RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: SPO-F02

DDoS: Barbarians at the Gate(way)

Dave Lewis

Global Security Advocate
Akamai Technologies
@gattaca

Agenda

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

How This Applies To You

- Overall Actions:
  - Gain an understanding of your adversary
  - Learn the security landscape from the data
- Specific Actions:
  - Review what are you doing for DDoS prevention?
  - Have you assessed the risk to your environment?
  - Quantify the expected financial loss due to an outage to your site?

Actors: For Hire

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.
Browse
OR
Start a Project for Free

Actors: Bored Kids

Actors: Hacktivists

Actors: Nation States

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.

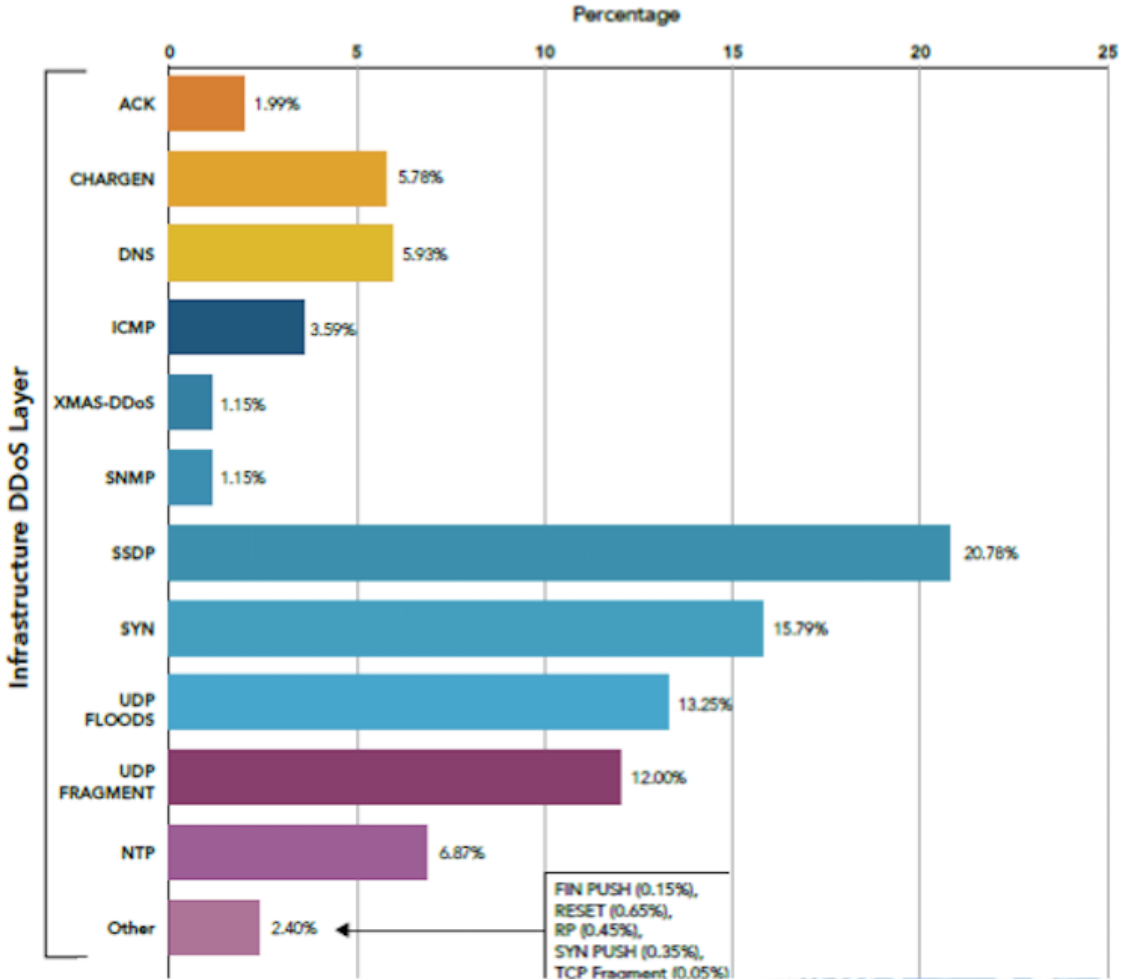
Attacks

Types of Attacks

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

Attacks: Volumetric

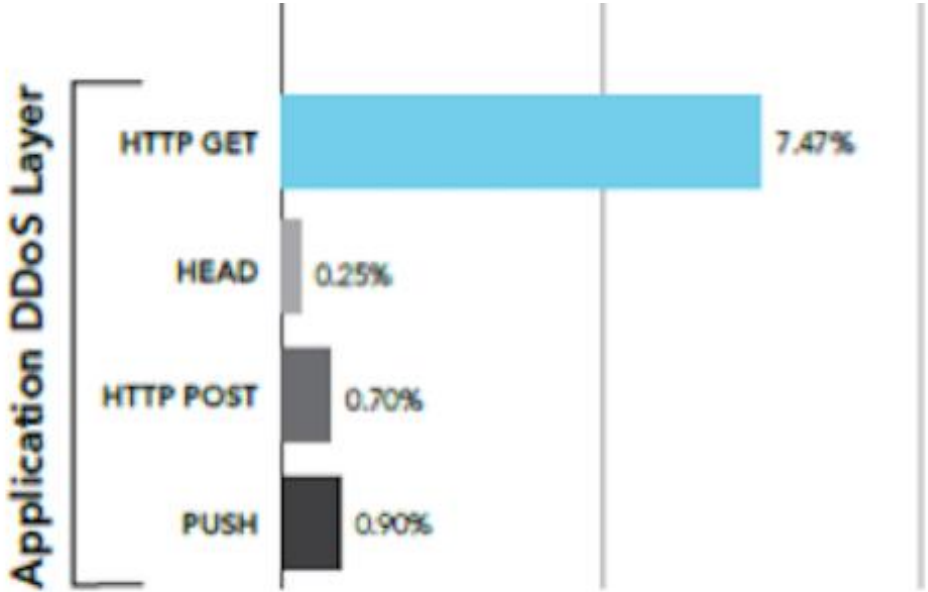
Types of DDoS attacks and their relative distribution in Q1 2015

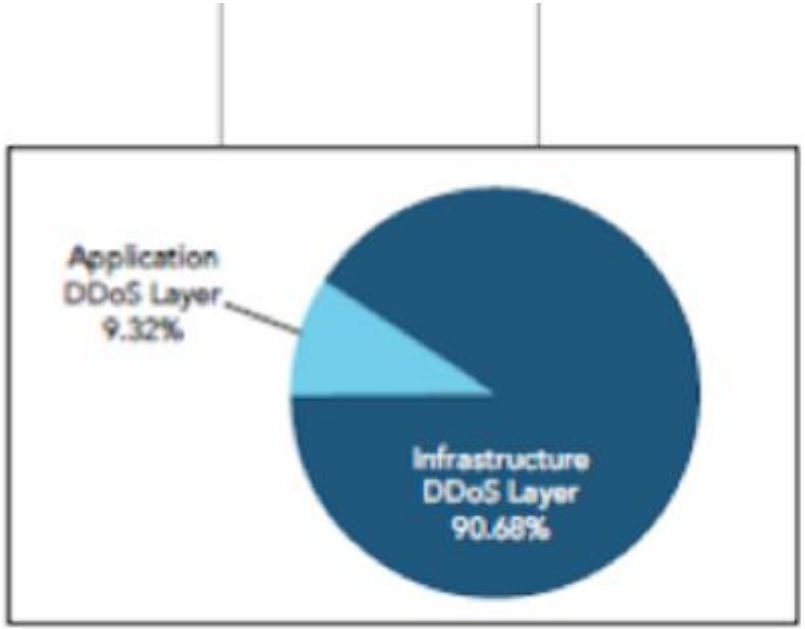


Simple Service Discovery Protocol (SSDP)

Attacks: Application Layer

Application Attacks





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 were quiet for a while, now have returned

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

Hello,

To introduce ourselves first:

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

http:// :com/bitalo.html

http:// /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.

