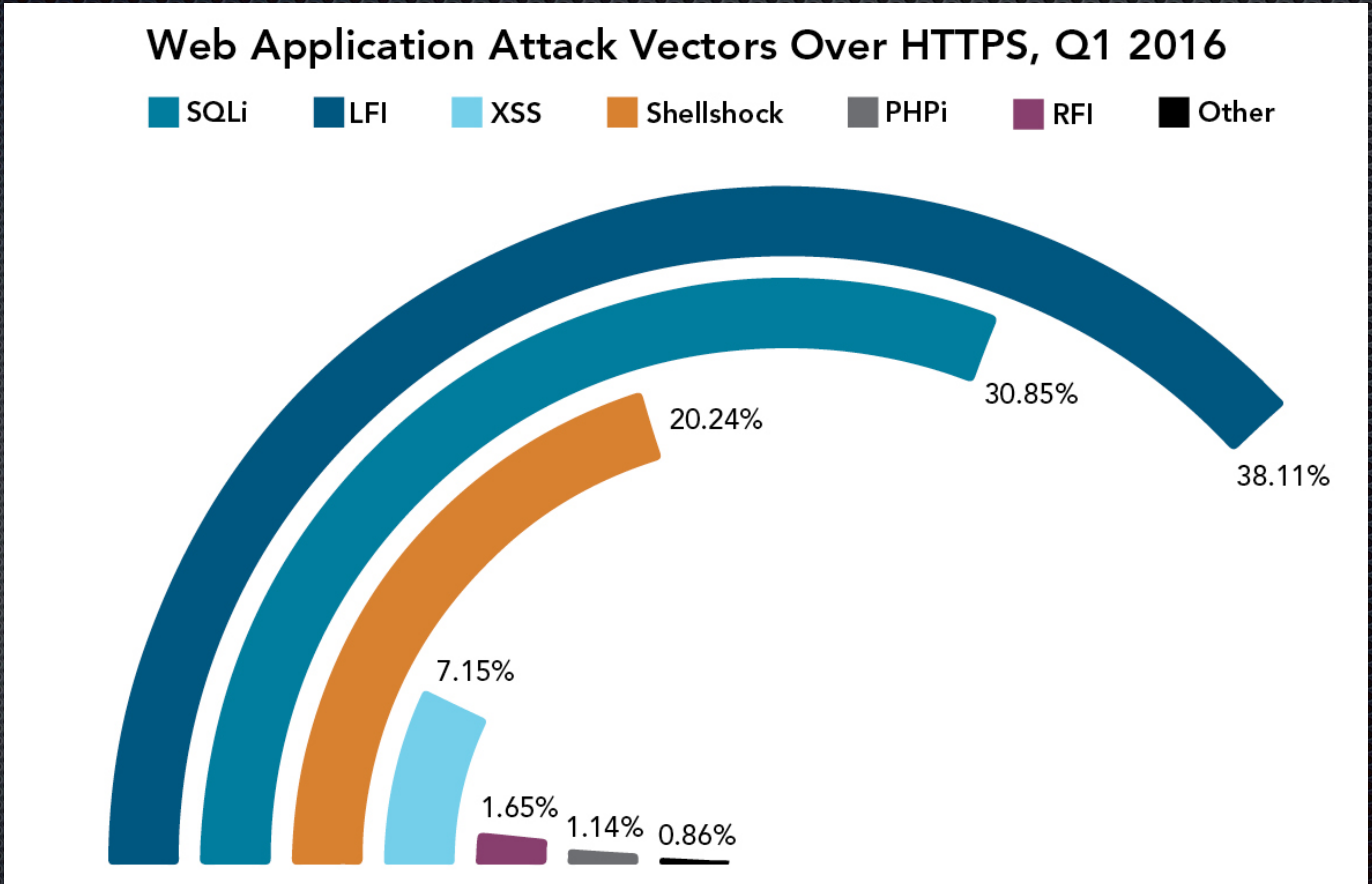
Attacks

Attack Vectors Over HTTP



Akamai

Attack Vectors Over HTTPS



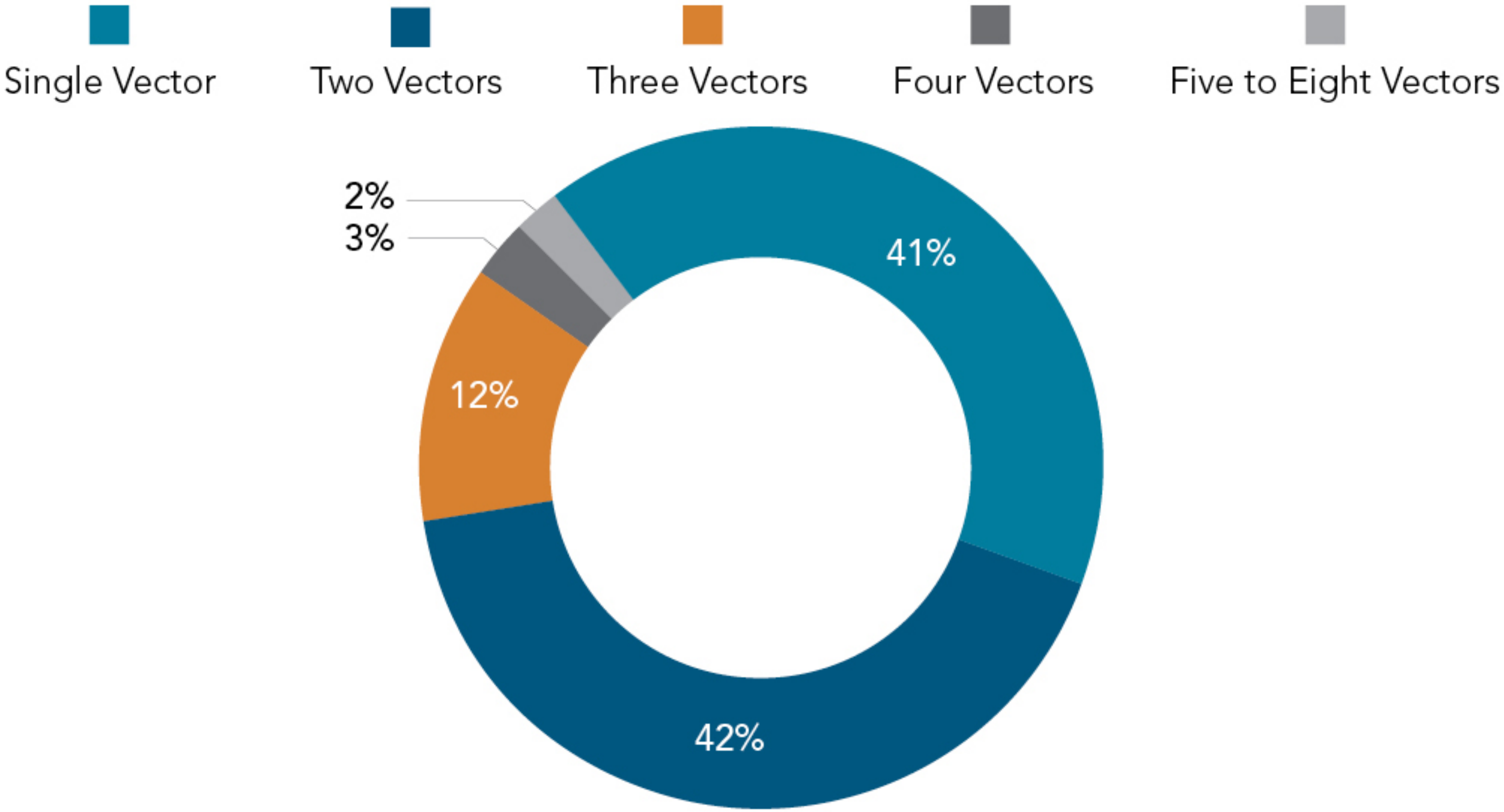
Types of Attacks

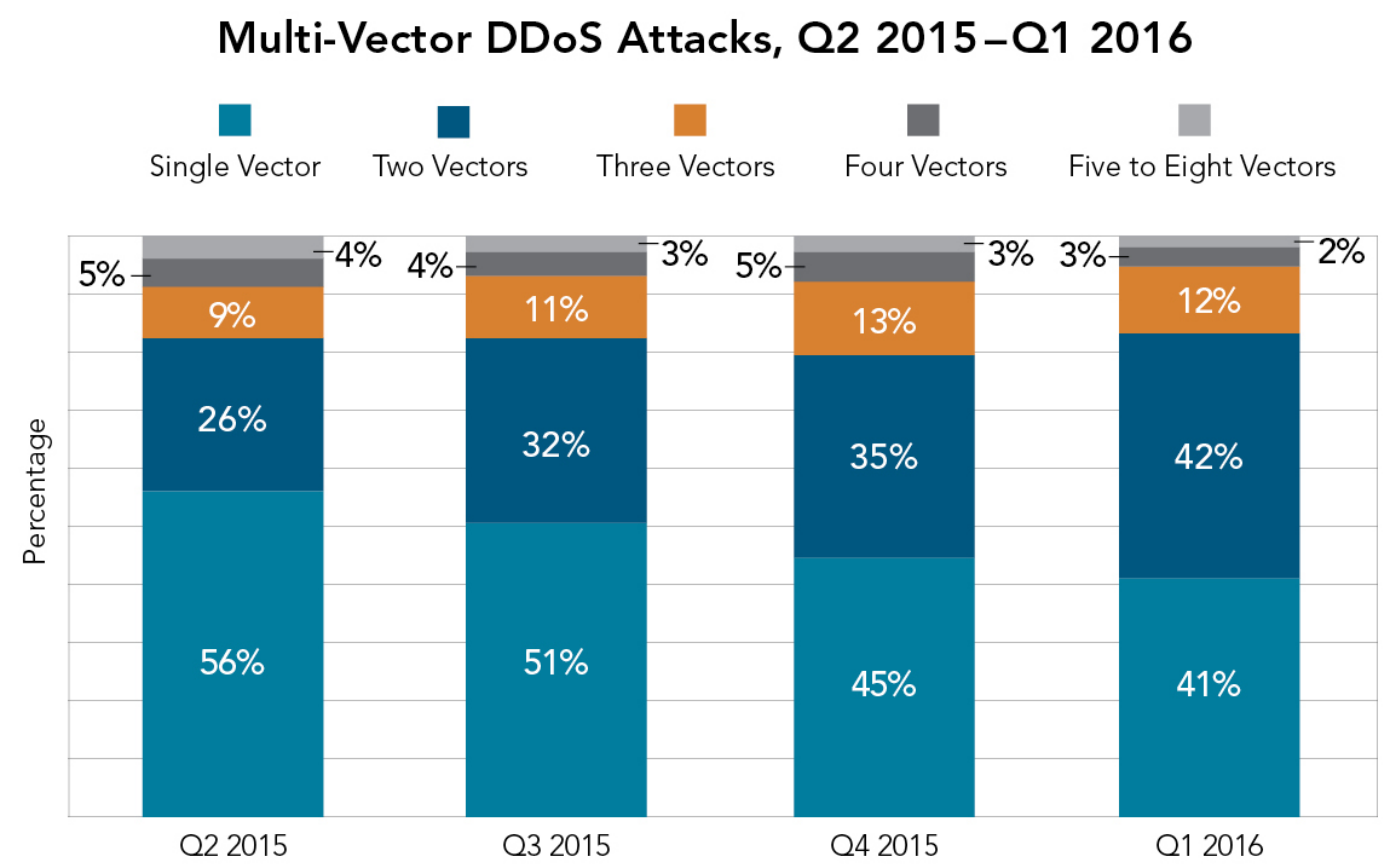
- SYN Floods
- UDP Floods
- ICMP Floods
- NTP Amplification
- HTTP Flood

Attacks: Volumetric

Your website can be overwhelmed…

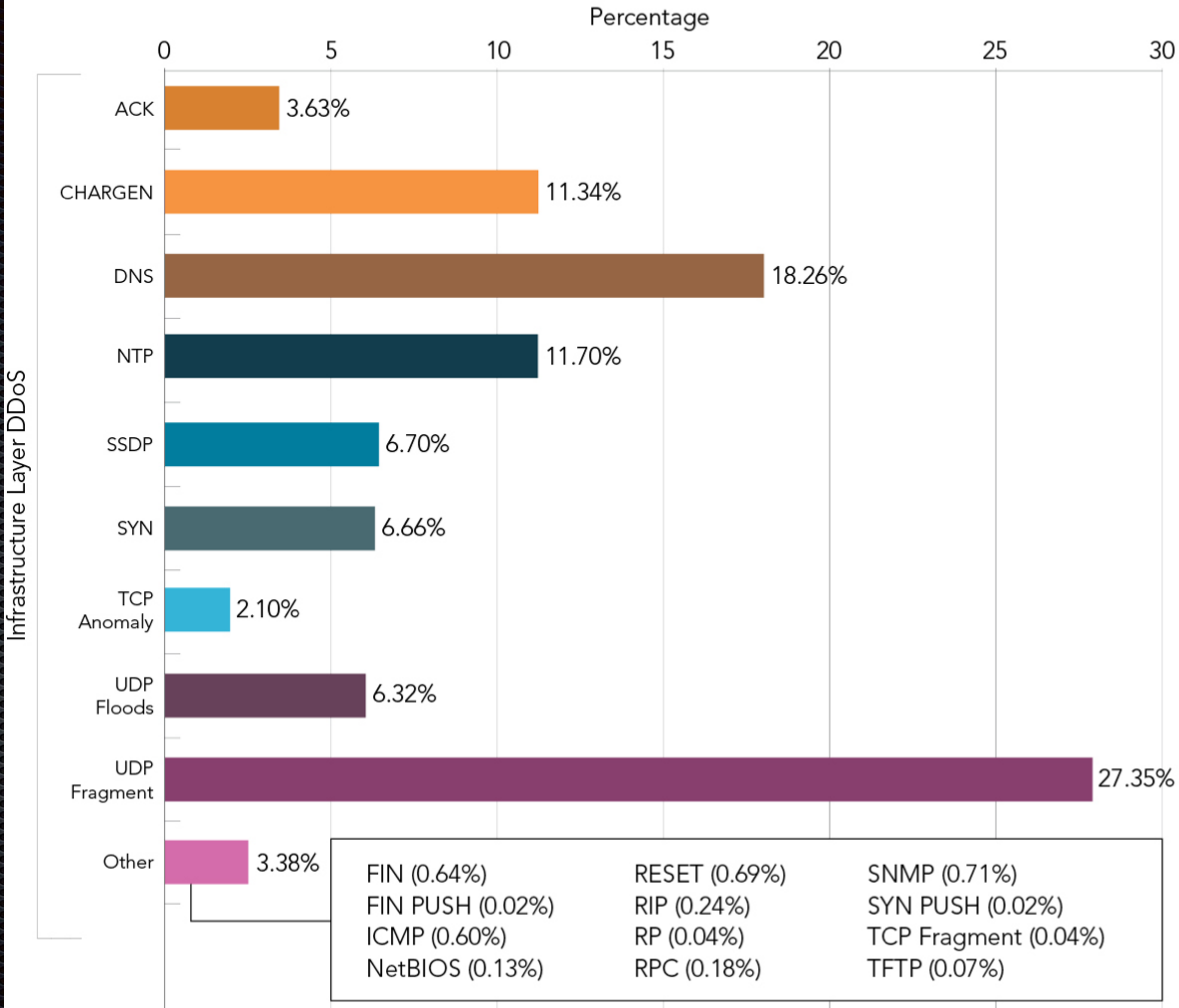
Multi-Vector DDoS Attacks, Q1 2016





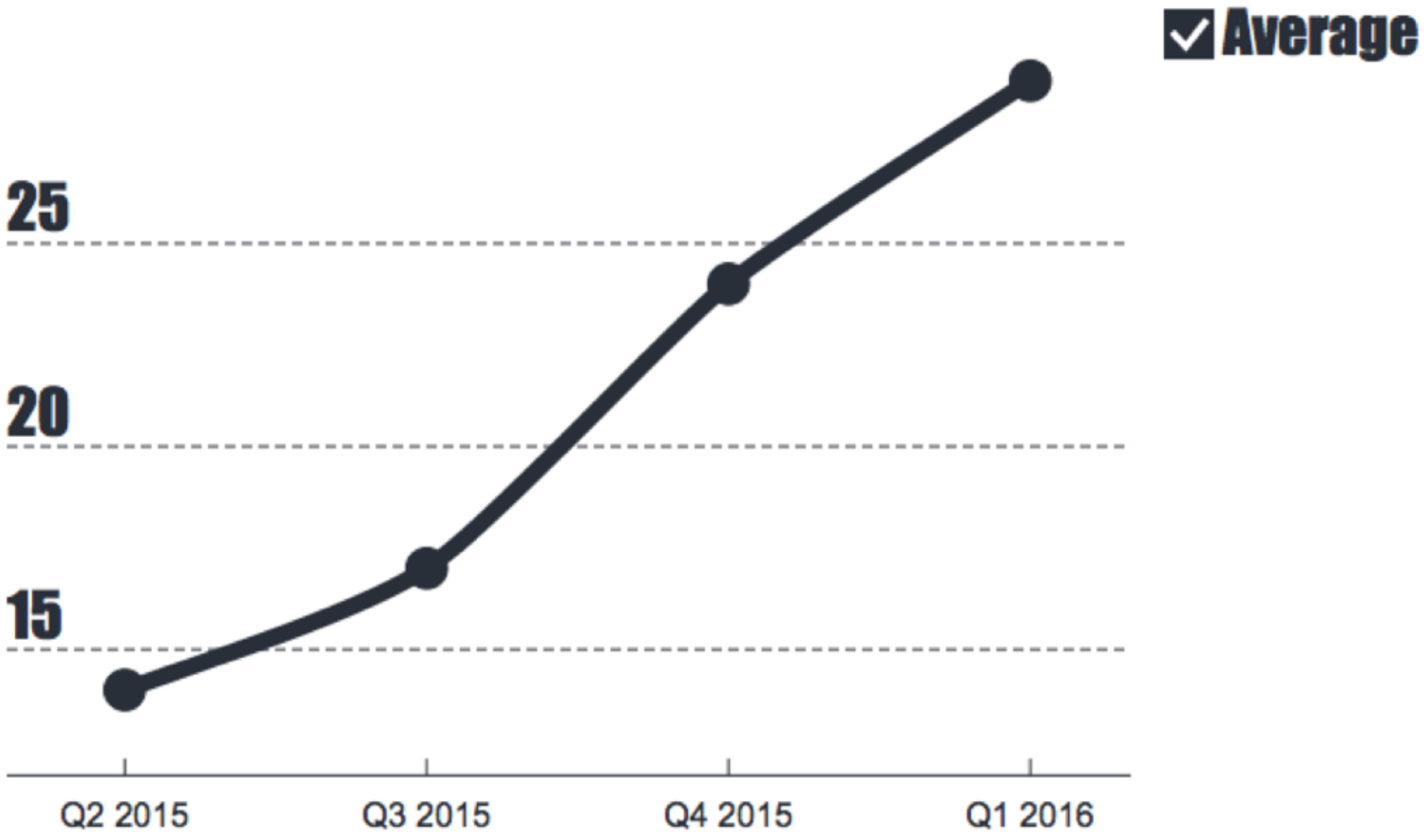
Multi-Vector DDoS Attacks, Q2 2015–Q1 2016