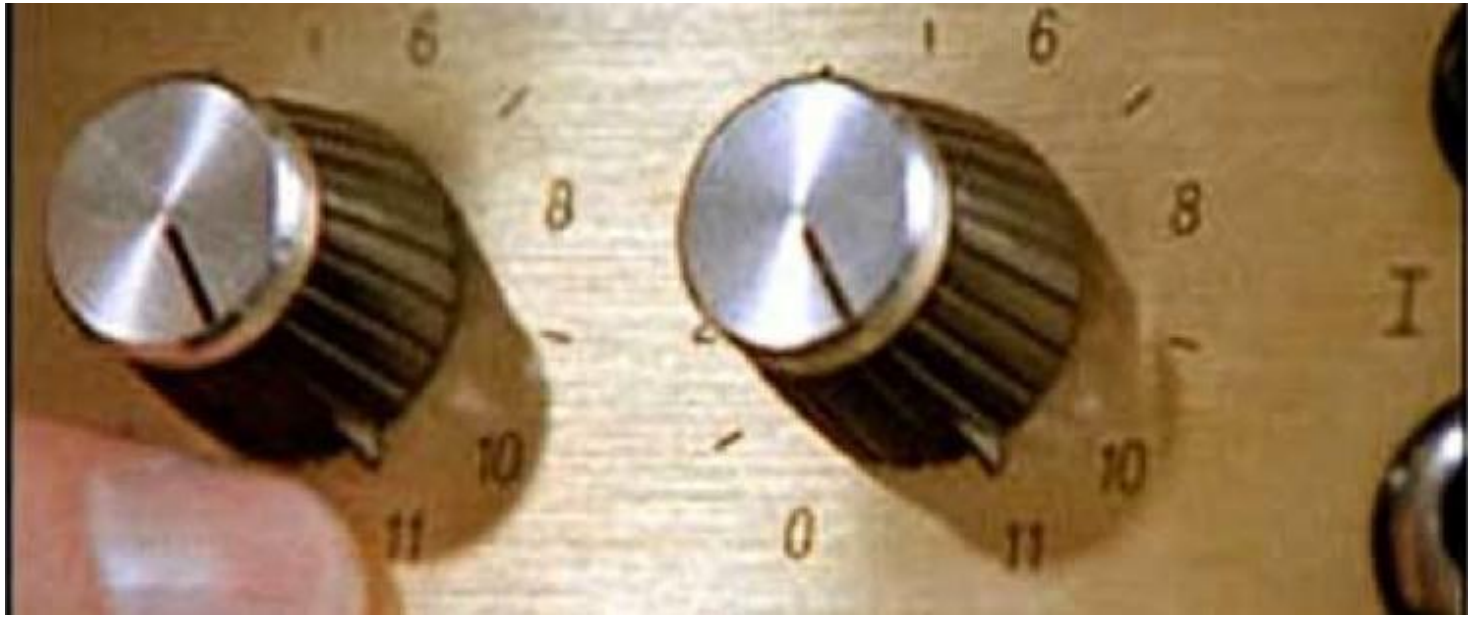
So, it's your turn!

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 in early May.

Attacks: Amplification



Anatomy of an attack

- Peak bandwidth: 4.3 Gigabits per second (Gbps)
- Attack vectors: DNS reflection and amplification
- Source: port(s): 53
- Destination port(s): 80, random

Sample Intercepted Packet

21:38:55.972524 IP X.X.X.X.53 > X.X.X.X.52967: 5856 13/0/3 A 50.63.202.58, NS ns71.somedomain.com., NS ns72.somedomain.com., SOA, MX mailstore1.example.net. 10, MX smtp.example.net. 0, TXT "President Obama is taking action to help ensure opportunity for all Americans. President Obama Signing <snip>

13:43:36.094522 IP X.X.X.X.53 > X.X.X.X.52506: 11532 10/13/16 TXT "Presidenftxt Obama is taking action <snip> ", TXT[|domain]

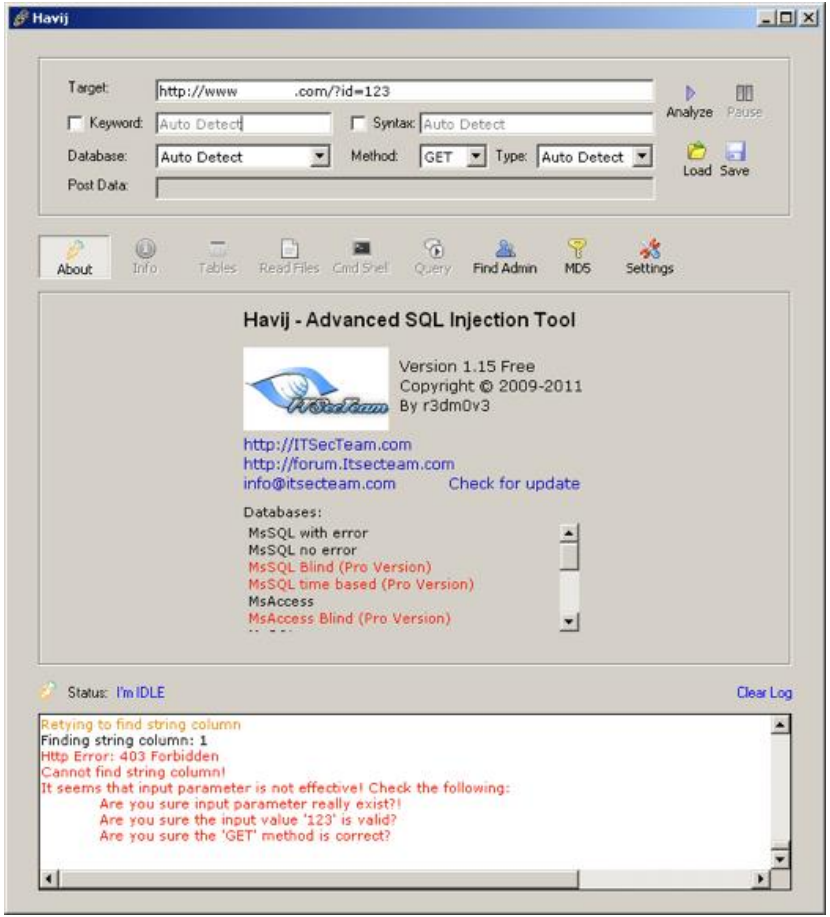
13:43:36.094854 IP X.X.X.X.53 > X.X.X.X.5926: 35408 10/13/16 TXT "<snip> President also outlines" " the details about the transmission and treatment of Ebola", TXT[|domain]

Tools

Weapons Locker

- Volumetric
- SQLi
- Scanners

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: 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: Torshammer

```
/*
* Tor's Hammer
* Slow POST DoS Testing Tool
* entropy [at] phiral.net
* Anon-ymized via Tor
* We are Legion.
*/
```

Torshammer (con't)

./torshammer.py -t <target> [-r <threads> -p <port> -T -h]

-t|--target <Hostname|IP>

-r|--threads <Number of threads> Defaults to 256

-p|--port <Web Server Port> Defaults to 80

-T|--tor Enable anonymising through tor on 127.0.0.1:9050

-h|--help Shows this help

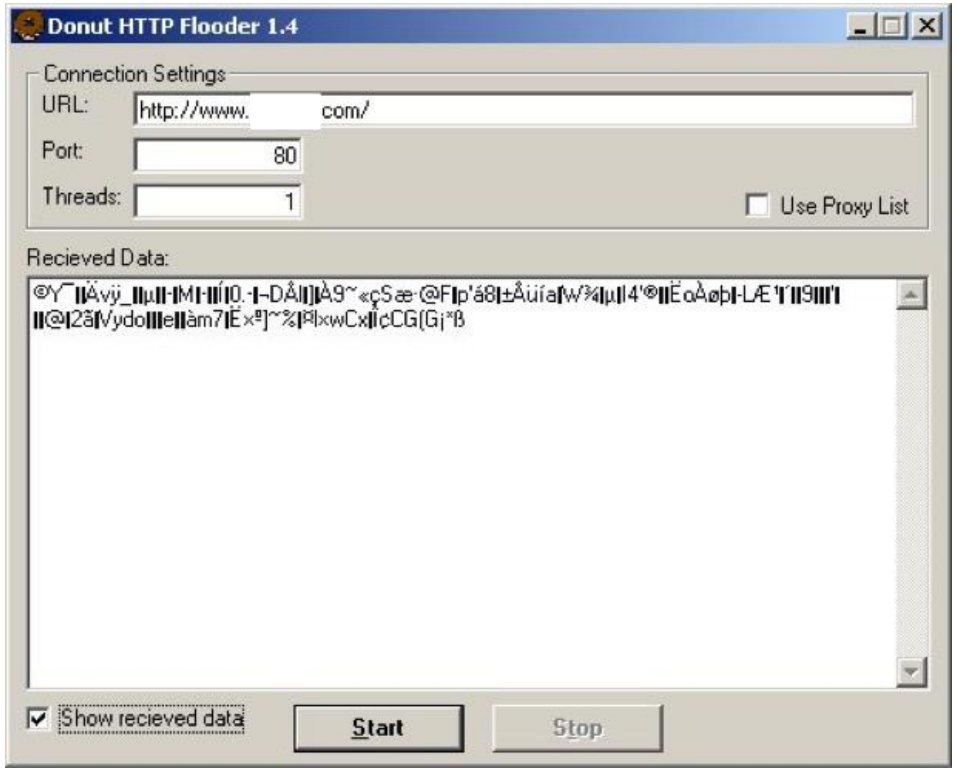
Eg. ./torshammer.py -t 192.168.1.100 -r 256

Tools: Torshammer (con't)

Tor's Hammer is a slow post dos testing tool written in Python. It can also be run through the Tor network to be anonymized.

If you are going to run it with Tor it assumes you are running Tor on 127.0.0.1:9050. Kills most unprotected web servers running Apache and IIS via a single instance.