DDoS Attack Vector Frequency, Q1 2016



SSDP

Average Number of DDoS Attacks Per Target



Top target organization attack count

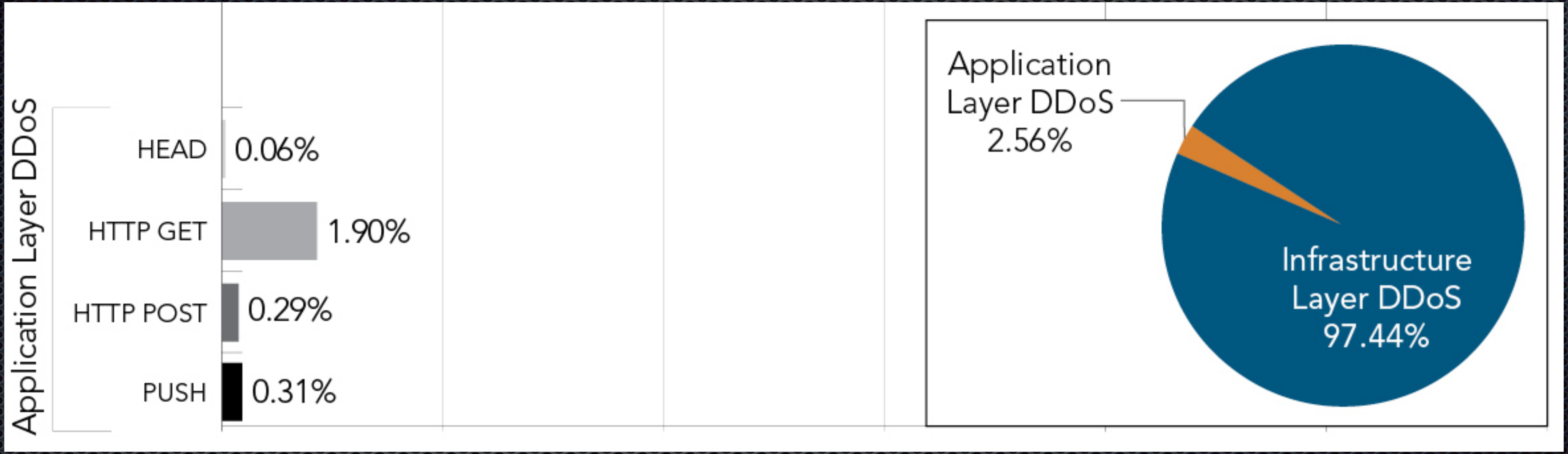
283

Average Number by Quarter

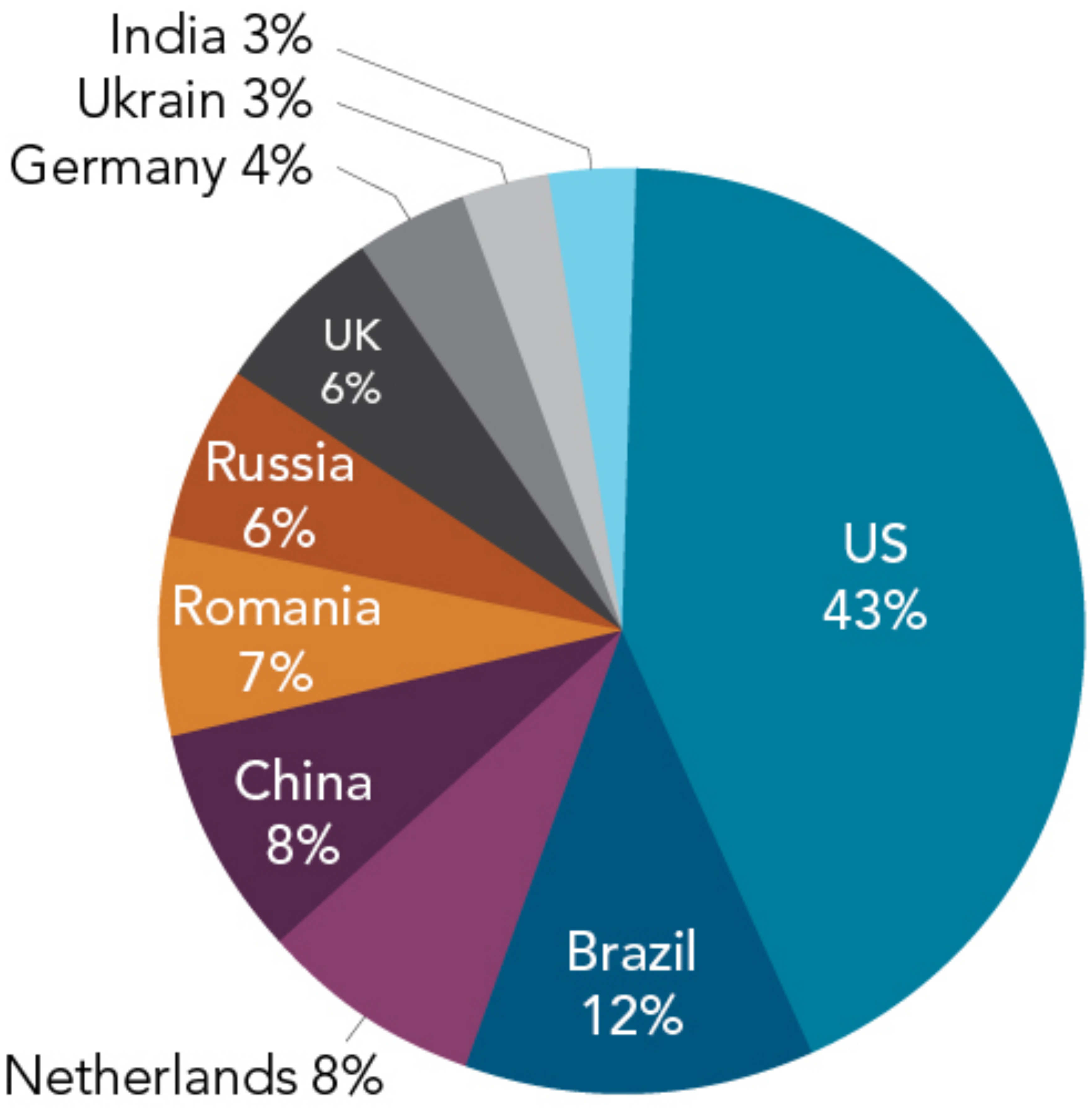
Q2 2015 - 14
Q3 2015 - 17
Q4 2015 - 24
Q1 2016 - 29

Attacks: Application Layer

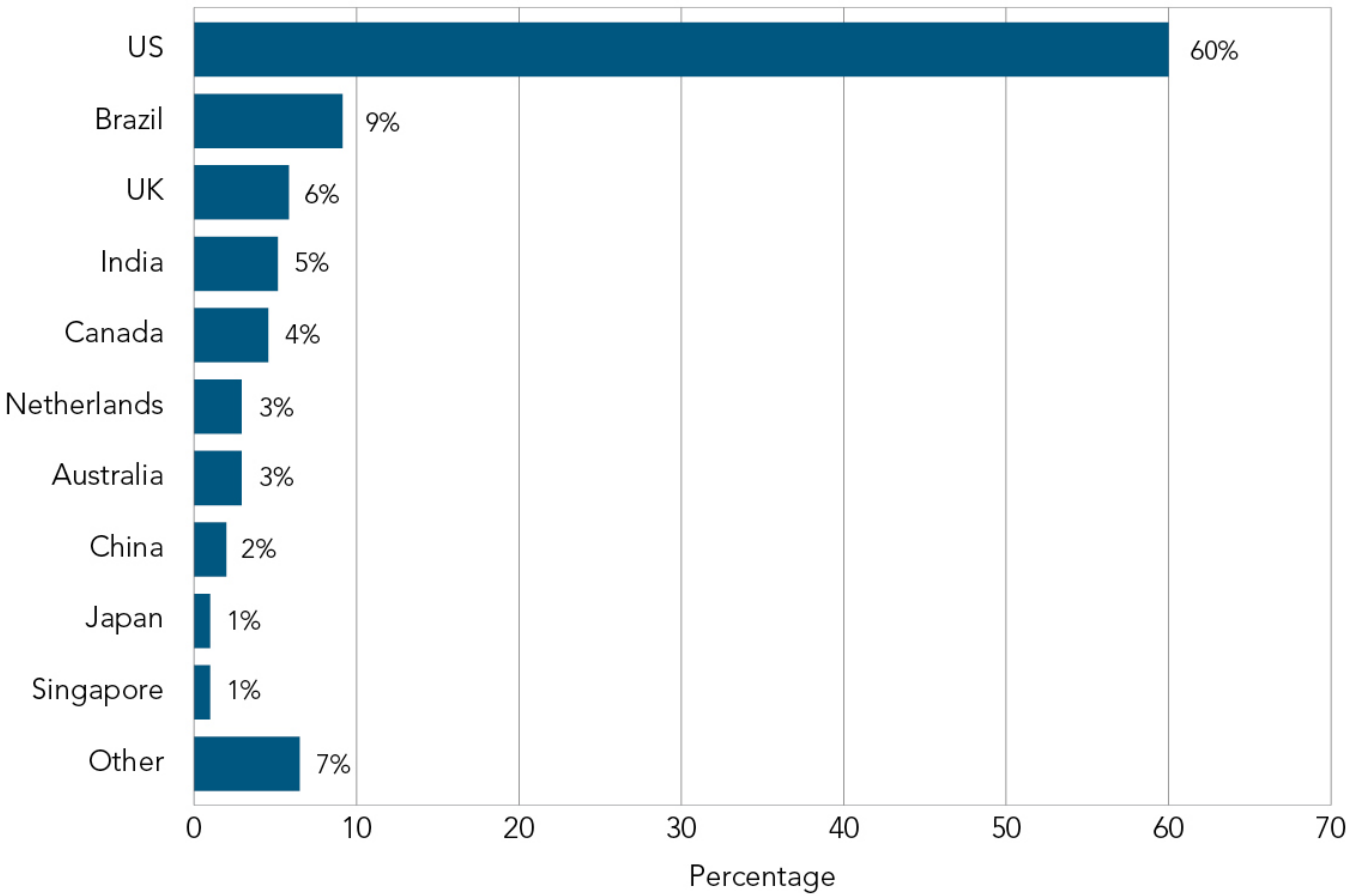
Application Layer DDoS

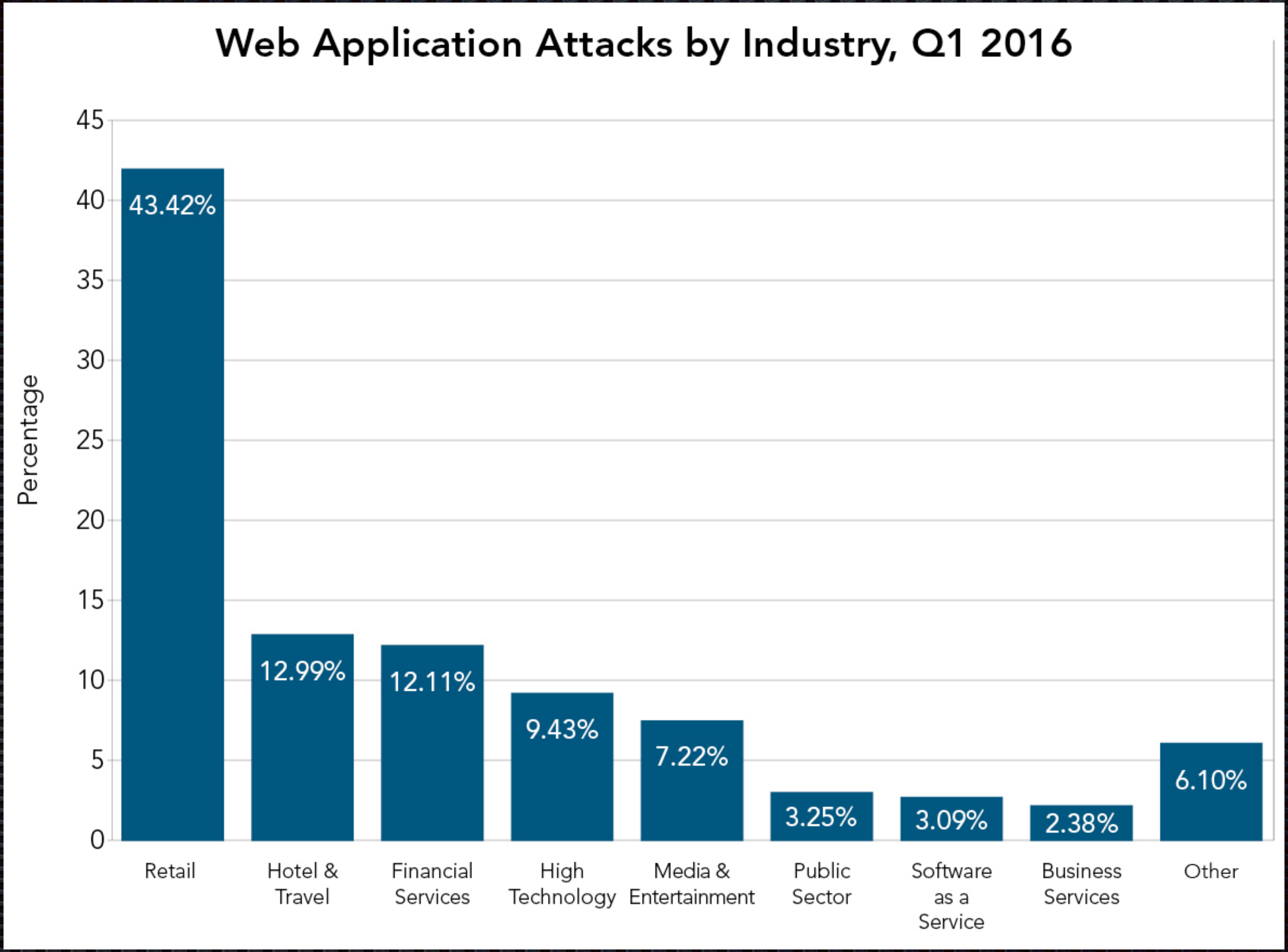


Top 10 Source Countries for Web Application Attacks, Q1 2016



Top 10 Target Countries for Web Application Attacks, Q1 2016

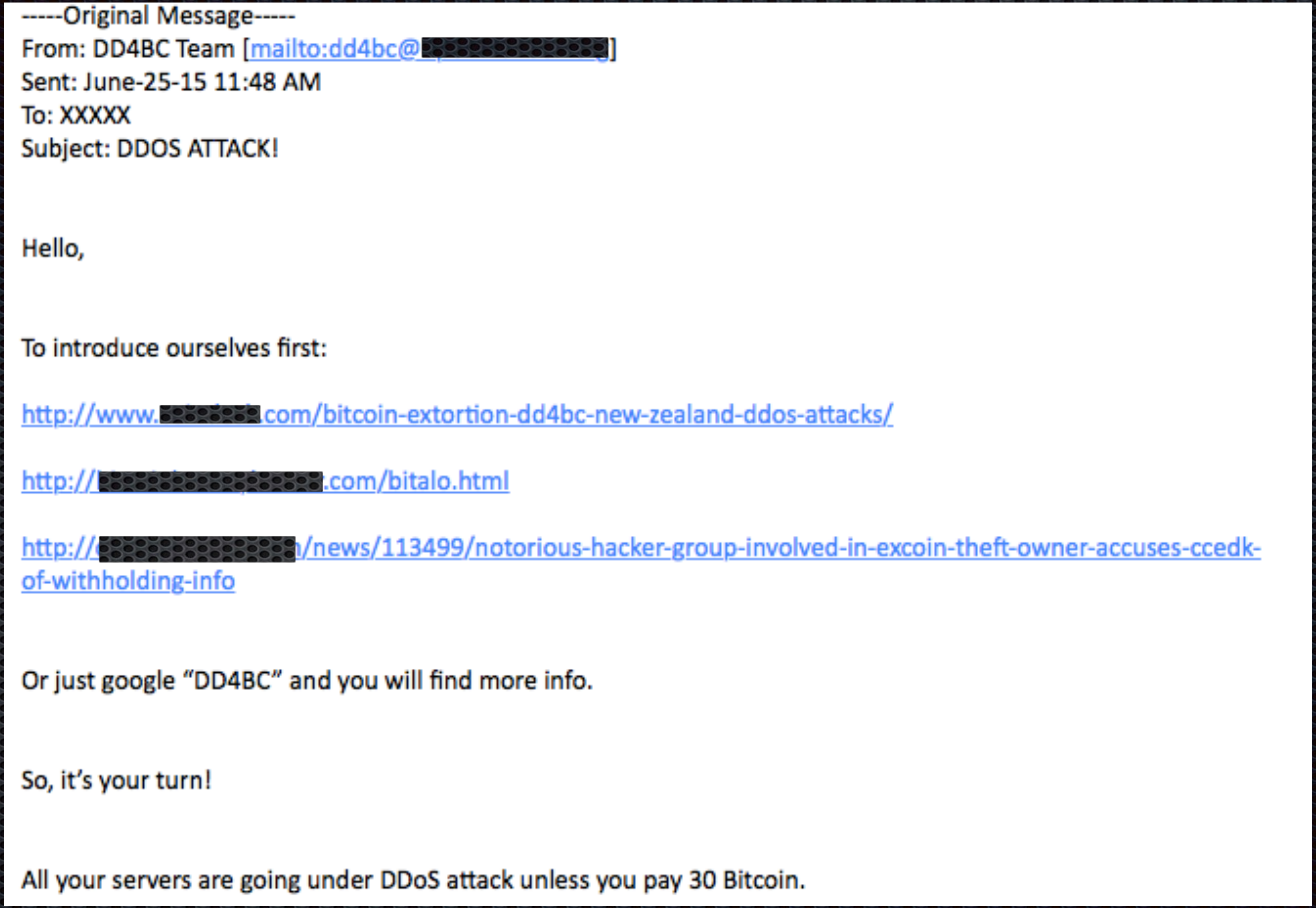



Web Application Attacks by Industry, Q1 2016
Percentage
45
40
35
30
25
20
15
10
5
0
43.42%
12.99%
12.11%
9.43%
7.22%
3.25%
3.09%
2.38%
6.10%
Retail
Hotel & Travel
Financial Services
High Technology
Media & Entertainment
Public Sector
Software as a Service
Business Services
Other