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

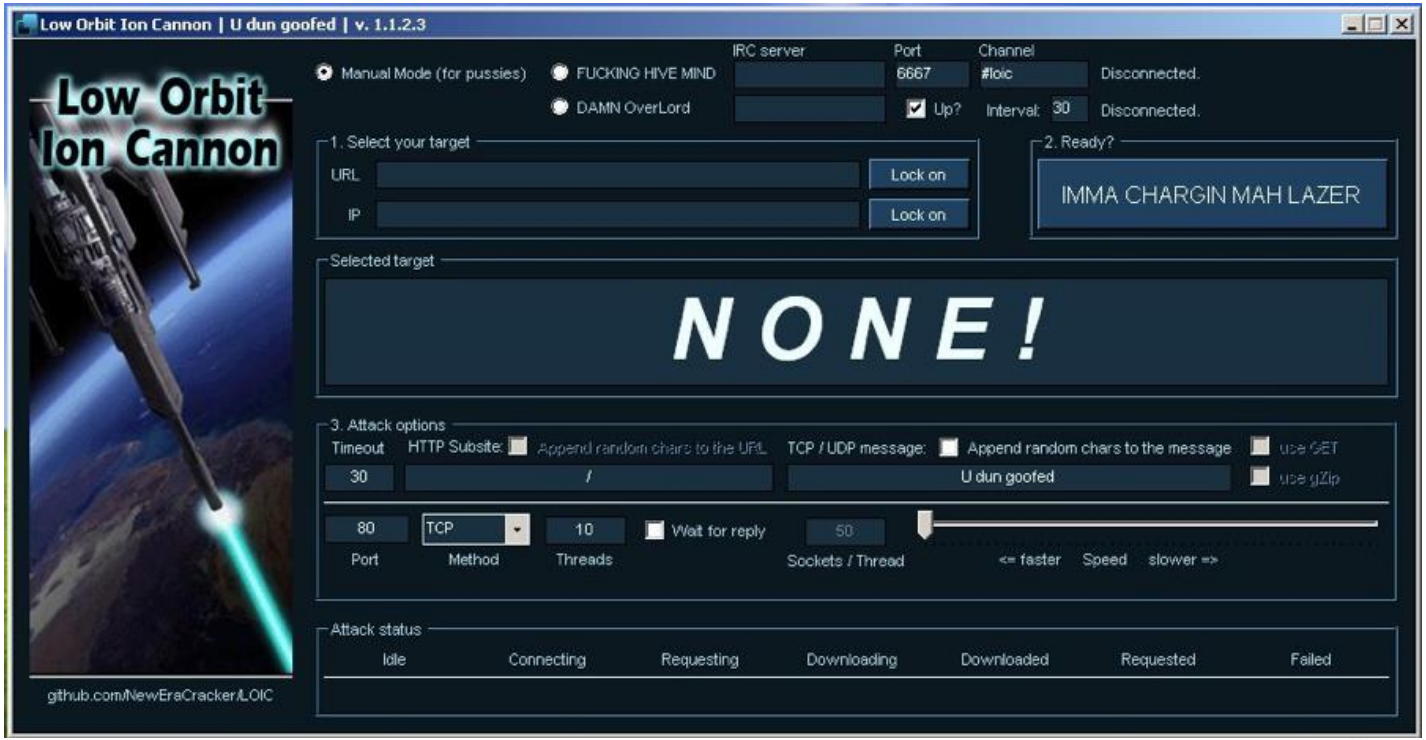
Accept-Encoding: gzip, deflate

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

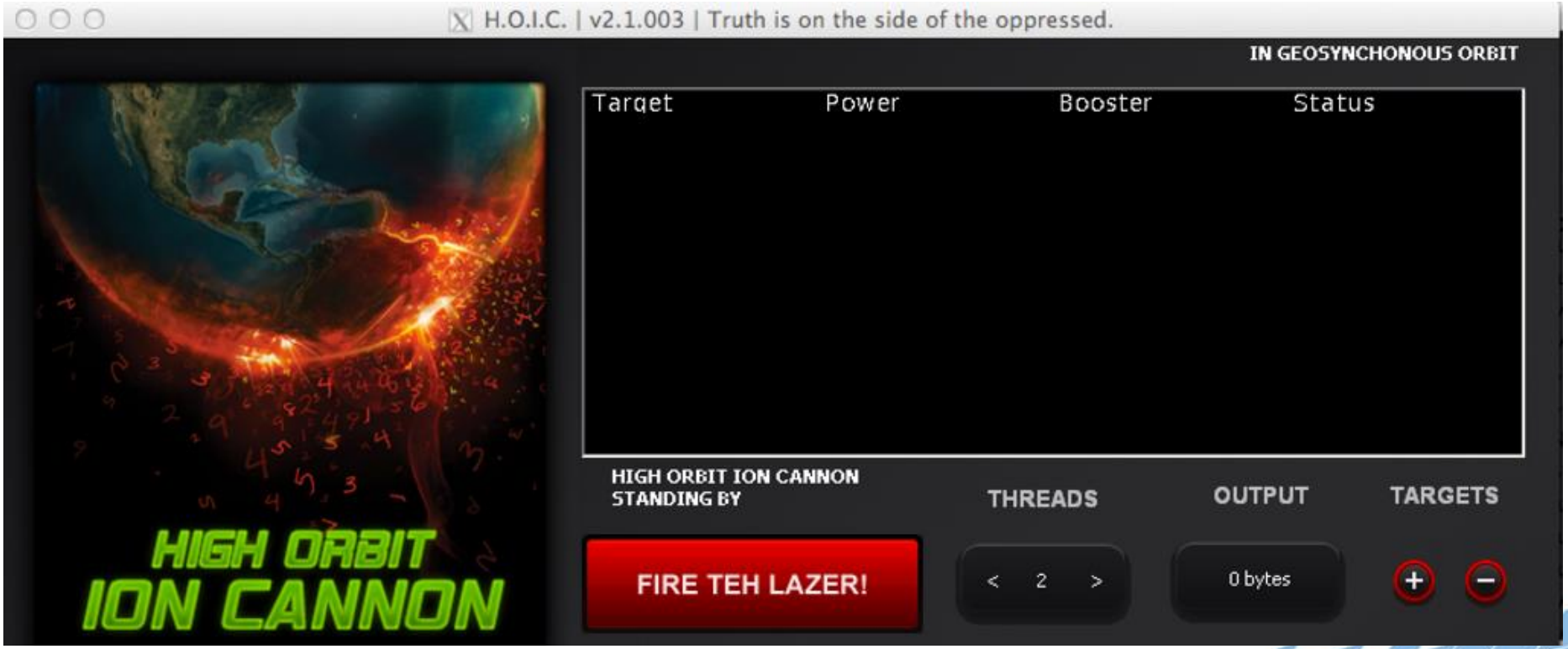
Host: www.foo.bar

Connection: Close

Tools: 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

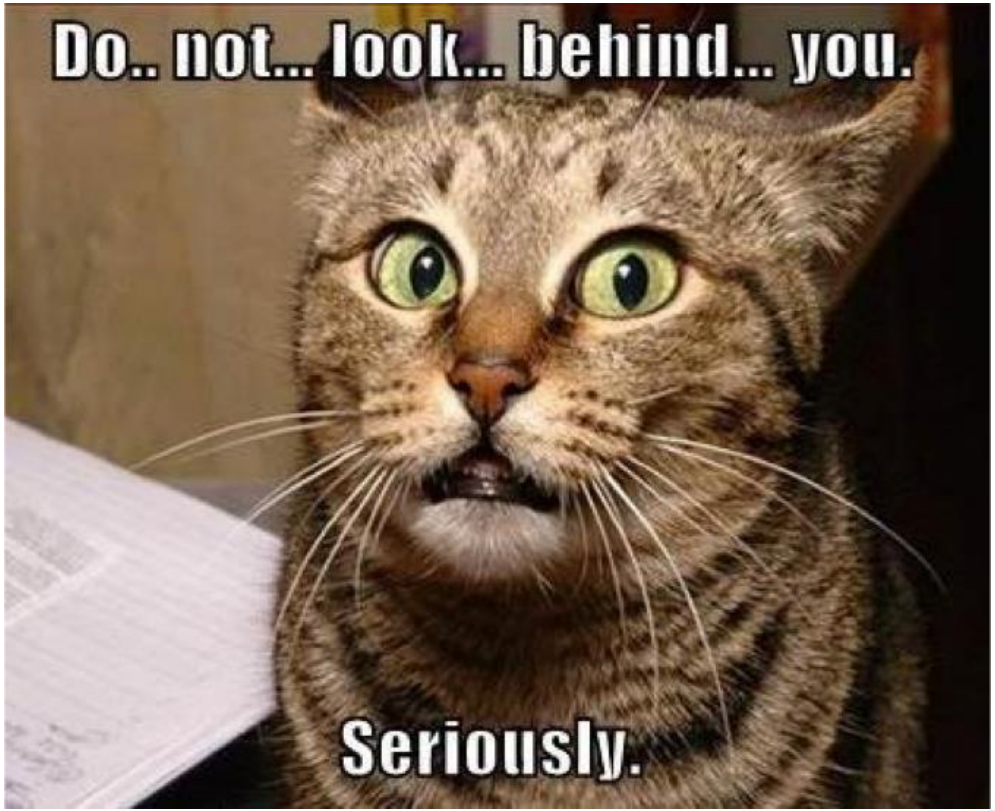
Tools: HOIC


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: WGET



Trends

Media Grandstanders

Commoditization of DDoS

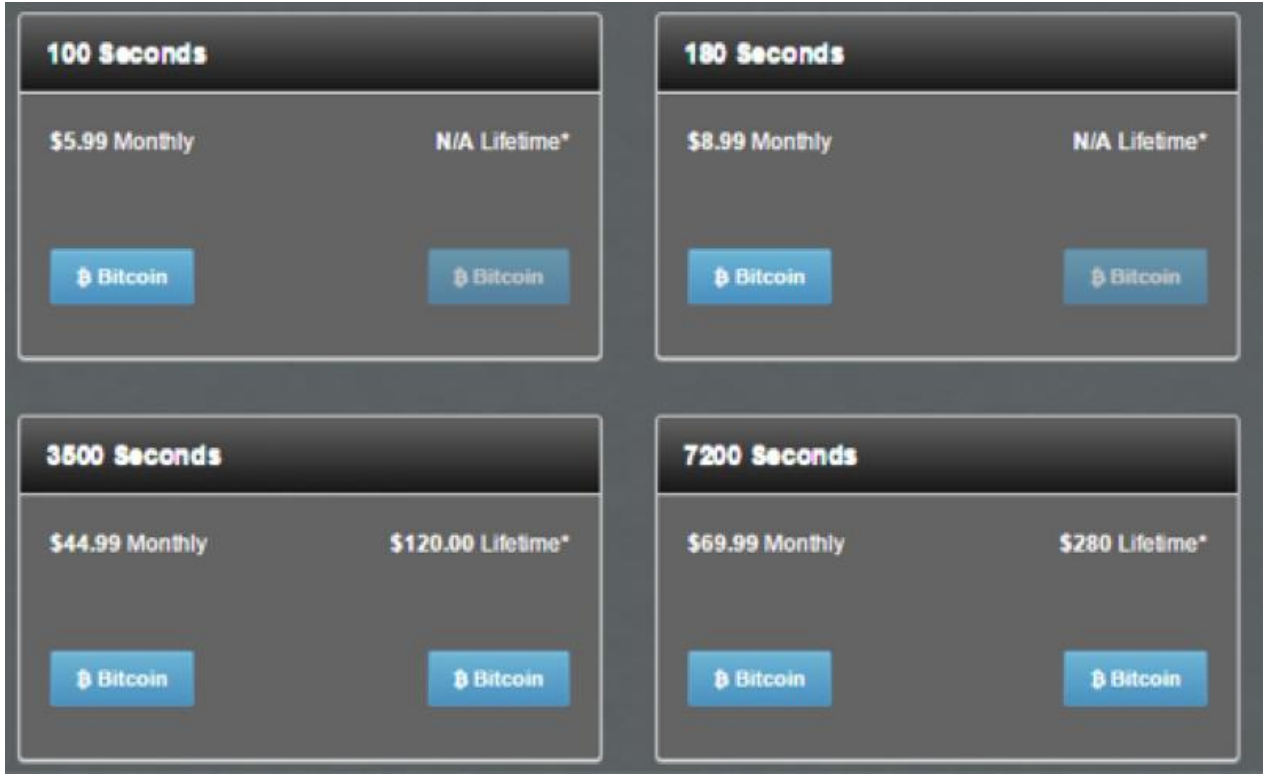
Lizard Squad launches DDoS tool that lets anyone take down online services, starting at $6 per month

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?

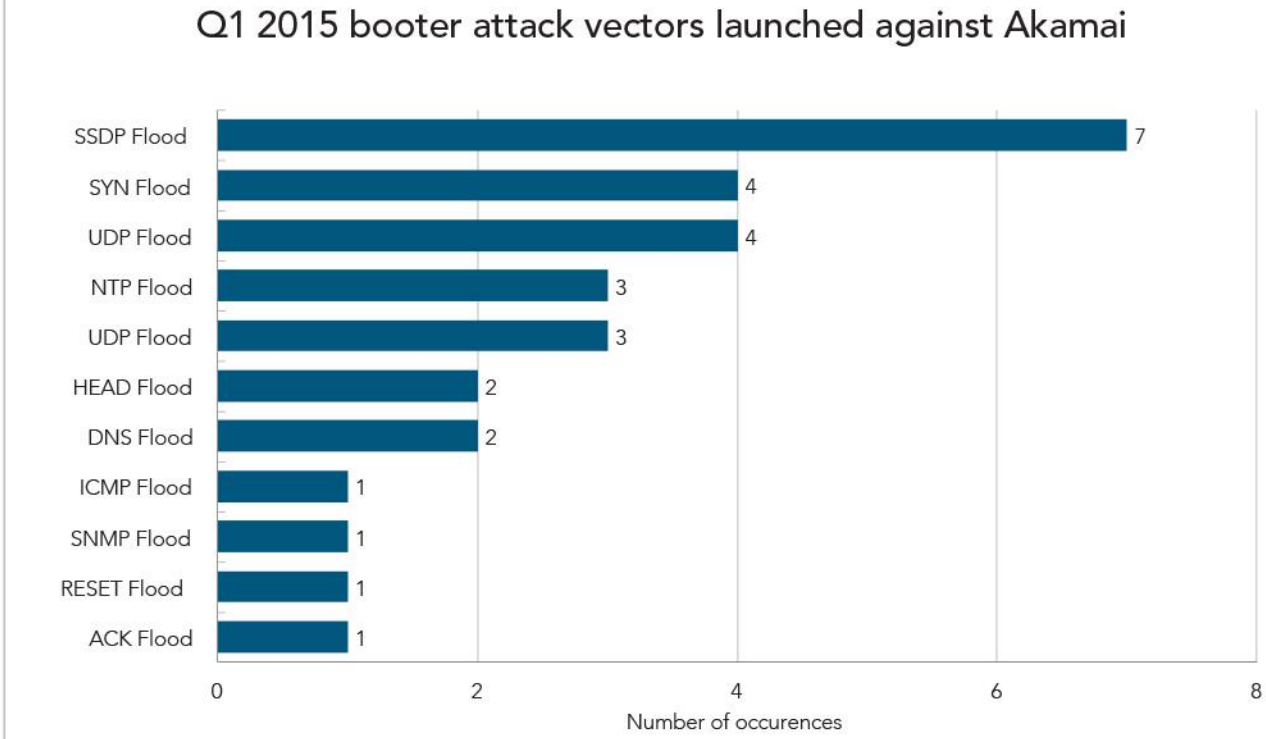
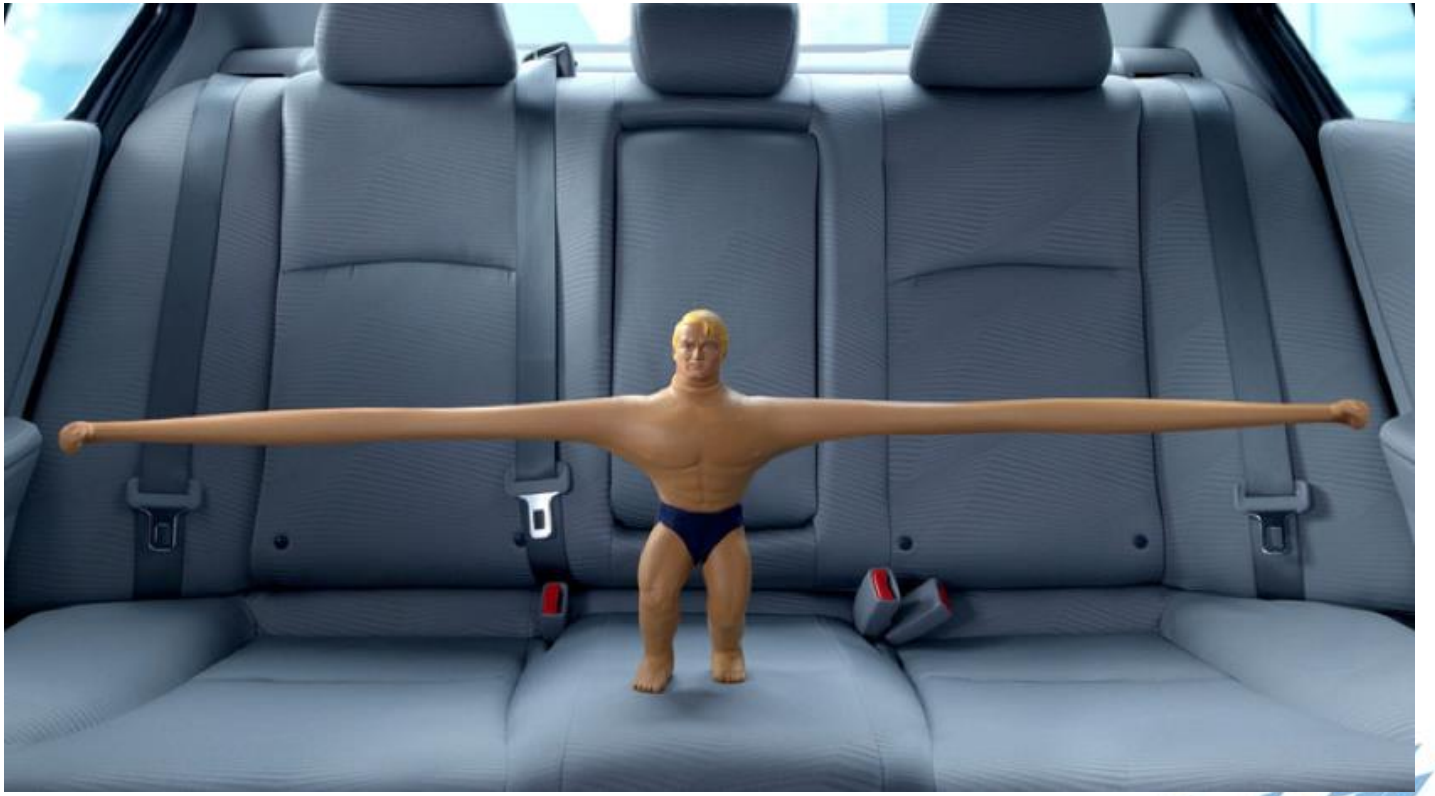