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

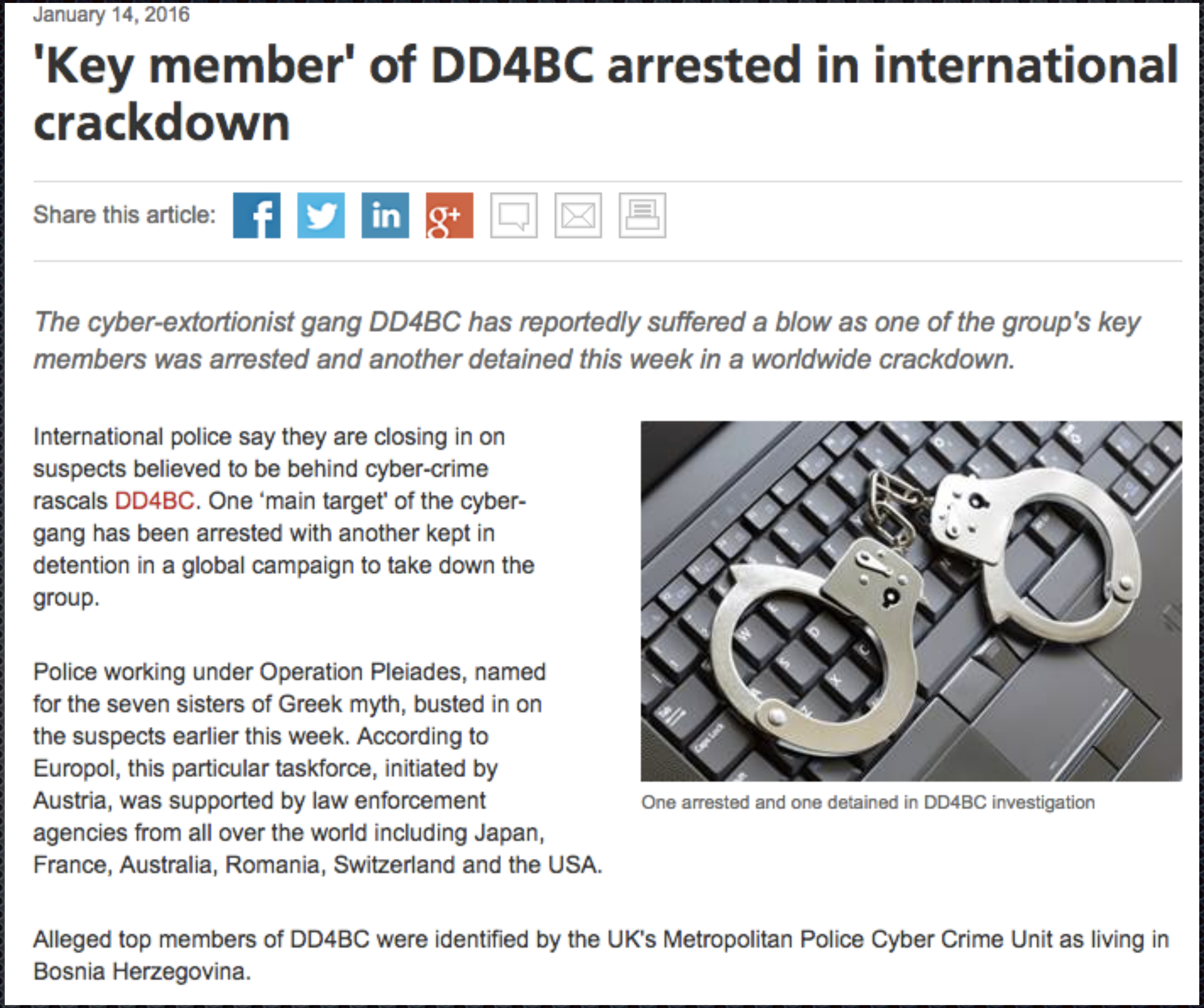
Or just google "DD4BC" and you will find more info.

So, it's your turn!

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

More recently…

- 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:

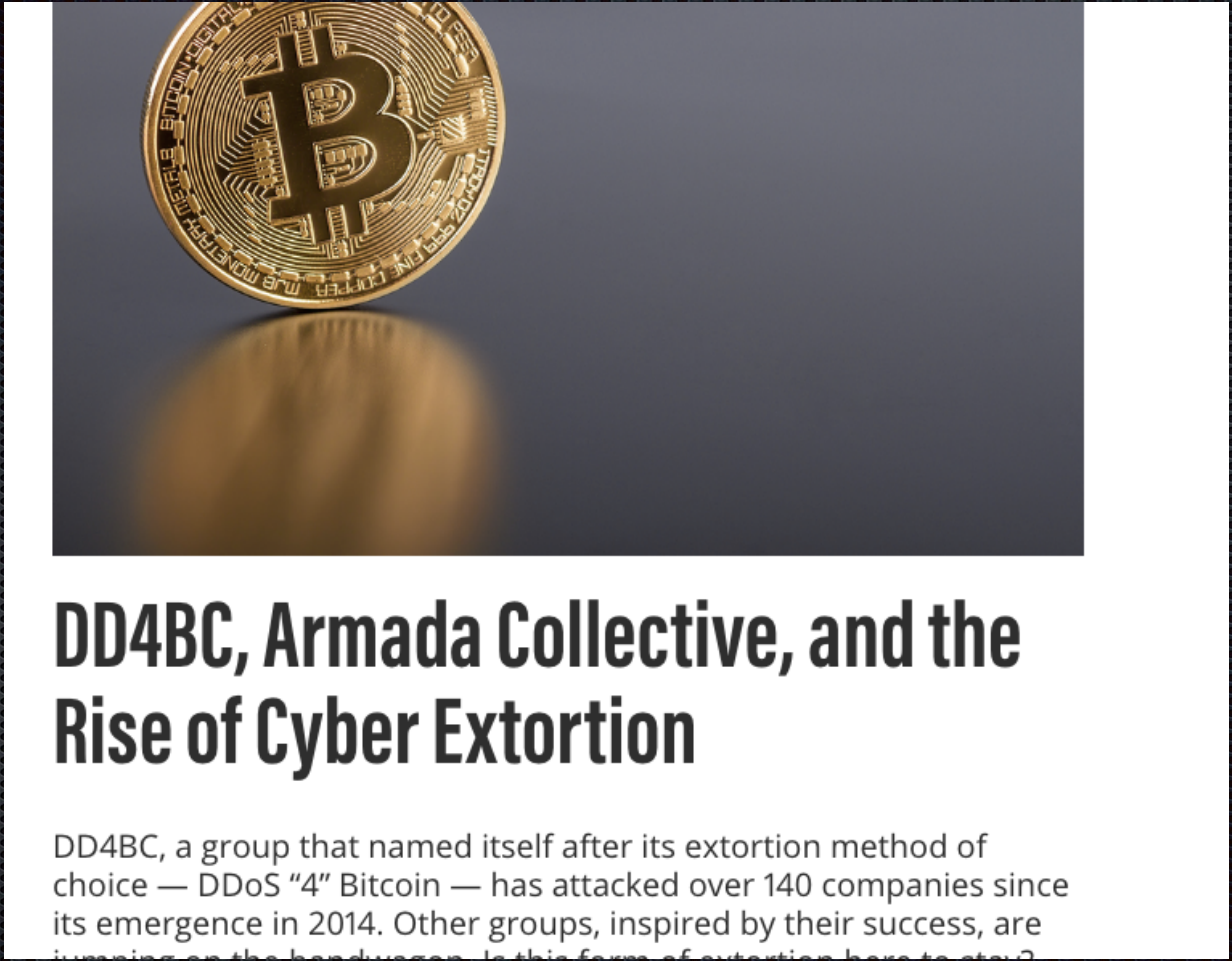
The cyber-extortionist gang DD4BC has reportedly suffered a blow as one of the group's key members was arrested and another detained this week in a worldwide crackdown.

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.

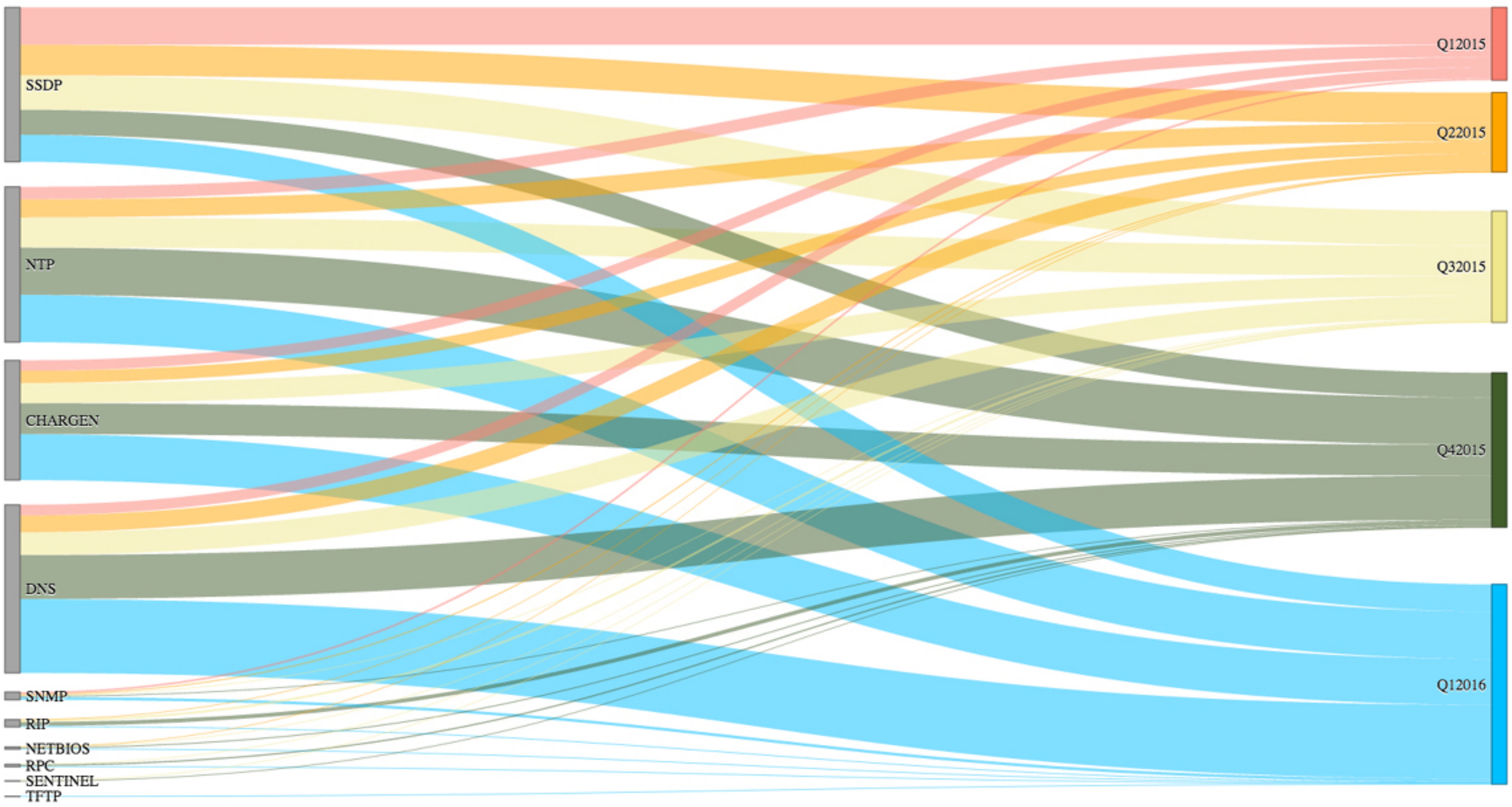


DD4BC, Armada Collective, and the Rise of Cyber Extortion

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 jumping on the bandwagon. Is this form of extortion here to stay?

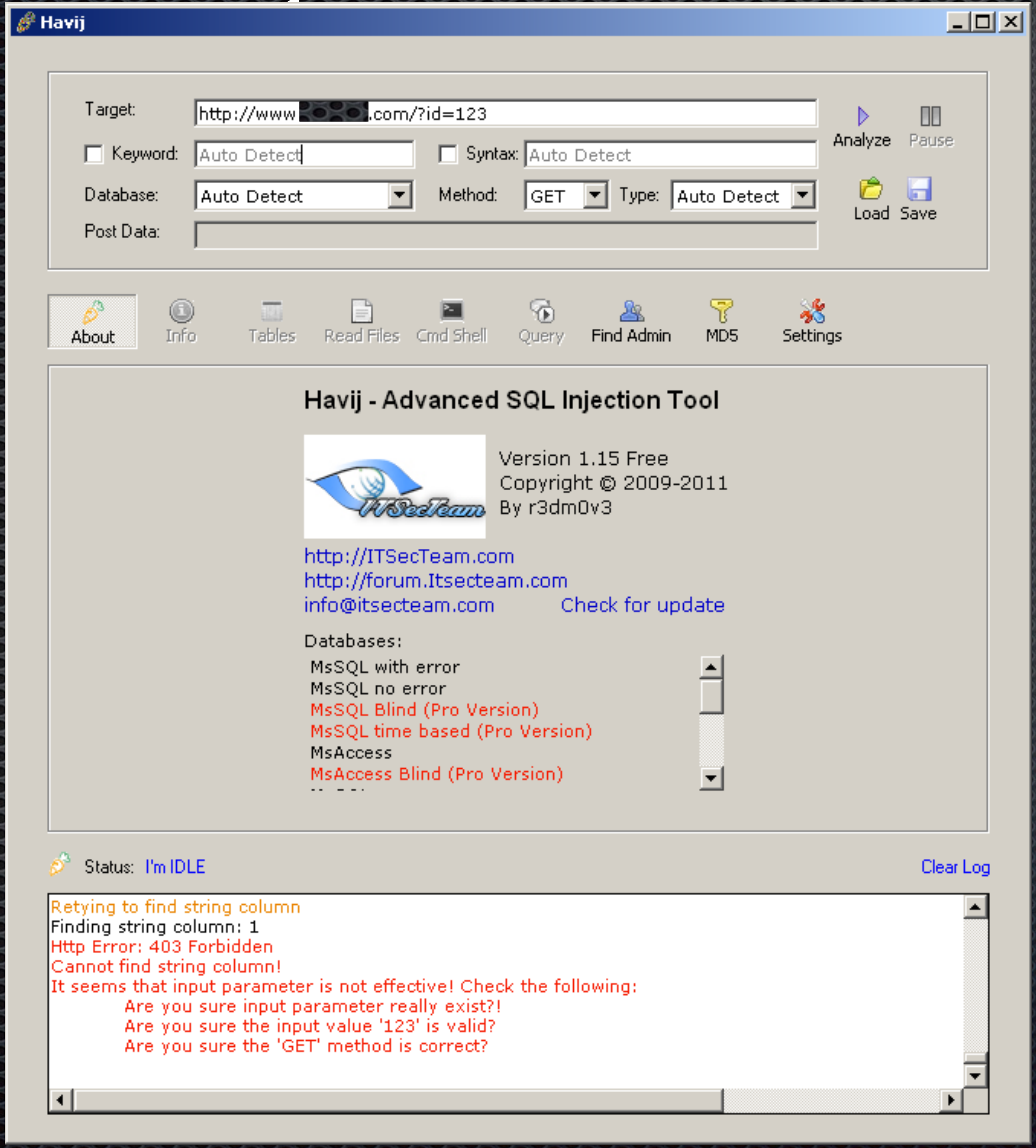
Attacks: Amplification

Reflection-Based DDoS Attacks, Q1 2015–Q1 2016



Tools

Tools: Havij



Target: http://www[redacted].com/?id=123

□ Keyword: Auto Detect

□ Syntax: Auto Detect

Database: Auto Detect

Method: GET

Type: Auto Detect

Post Data:

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

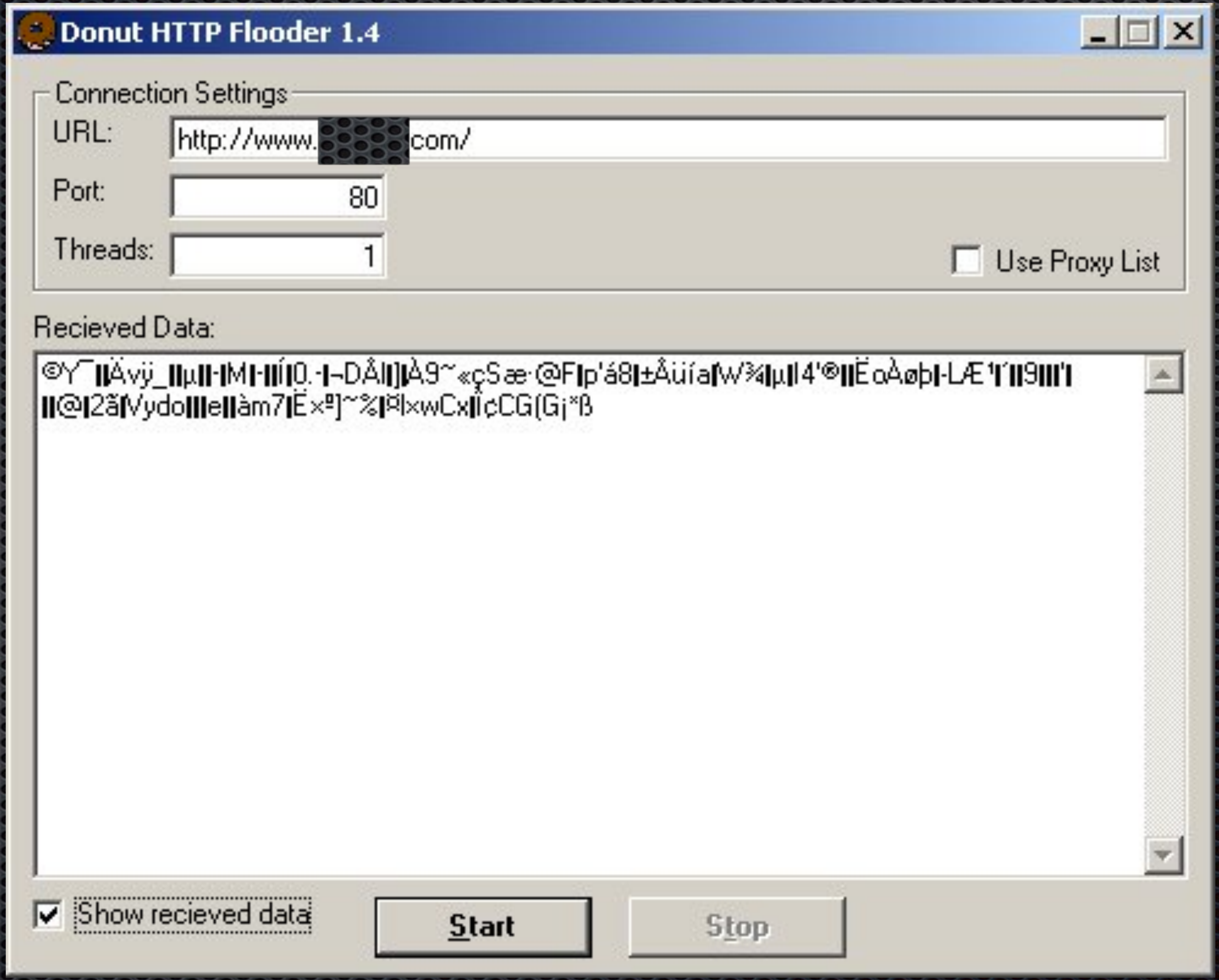
Databases:

MsSQL with error
MsSQL no error
MsSQL Blind (Pro Version)
MsSQL time based (Pro Version)
MsAccess
MsAccess Blind (Pro Version)

Status: I'm IDLE

```
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.[redacted]com/

Port: 80

Threads: 1

□ Use Proxy List

Recieved Data:

```
©Y¯▌▌Ävÿ_▌▌µ▌▌-▌M▌-▌▌Í▌0.-▌¬DÅ▌▌]▌À9~«çSæ·@F▌p'á8▌±Åüía▌W¾▌µ▌4'®▌▌ËαÀøþ▌-LÆ¹▌´▌▌9▌▌▌'▌
▌▌@▌2ã▌Vydo▌▌▌e▌▌àm7▌Ë×º]~%▌¤▌xwCx▌Ï¢CG(G¡*ß
```

☑ Show recieved data

Tools: Donut (con’t)

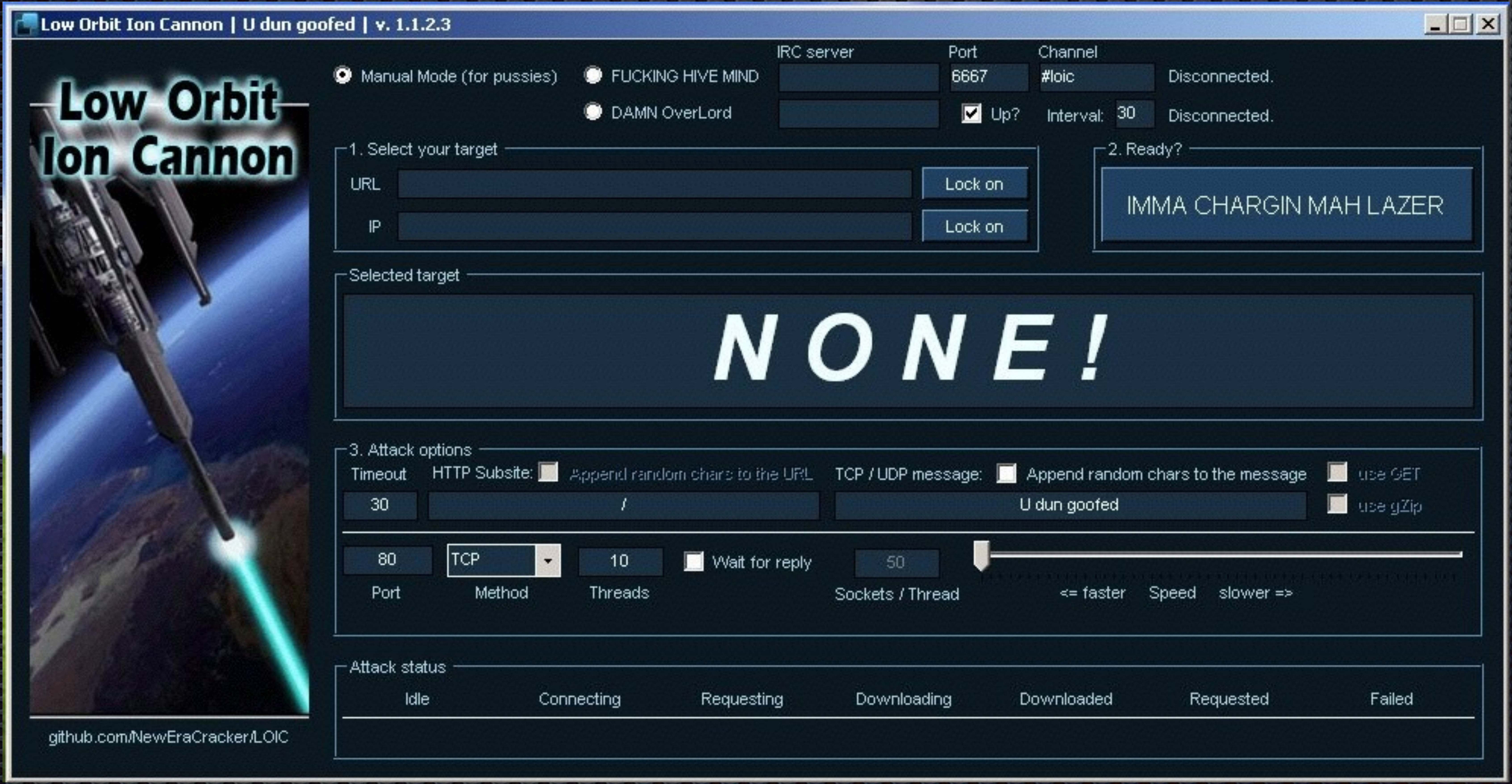
```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-powerpoint, application/vnd.ms-excel, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 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
```

Tools: LOIC



Low Orbit Ion Cannon | U dun goofed | v. 1.1.2.3

● 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

IP

2. Ready?

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

Port: 80 — Method: TCP — Threads: 10 — □ Wait for reply — Sockets / Thread: 50

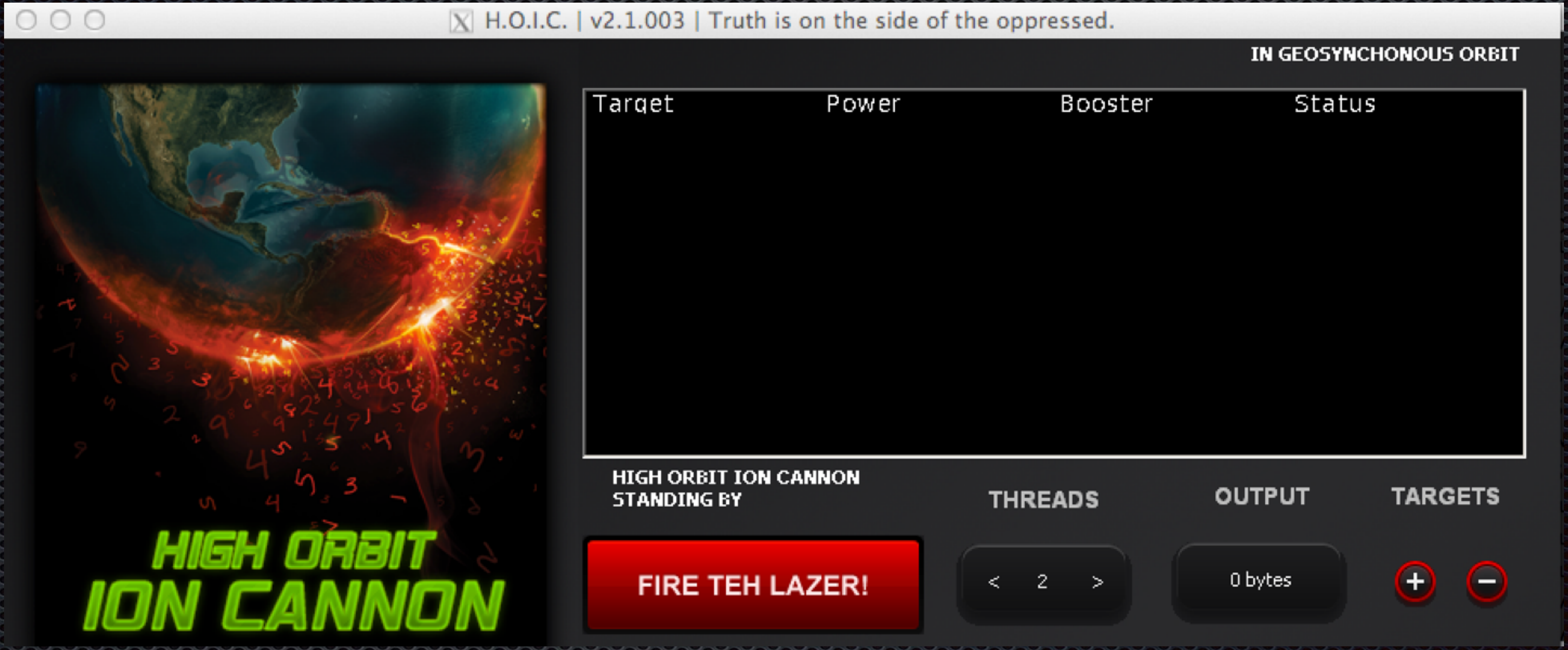
<= faster Speed slower =>

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

github.com/NewEraCracker/LOIC

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
STANDING BY

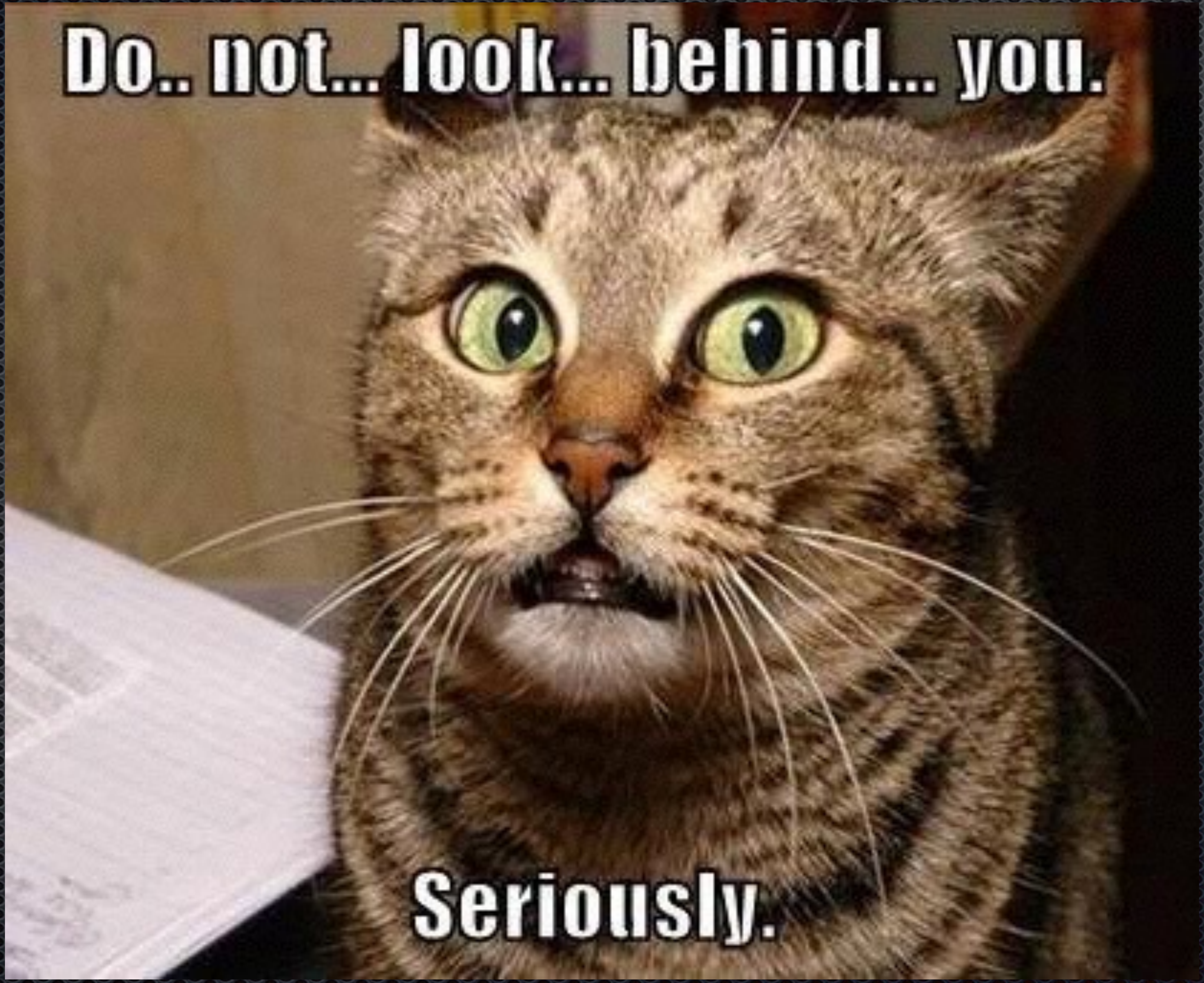
THREADS: 2

OUTPUT: 0 bytes

Tools: Brobot

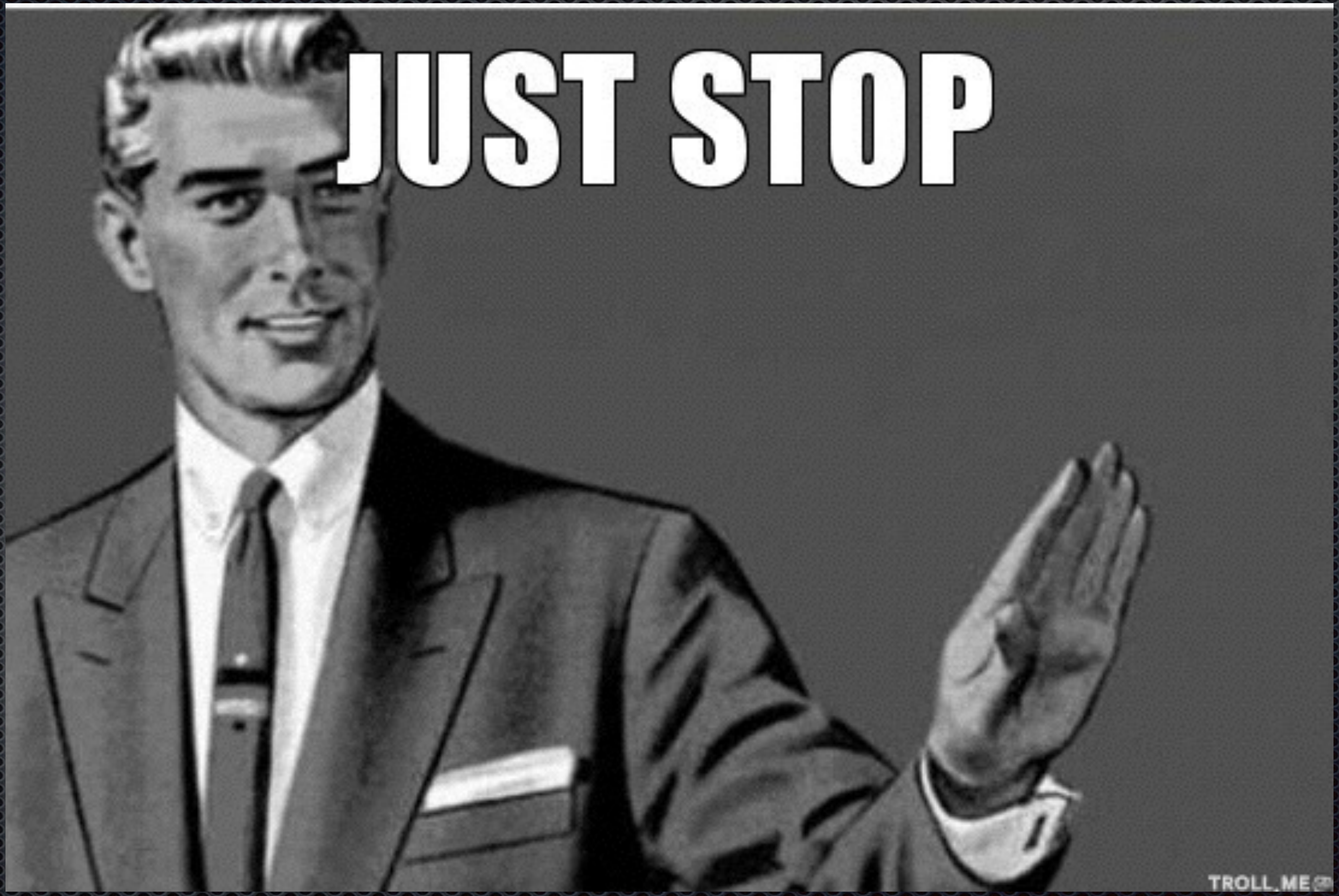
Brobot is a PHP trojan that allows an attacker to take control of a victim's compromised hosted Web server and use it to launch DDOS attacks.

Tools: WGET

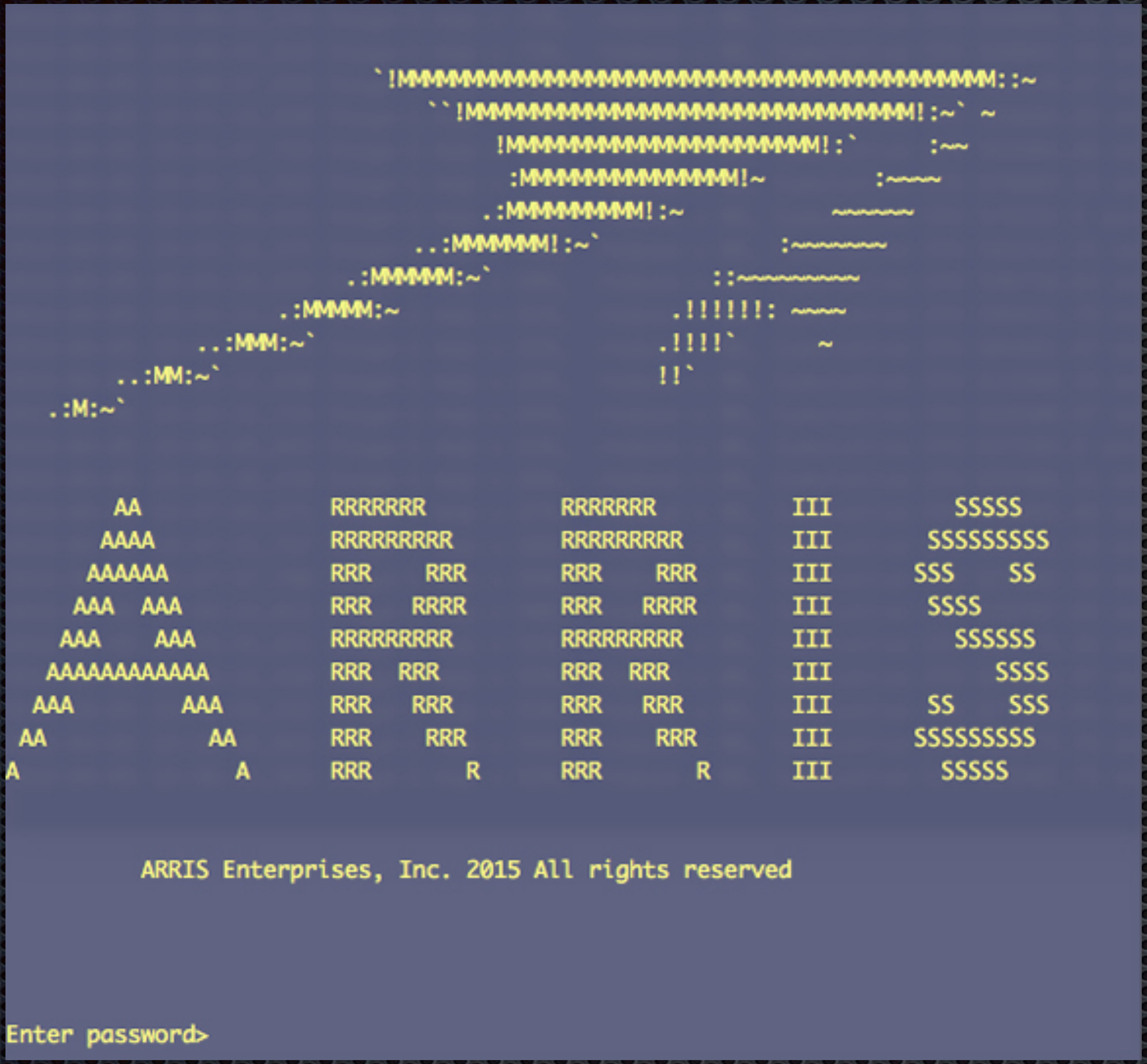


Trends

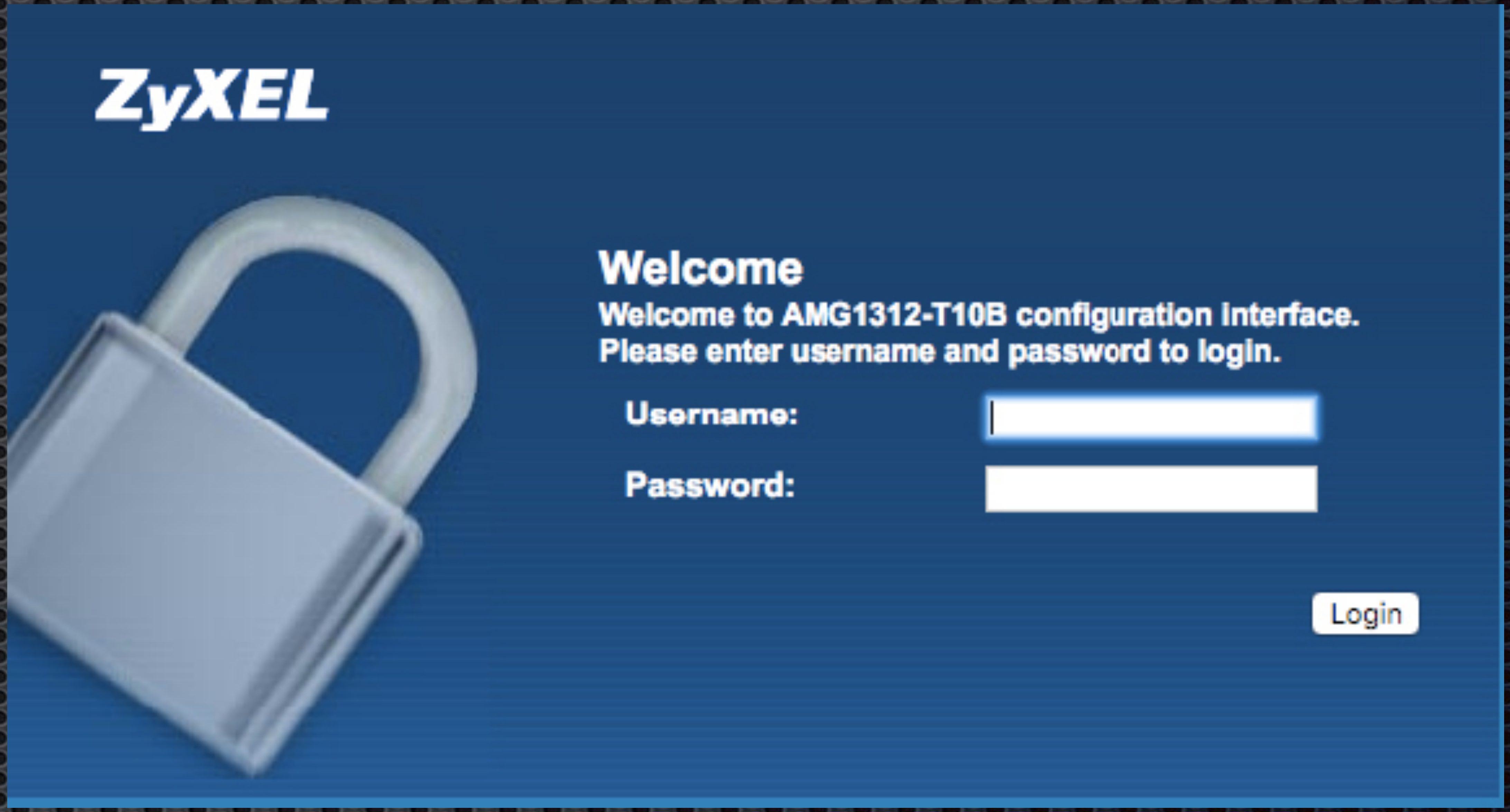
Media Grandstanding



Commoditization of DDoS