Figure 2-1: Attack occurrence by vector against the Akamai property during Q1 2015

OK, What's a Stresser?



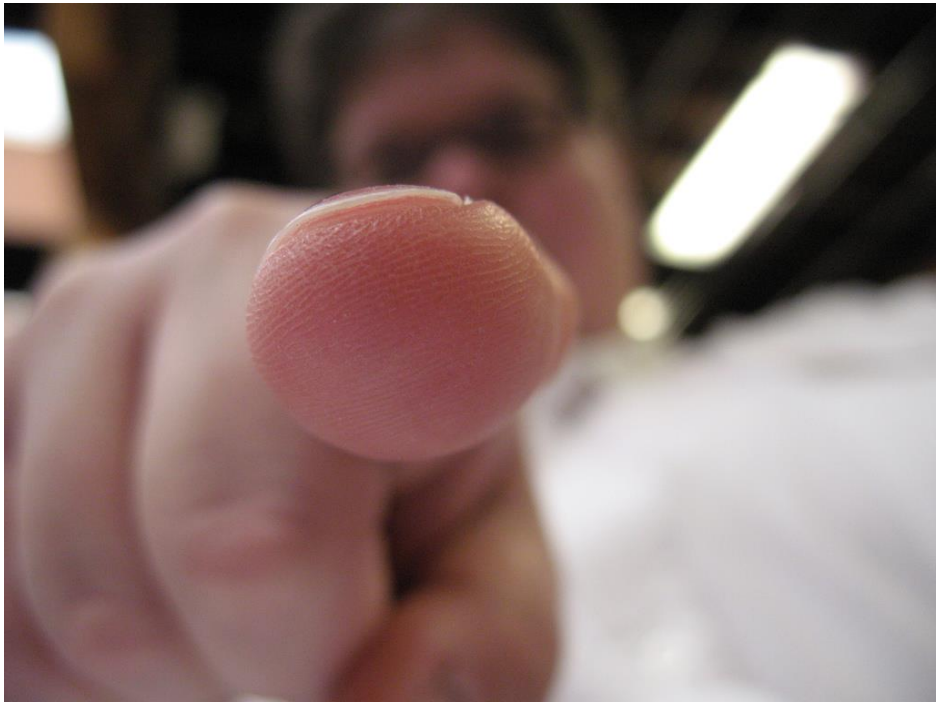
Stressers & Booters

- 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

Attributions



Top 10 source countries for web application attacks, Q1 2015

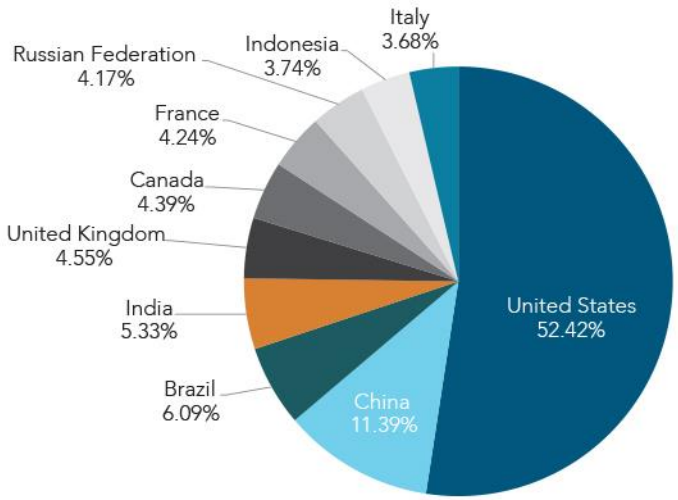
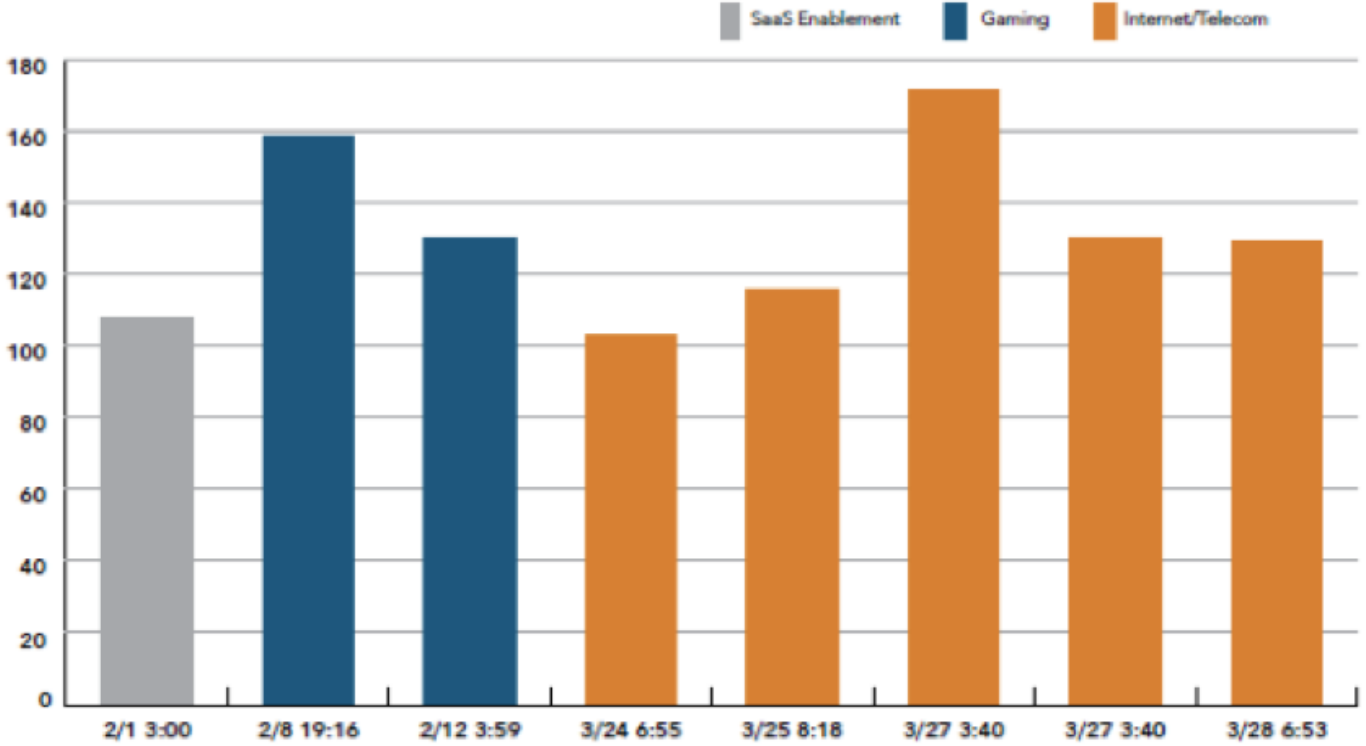


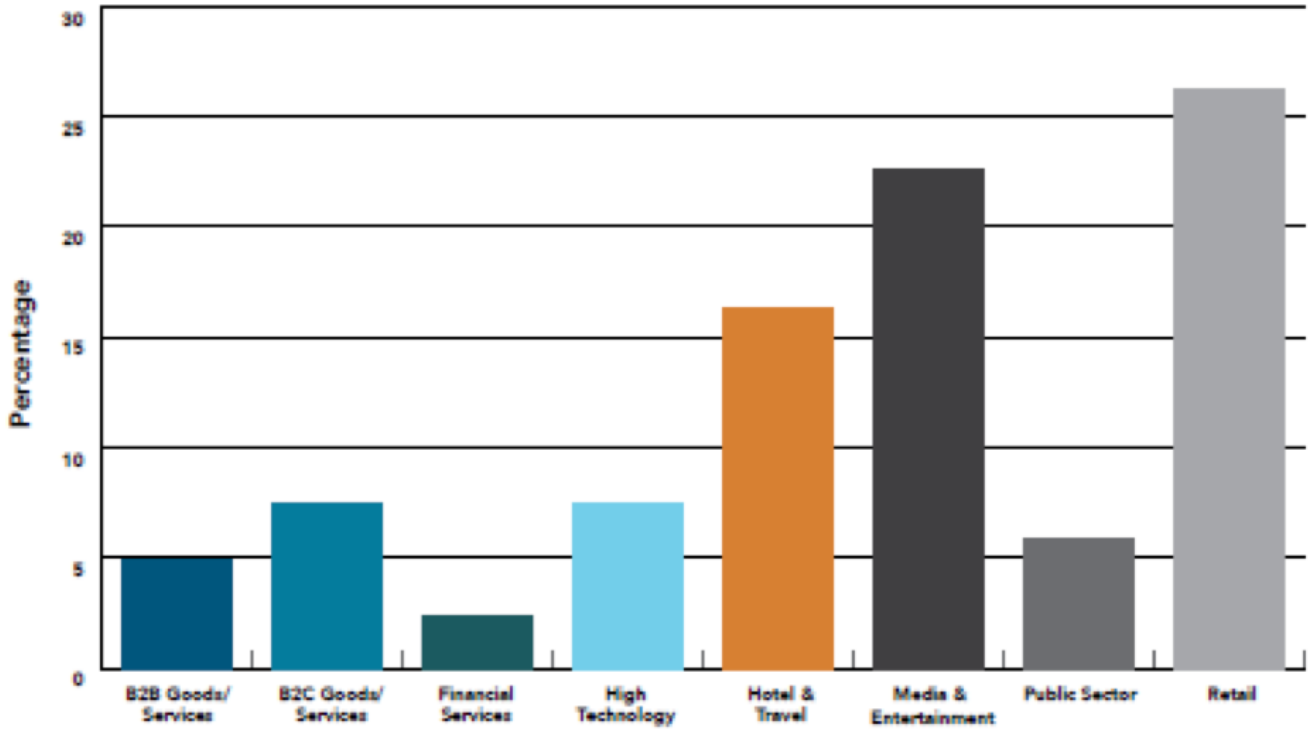
Figure 1-14: The US and BRIC (Brazil, Russia, India, China) countries were responsible for nearly 80 percent of web application attacks analyzed in Q1 2015

Q1 2015 DDoS Attacks > 100 Gbps



Application Security

Web application attacks by vertical, Q1 2015



Top 10 target countries for web application attacks, Q1 2015

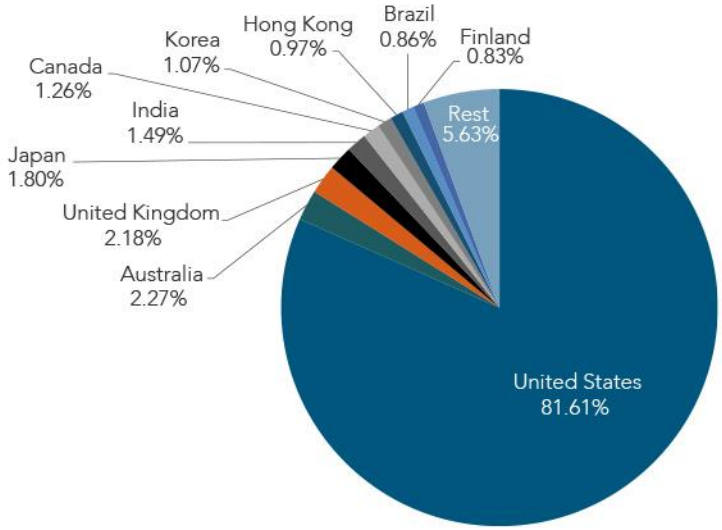


Figure 1-15: The US was targeted with web application attacks in 81 percent of the analyzed attacks

Syn Floods

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>.....

By The Numbers

Compared to Q4 2014

- 35.24 percent increase in total DDoS attacks
- 22.22 percent increase in application layer (Layer 7) DDoS attacks
- 36.74 percent increase in infrastructure layer (Layer 3 & 4) DDoS attacks
- 15.37 percent decrease in average attack duration: 24.82 vs. 29.33 hours
- China was the top source of attacking IPs

Compared to Q1 2014

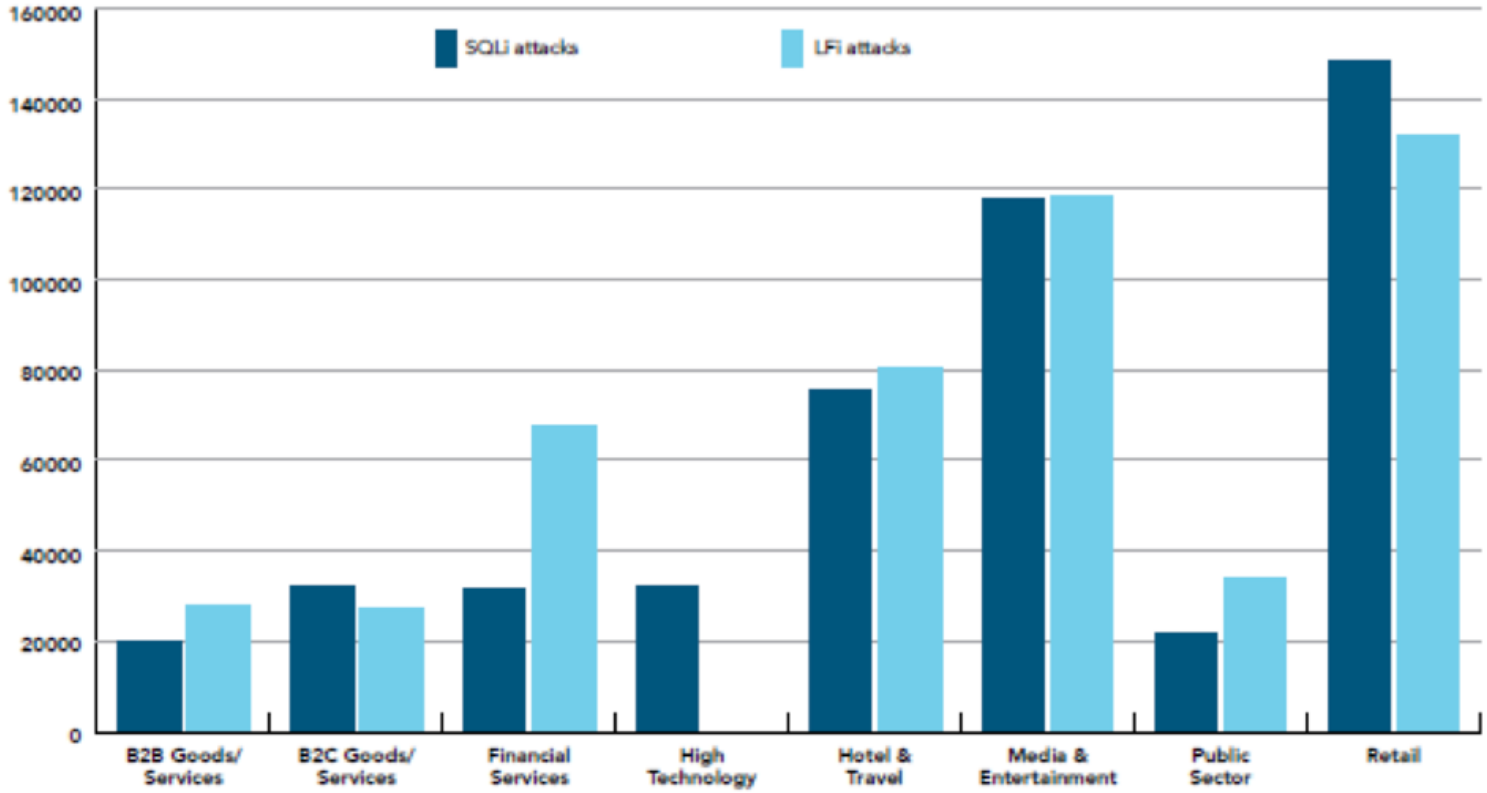
- 116.5 percent increase in total DDoS attacks
- 59.83 percent increase in application layer (Layer 7) DDoS attacks
- 124.69 percent increase in infrastructure layer (Layer 3 & 4) DDoS attacks
- 42.8 percent increase in the average attack duration: 24.82 vs. 17.38 hours