```
                           `!MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM::~
                               ``!MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM!:~` ~
                                    !MMMMMMMMMMMMMMMMMMMMMMM!:`     :~~
                                     :MMMMMMMMMMMMMMMMM!~       :~~~~
                                   .:MMMMMMMMMM!:~           ~~~~~~
                              ..:MMMMMMM!:~`             :~~~~~~~
                         .:MMMMM:~`                 ::~~~~~~~~~
                    .:MMMM:~                     .!!!!!!: ~~~~
              ..:MMM:~`                         .!!!!`      ~
        ..:MM:~`                                !!`
   .:M:~`


        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
   AAAAAAAAAAAA         RRR  RRR         RRR  RRR         III            SSSS
  AAA        AAA        RRR   RRR        RRR   RRR        III       SS    SSS
 AA            AA       RRR    RRR       RRR    RRR       III      SSSSSSSSS
A                A      RRR       R      RRR       R      III        SSSSS


          ARRIS Enterprises, Inc. 2015 All rights reserved



Enter password>
```

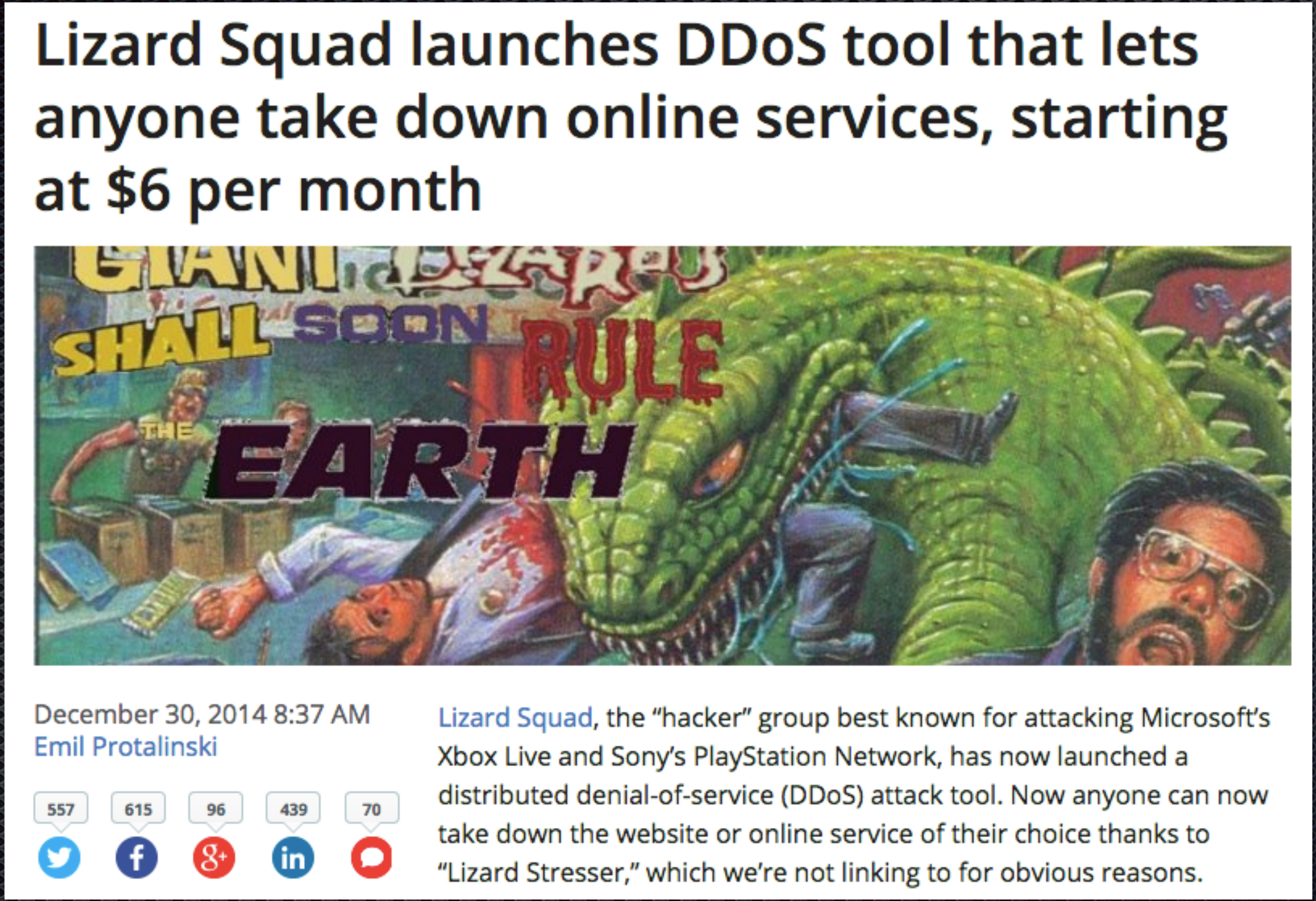


Welcome

Welcome to AMG1312-T10B configuration interface.
Please enter username and password to login.

Username:

Password:

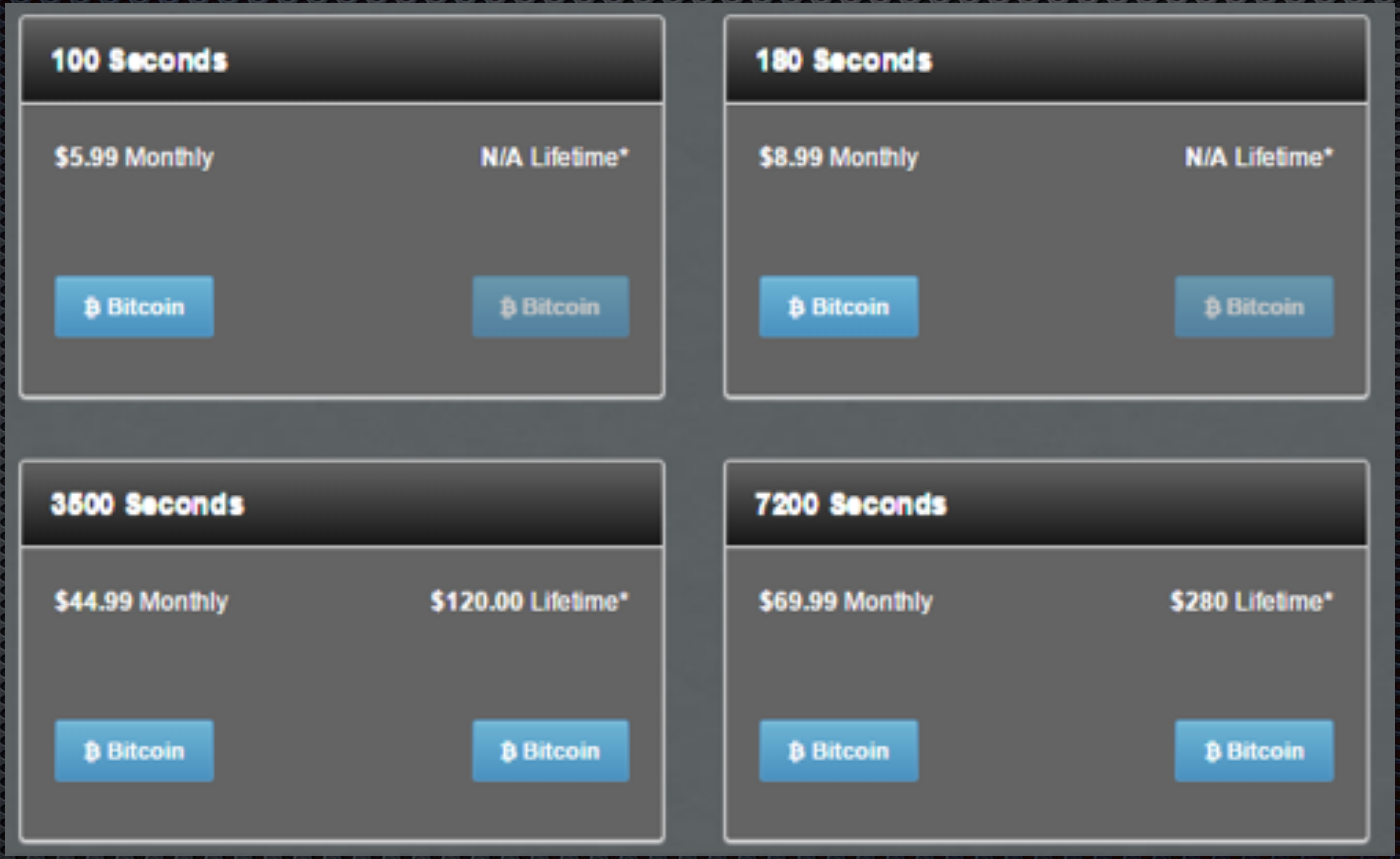


Lizard Squad launches DDoS tool that lets anyone take down online services, starting at $6 per month

December 30, 2014 8:37 AM
Emil Protalinski

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?



100 Seconds

$5.99 Monthly N/A Lifetime*

180 Seconds

$8.99 Monthly N/A Lifetime*

3500 Seconds

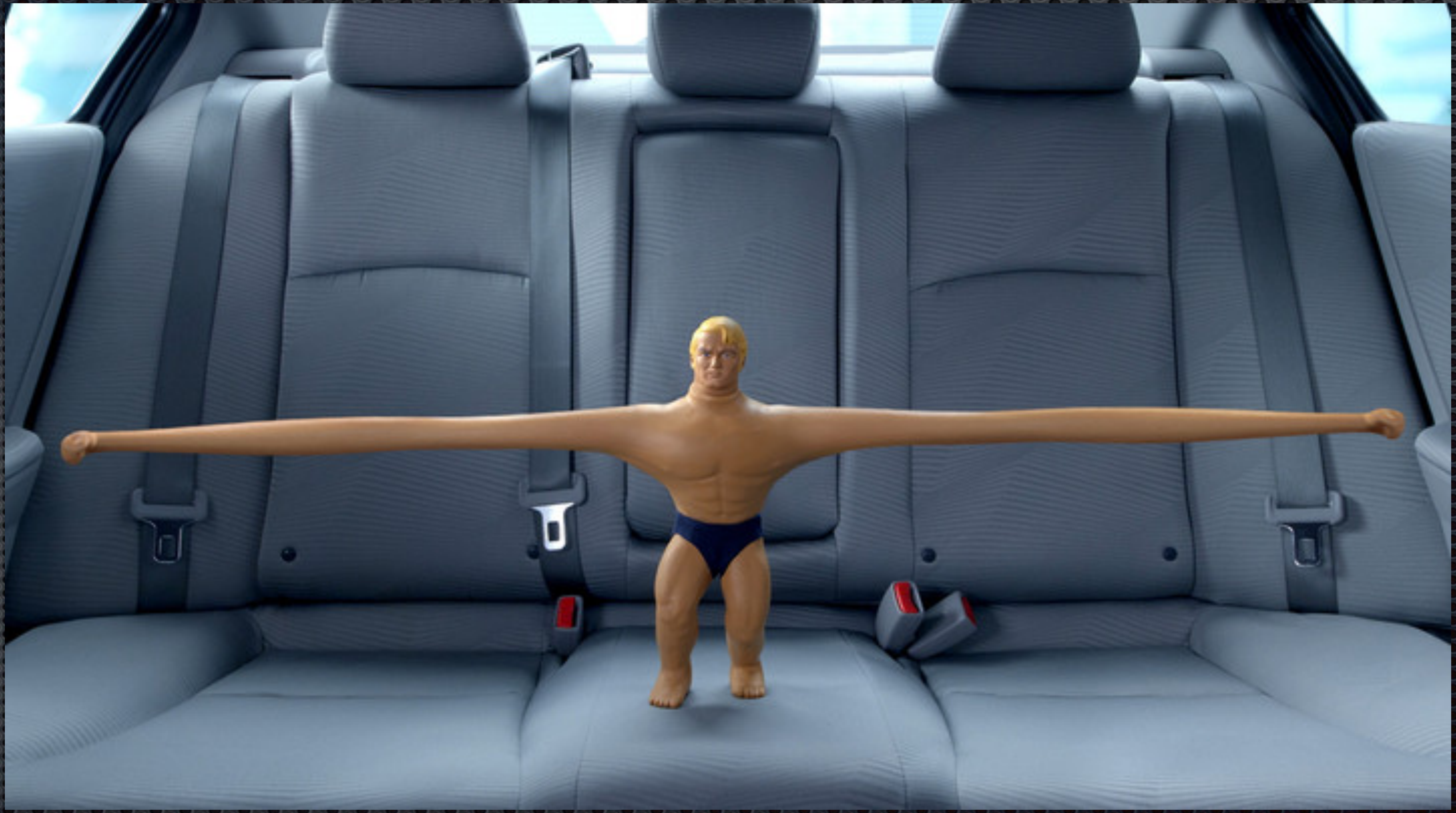
$44.99 Monthly $120.00 Lifetime*

7200 Seconds

$69.99 Monthly $280 Lifetime*

What's a Booter?

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.

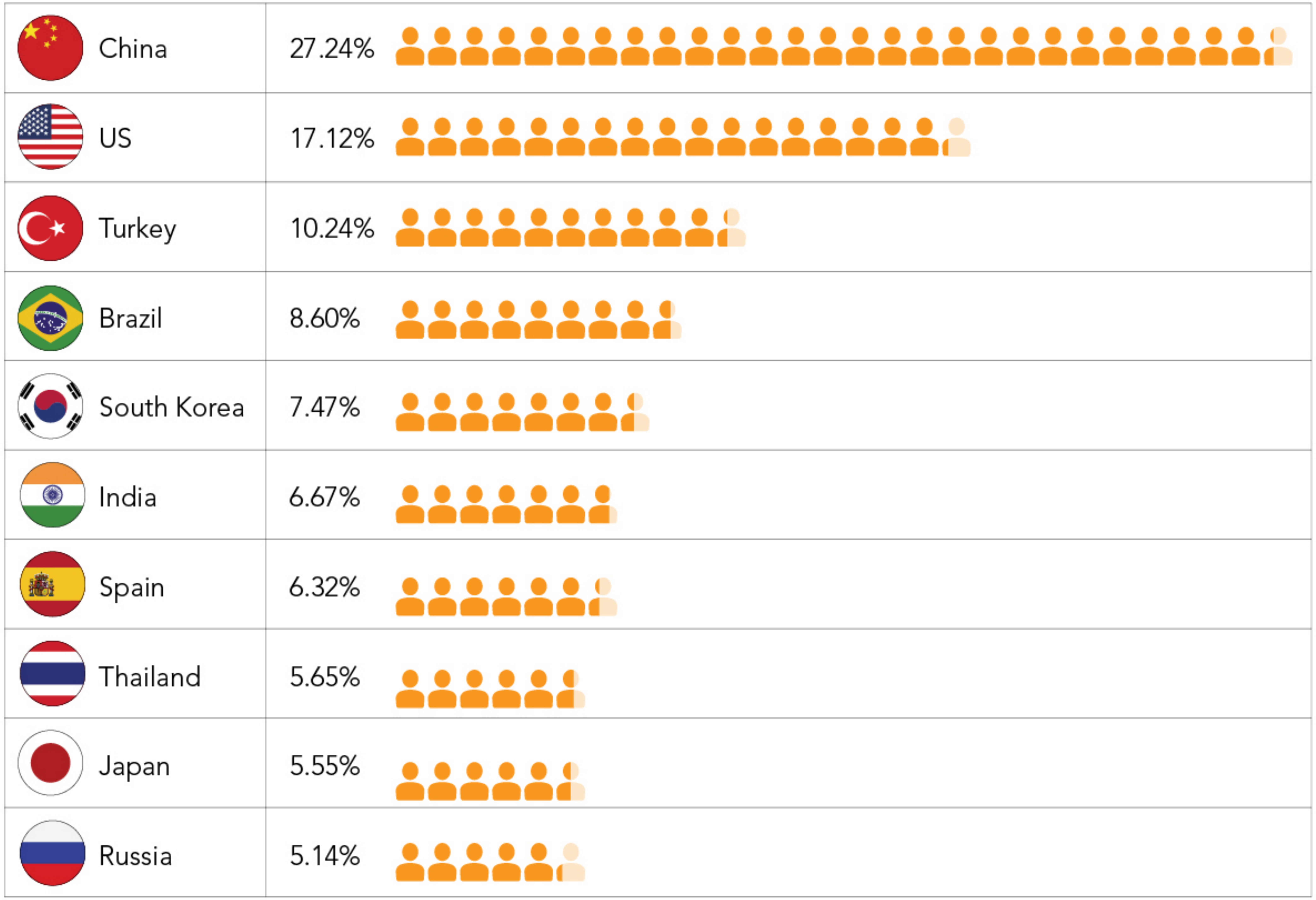
Some other highlights

- 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?

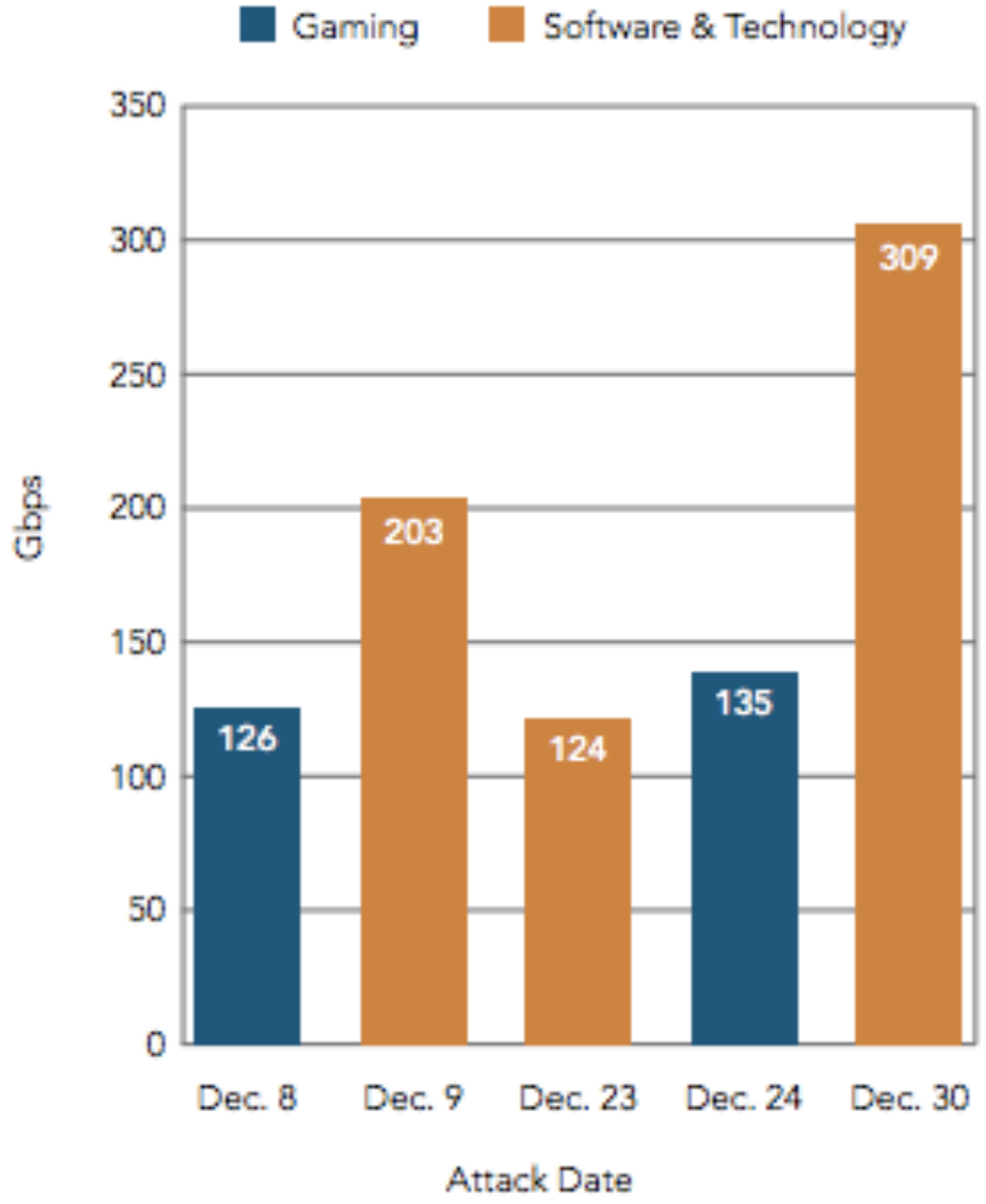
CYBER-
THEFT
CHINA

Top 10 Source Countries for DDoS Attacks, Q1 2016

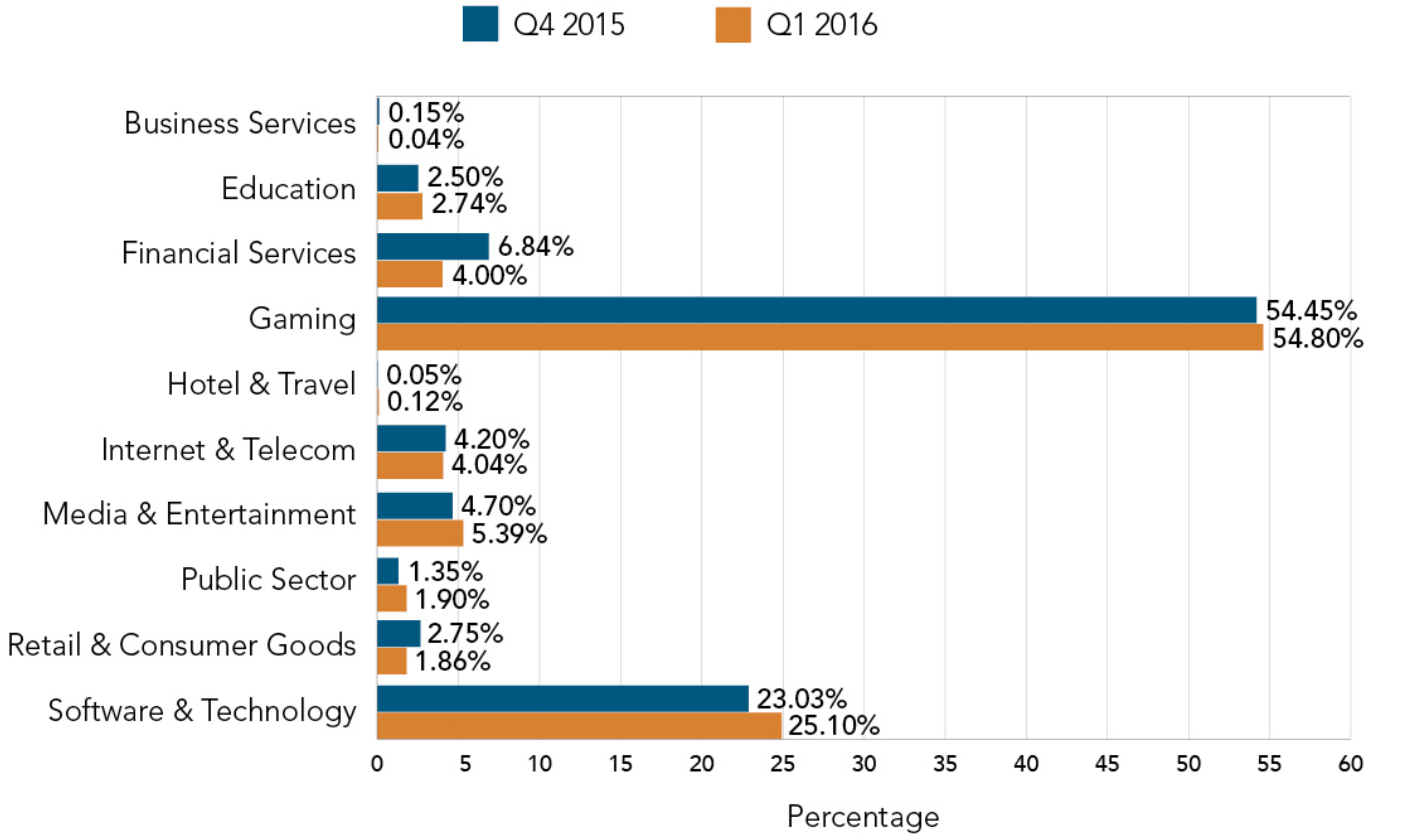


China	27.24%
US	17.12%
Turkey	10.24%
Brazil	8.60%
South Korea	7.47%
India	6.67%
Spain	6.32%
Thailand	5.65%
Japan	5.55%
Russia	5.14%

Q4 2015 DDoS Attacks > 100 Gbps



DDoS Attack Frequency by Industry, Q1 2016



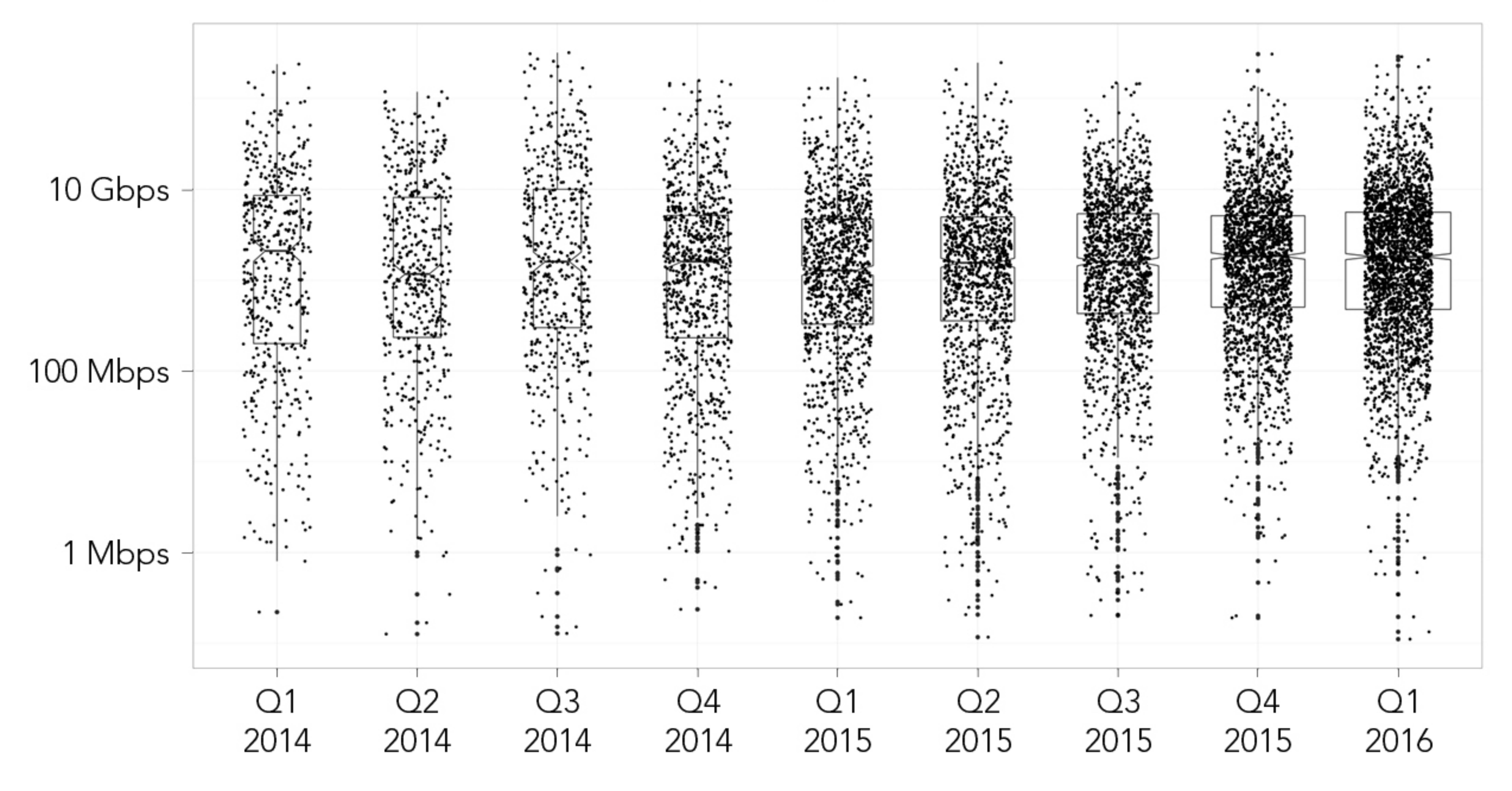
Akamai

MEGA MEGA MEGA

These large attacks all contained SYN floods