Other Observations

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

SQL Injection…still

Normalized SQLi and LFI attacks by industry, Q1 2015



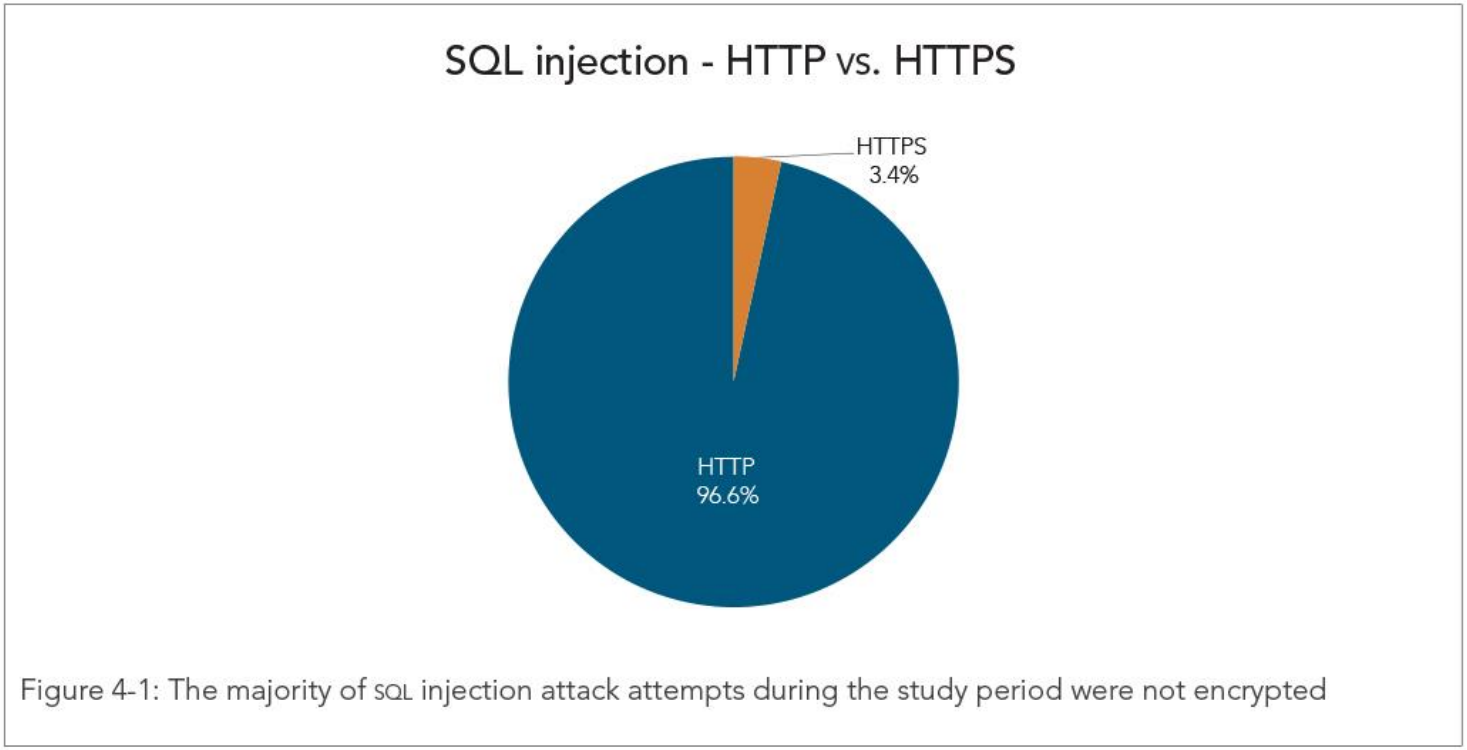


Figure 4-1: The majority of SQL injection attack attempts during the study period were not encrypted

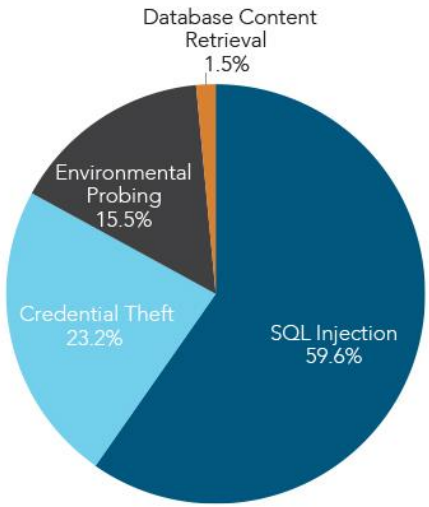
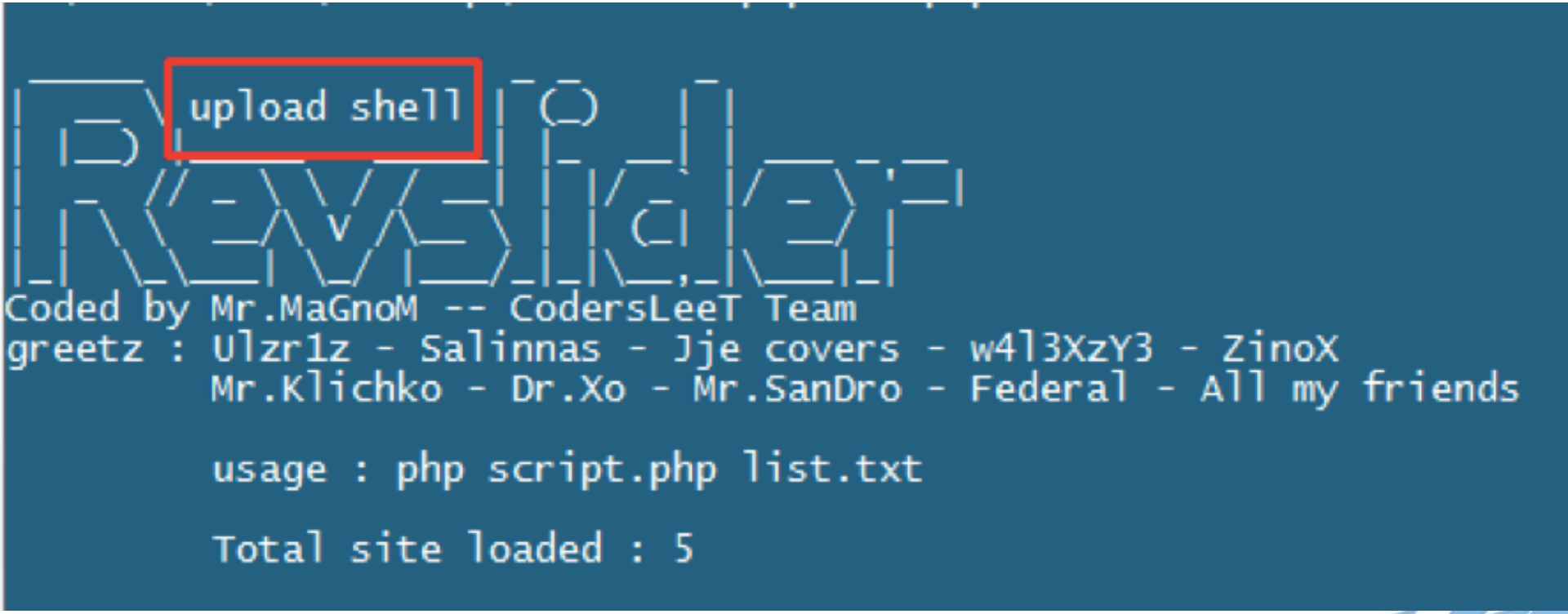


Figure 4-2: SQL injection probing, credential theft and environment probing were the most common attack types during the study period (rounded to the nearest percent). Content Injection, Data Corruption, File Exfiltration, Login Bypass and Remote Command Execution combined account for only 0.2 percent of SQL injection attacks during the research period.