```
12:34:04.270528 IP X.X.X.X.54202 > Y.Y.Y.Y.80: Flags [S], seq
1801649395:1801650365, win 64755, length 970

....E.....@...}.
6.....6....Pkb......P...c......................................................................
<snip>.....................................................
```

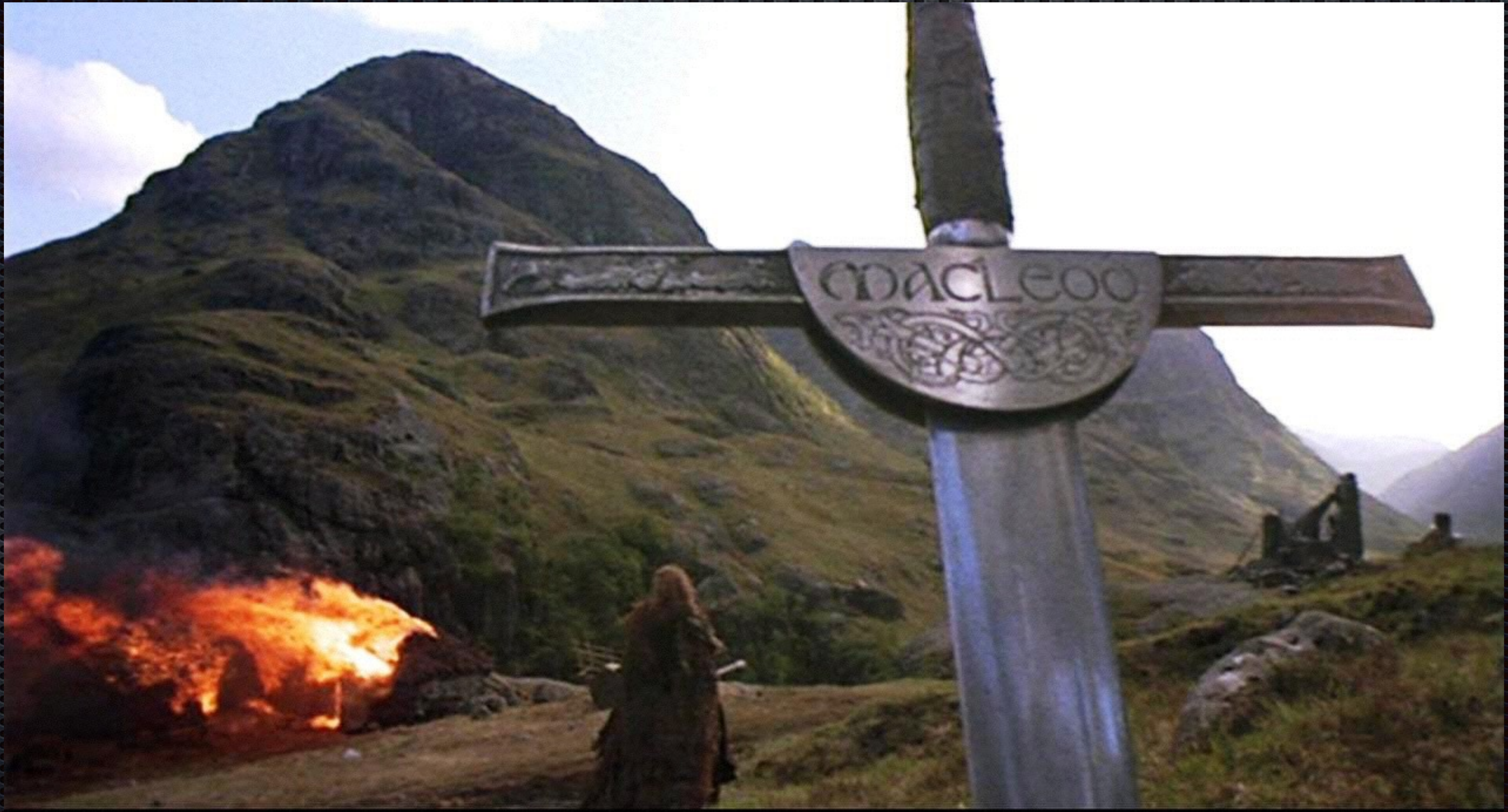
DDoS: Function of Time

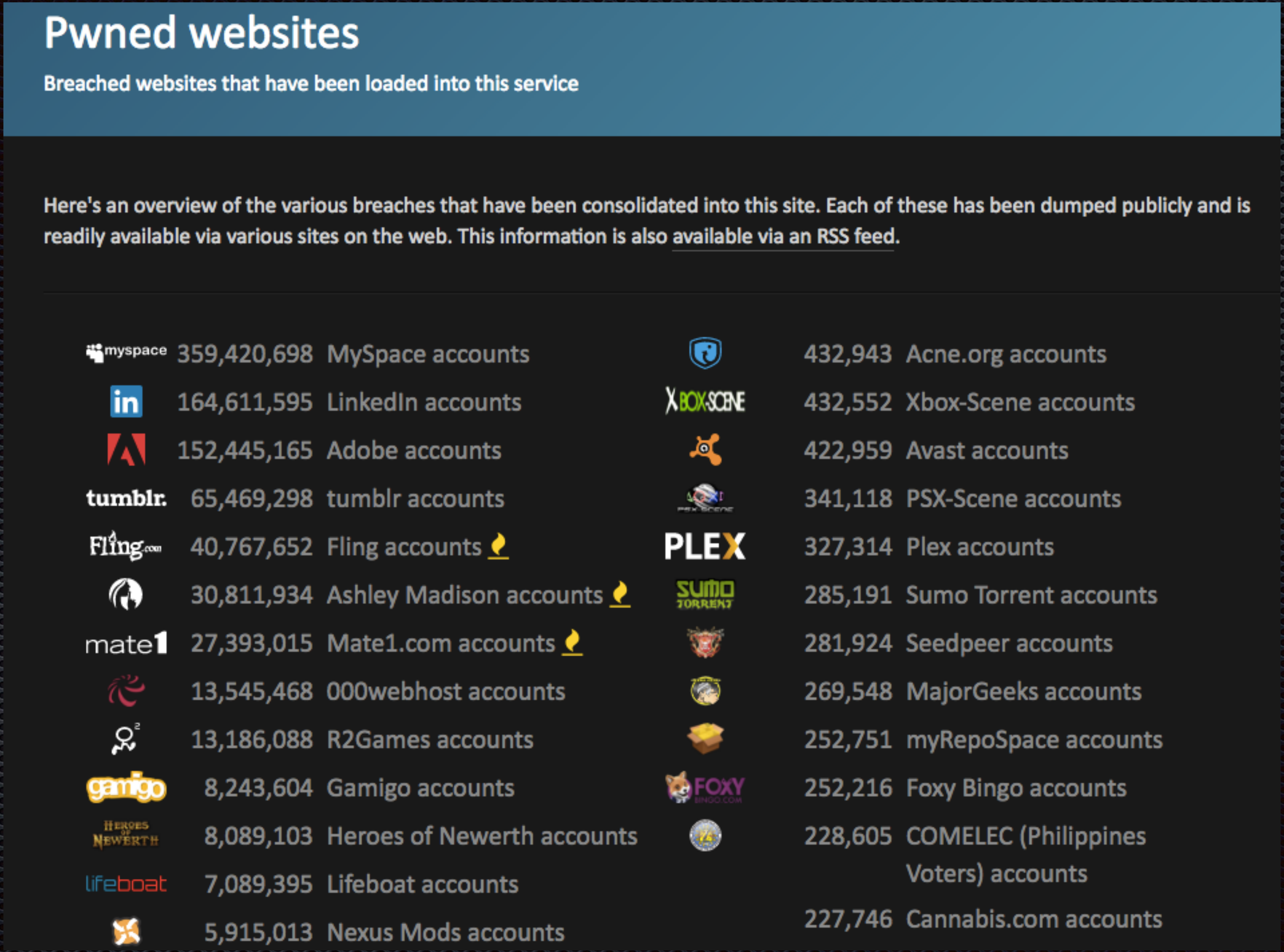


Other Observations

- SQLi
- Local/Remote File Inclusion
- Popping shells
- PHP Injection
- Malicious File upload
- JAVA …best remote access platform ever!

SQL Injection…still





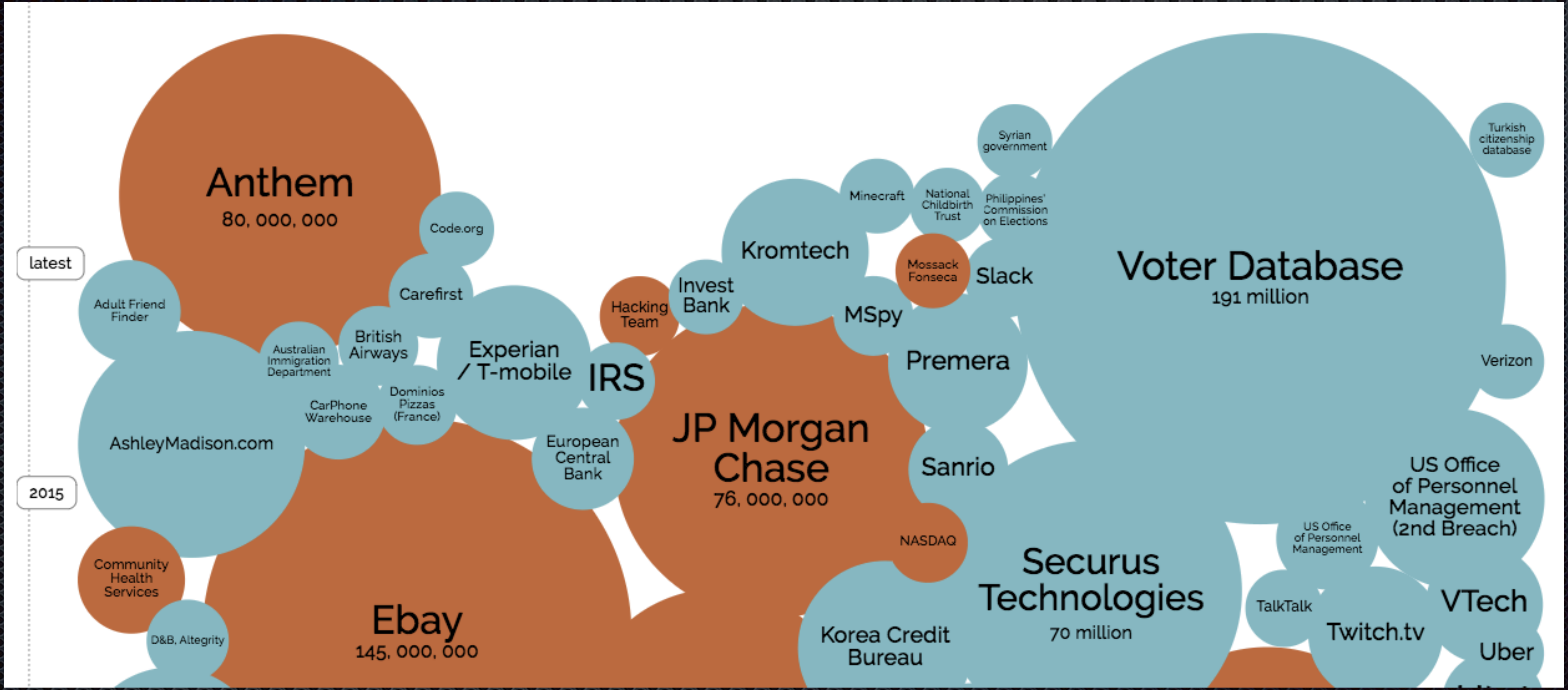
Pwned websites

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.

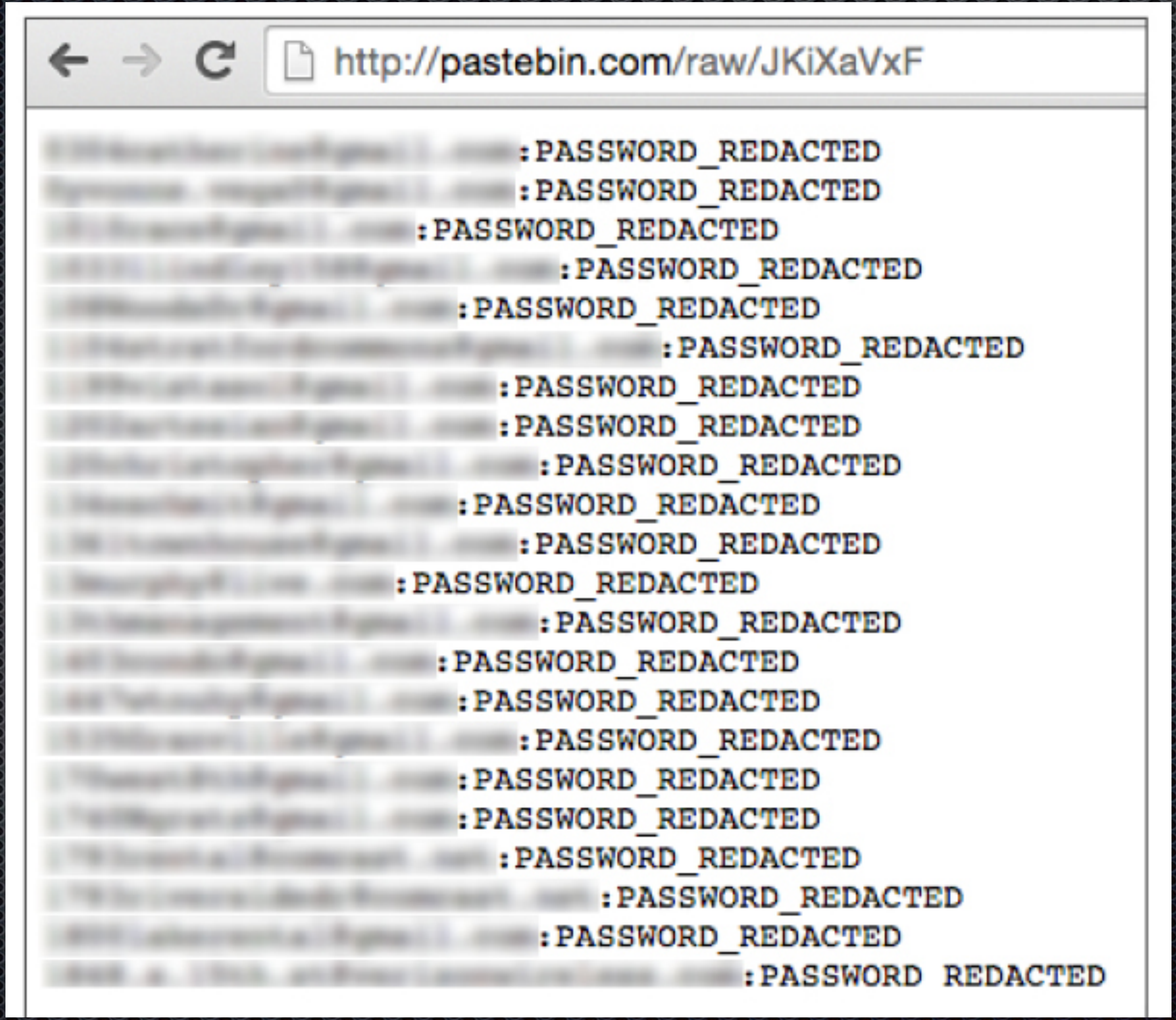
359,420,698	MySpace accounts	432,943	Acne.org accounts
164,611,595	LinkedIn accounts	432,552	Xbox-Scene accounts
152,445,165	Adobe accounts	422,959	Avast accounts
65,469,298	tumblr accounts	341,118	PSX-Scene accounts
40,767,652	Fling accounts 🔥	327,314	Plex accounts
30,811,934	Ashley Madison accounts 🔥	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		

Why this is a problem.

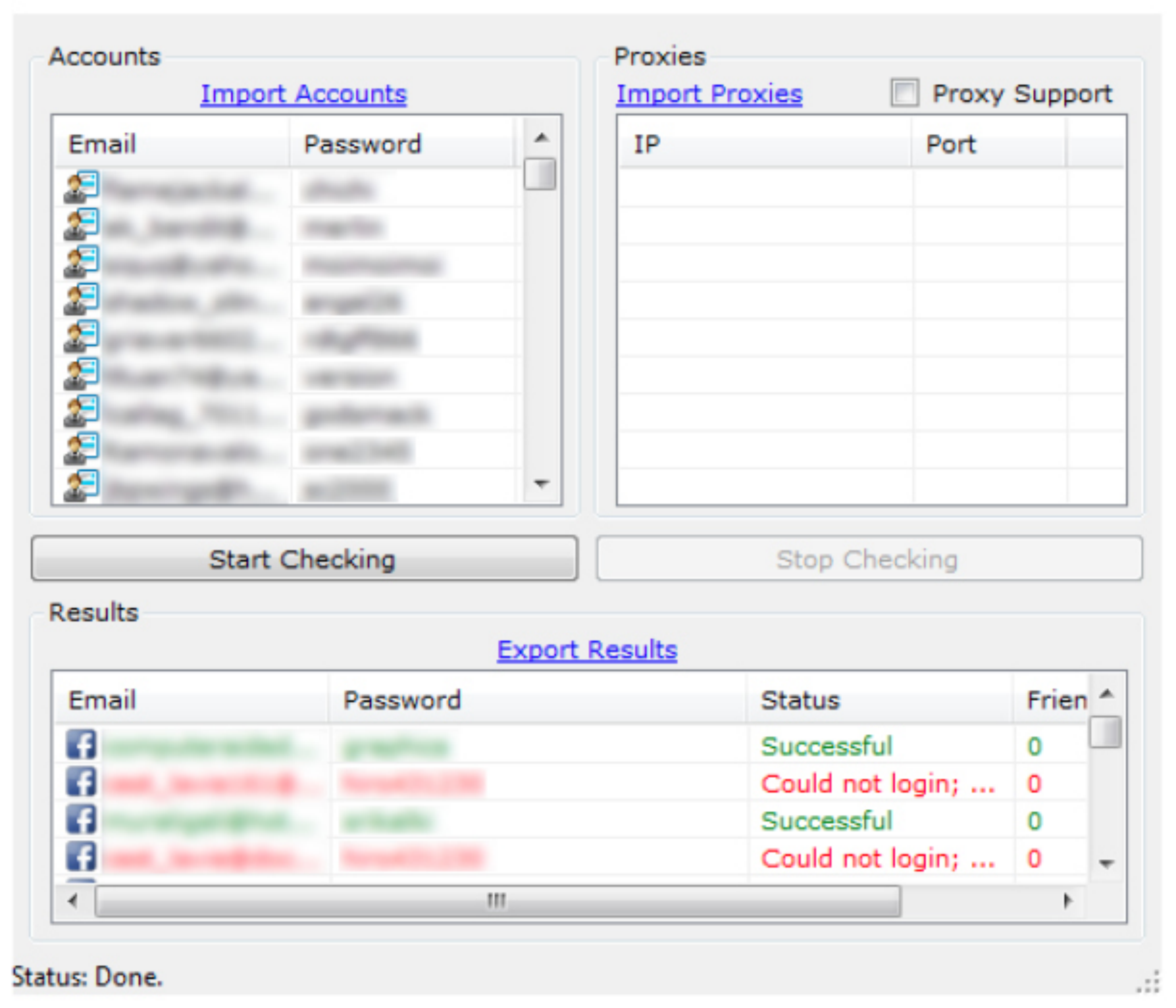


Akamai

Passwords



```
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD_REDACTED
[redacted]:PASSWORD REDACTED
```



Accounts

Import Accounts

Email	Password
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Proxies

Import Proxies ☐ Proxy Support

IP	Port

Start Checking

Stop Checking

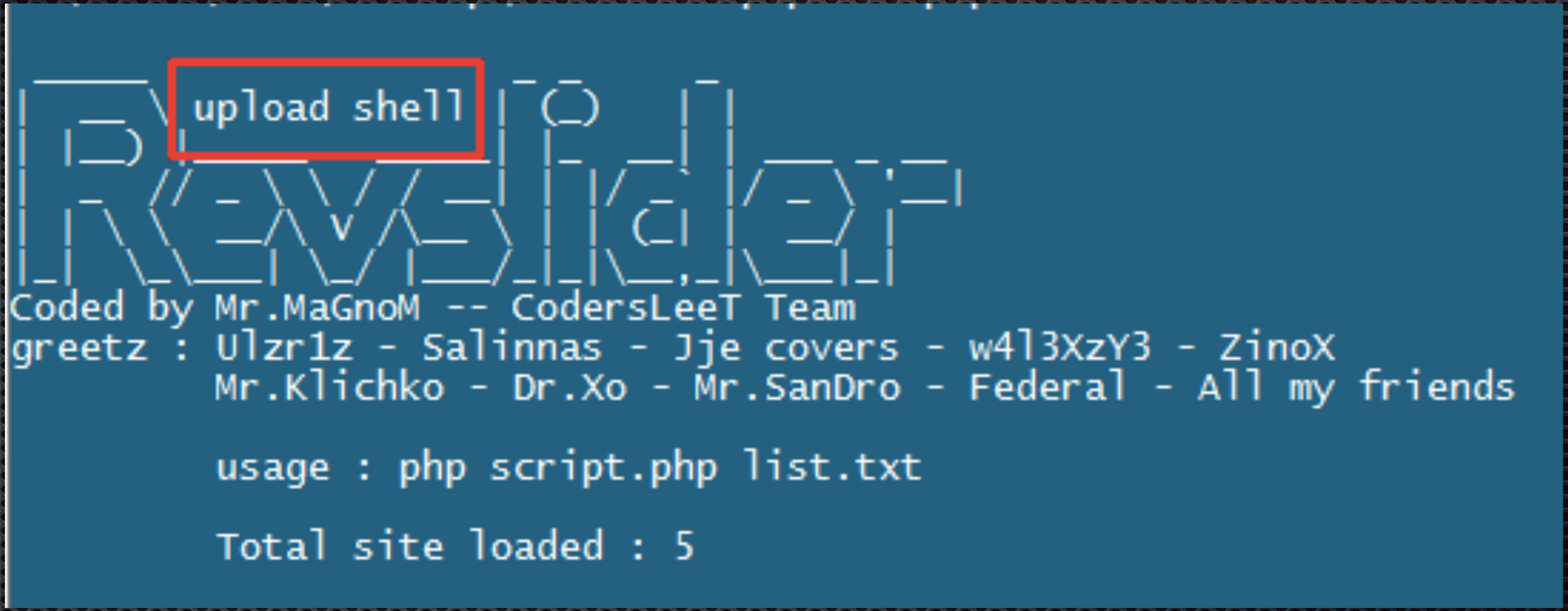
Results

Export Results

Email	Password	Status	Frien
[redacted]	[redacted]	Successful	0
[redacted]	[redacted]	Could not login; ...	0
[redacted]	[redacted]	Successful	0
[redacted]	[redacted]	Could not login; ...	0

Status: Done.

File Inclusions



upload shell

```
Coded by Mr.MaGnoM -- CodersLeeT Team
greetz : Ulzr1z - Salinnas - Jje covers - w4l3XzY3 - ZinoX
         Mr.Klichko - Dr.Xo - Mr.SanDro - Federal - All my friends

         usage : php script.php list.txt

         Total site loaded : 5
```

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

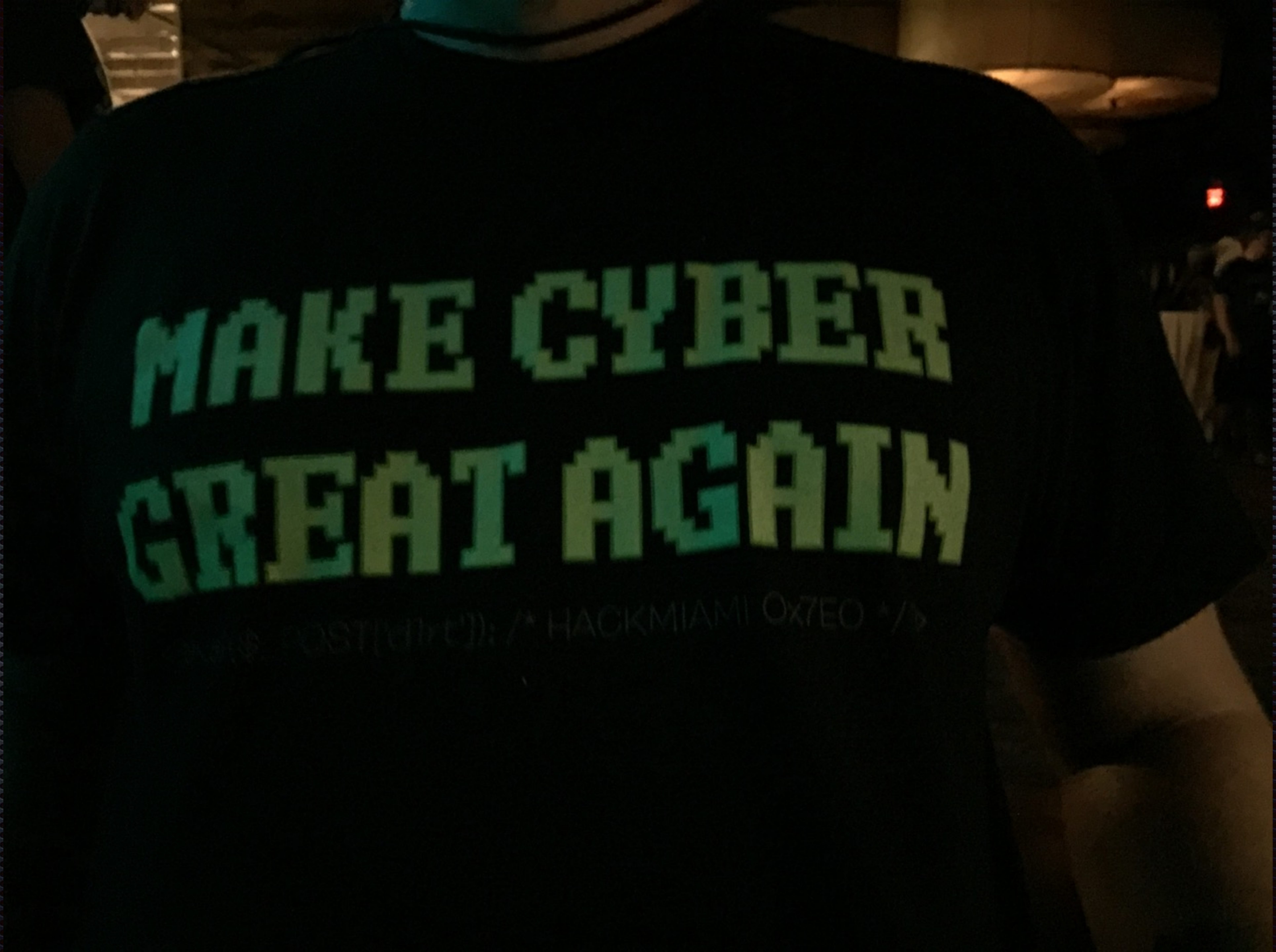
So, what to do?

- 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

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

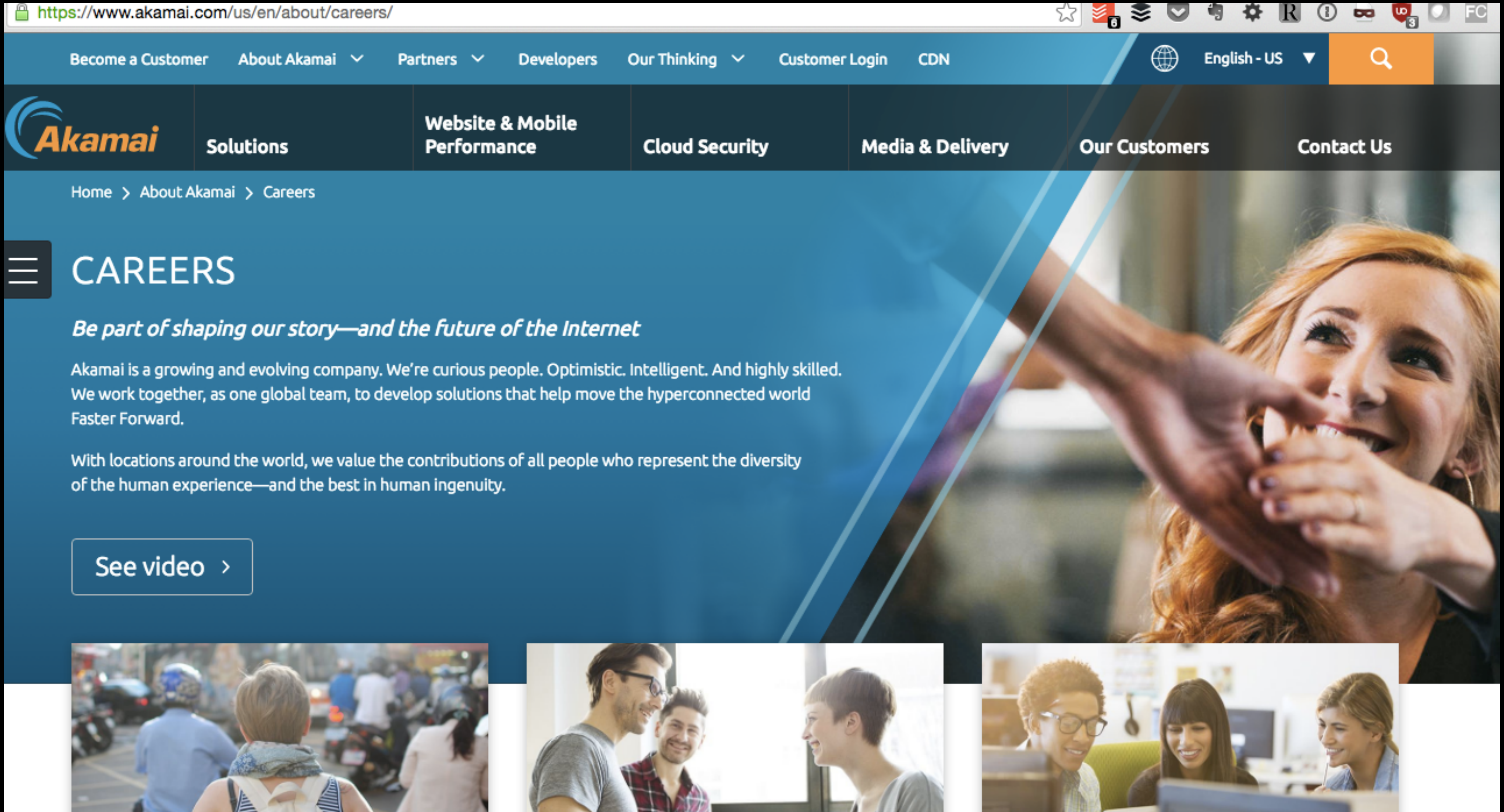
[state of the internet] brought to you by Akamai

STATEOFTHEINTERNET.COM


MAKE CYBER
GREAT AGAIN
$_POST['c']); /* HACKMIAMI 0x7E0 */>

AND WITH THAT...

AKAMAI IS HIRING!



https://www.akamai.com/us/en/about/careers/

CAREERS

Be part of shaping our story—and the future of the Internet

Akamai is a growing and evolving company. We're curious people. Optimistic. Intelligent. And highly skilled. We work together, as one global team, to develop solutions that help move the hyperconnected world Faster Forward.

With locations around the world, we value the contributions of all people who represent the diversity of the human experience—and the best in human ingenuity.

Thanks

THANKS FOR LISTENING

고맙습니다　QUESTIONS?

Akamai

FASTER FORWARD

Questions?
Thanks

Dave Lewis
@gattaca

dave@akamai.com