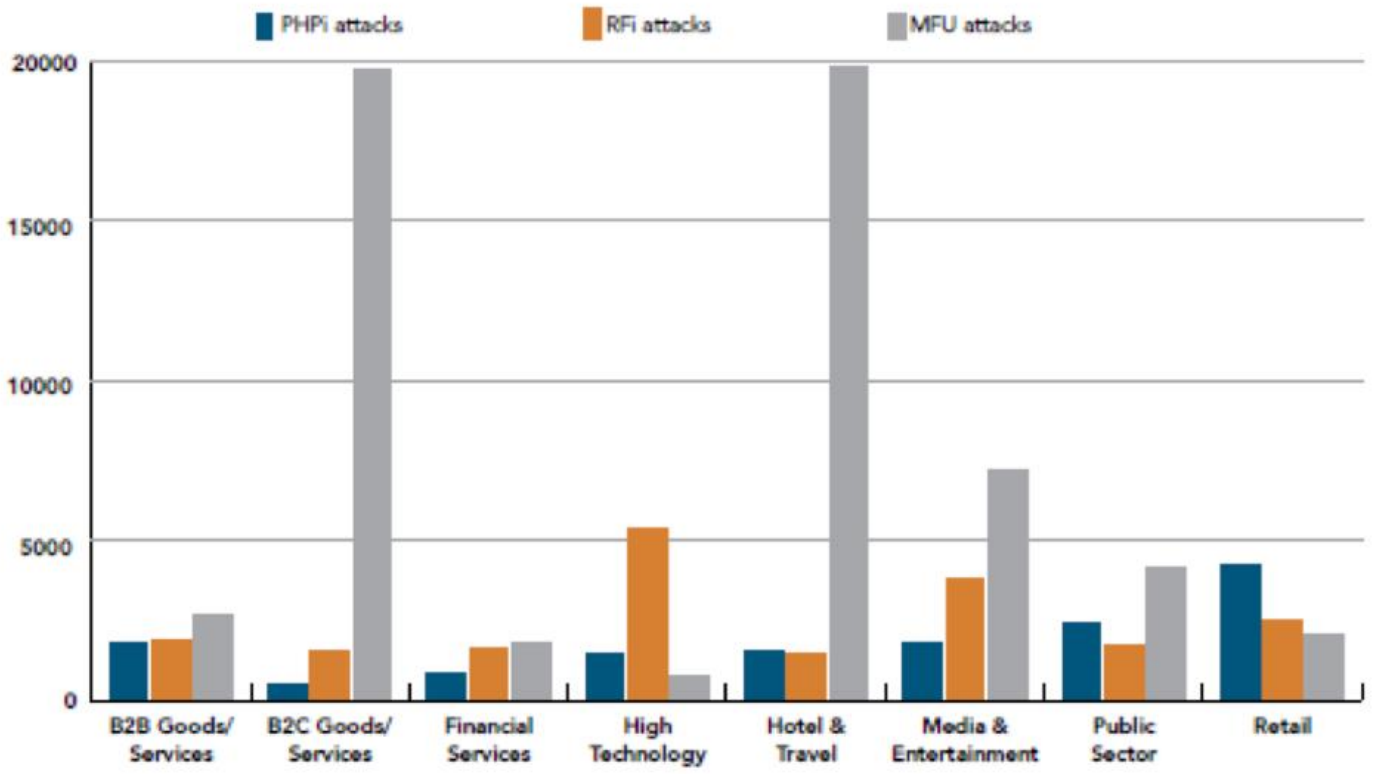
File Inclusions



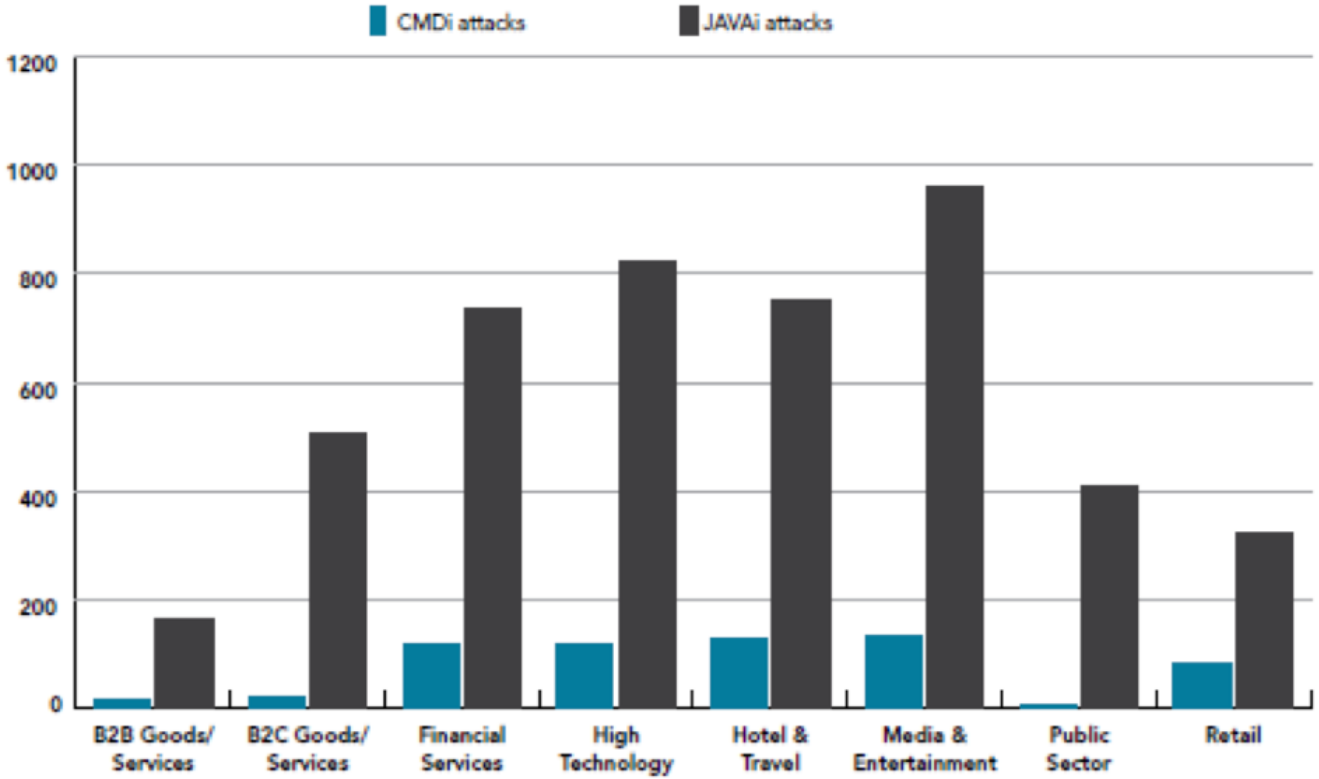
Malicious Uploads

- 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)

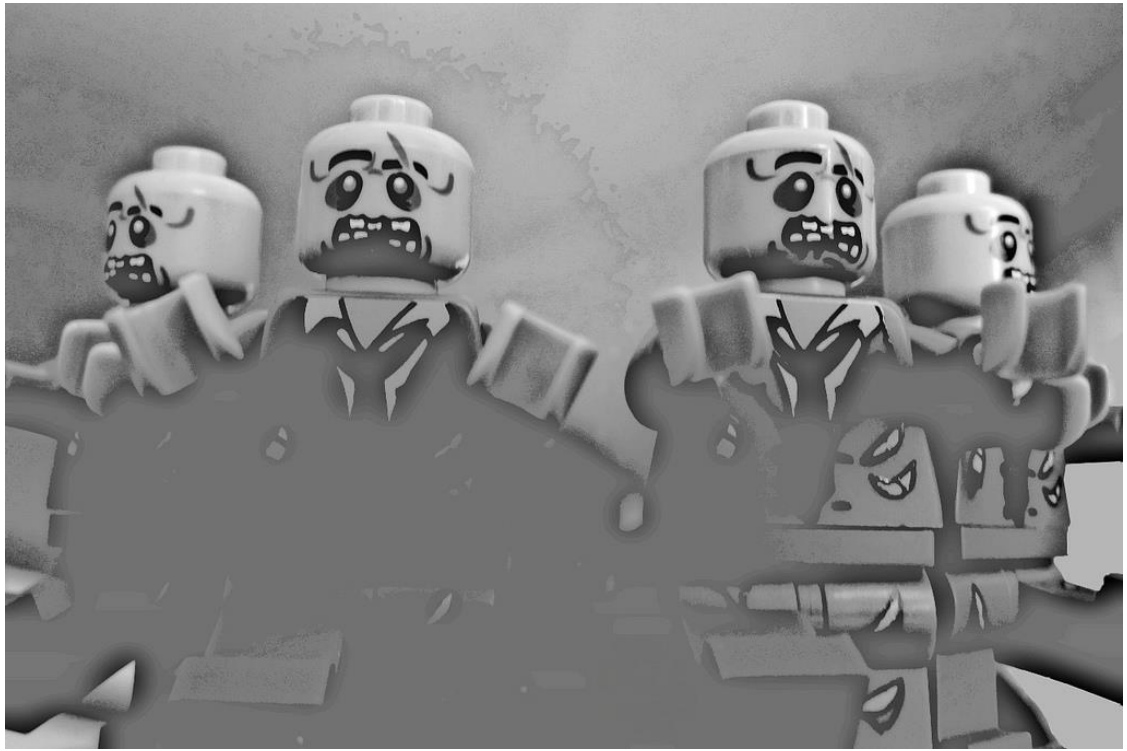
Normalized MFU, RFI and PHPi attack data by vertical



Normalized JAVAi and CMDI attacks by industry, Q1 2015



Zombie Bot Army



What Can You Do?

- Deploy cloud based web application firewalls
- Use a DDoS mitigation service. Appliances don't scale.
- SQL INJECTION IS A SOLVABLE PROBLEM
- Harden your systems
- Work with your ISP on mitigation strategies
- Use ACL lists to deal with known bad IPs
- IP Rate limiting / IP Reputation
- PATCH PATCH PATCH

Questions?

Thank You

Dave Lewis

Global Security Advocate

Akamai Technologies

Twitter: @gattaca

Email: dave@akamai.com