Barbarians At The Gate(way)

Examination of actors, tools and defenses
#whoami

Dave Lewis
@gattaca
dave@akamai.com
MYSTERY SOLVED!

WE FOUND HIM!
OLD MAN YELLS AT CLOUD

Older Abraham Jones
and his
friends
It left me wanting...
Game Plan

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

Browse OR Start a Project for Free
Actors: Bored Kids

Can I has milk?
AND

BORED TEENS
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

Web Application Attack Vectors Over HTTP, Q1 2016

- SQLi: 34.85%
- LFI: 7.84%
- XSS: 5.85%
- Shellshock: 1.60%
- PHPi: 1.36%
- RFI: 1.43%
- Other: 47.06%
Attack Vectors Over HTTPS

Web Application Attack Vectors Over HTTPS, Q1 2016

- SQLi: 38.11%
- LFI: 30.85%
- XSS: 20.24%
- Shellshock: 7.15%
- PHPi: 1.65%
- RFI: 1.14%
- Other: 0.86%

SANS
Web Application Attack Frequency, Q3 2016

- SQLi: 48.83%
- LFI: 39.97%
- XSS: 6.18%
- RFI: 2.11%
- PHPi: 2%
- MFU: 0.54%
- Other: 1.29%
Types of Attacks

- SYN Floods
- UDP Floods
- ICMP Floods
- NTP Amplification
- HTTP Flood
Attacks: Volumetric
Your website can be overwhelmed…
DDoS Attack Vector Frequency, Q1 2016

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>3.63%</td>
</tr>
<tr>
<td>CHARGEN</td>
<td>11.34%</td>
</tr>
<tr>
<td>DNS</td>
<td>18.26%</td>
</tr>
<tr>
<td>NTP</td>
<td>11.70%</td>
</tr>
<tr>
<td>SSDP</td>
<td>6.70%</td>
</tr>
<tr>
<td>SYN</td>
<td>6.66%</td>
</tr>
<tr>
<td>TCP Anomaly</td>
<td>2.10%</td>
</tr>
<tr>
<td>UDP Floods</td>
<td>6.32%</td>
</tr>
<tr>
<td>UDP Fragment</td>
<td>27.35%</td>
</tr>
<tr>
<td>Other</td>
<td>3.38%</td>
</tr>
</tbody>
</table>

Other: FIN (0.64%), FIN PUSH (0.02%), ICMP (0.60%), NetBIOS (0.13%), RESET (0.69%), RIP (0.24%), RP (0.04%), SNPMP (0.71%), SYN PUSH (0.02%), TCP Fragment (0.04%), TFTP (0.07%)
Average Number of DDoS Attacks Per Target

Top target organization attack count Q3 2016

427
Attacks: Application Layer
### Application Layer DDoS

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEAD</td>
<td>0.06%</td>
</tr>
<tr>
<td>HTTP GET</td>
<td>1.90%</td>
</tr>
<tr>
<td>HTTP POST</td>
<td>0.29%</td>
</tr>
<tr>
<td>PUSH</td>
<td>0.31%</td>
</tr>
</tbody>
</table>

- **Application Layer DDoS**: 2.56%
- **Infrastructure Layer DDoS**: 97.44%
US IS THE TOP APPLICATION ATTACK SOURCE

20%
US IS THE TOP APPLICATION ATTACK TARGET

66%
Top 10 Target Countries for Web Application Attacks, Q3 2016

- US: 66%
- Brazil: 5%
- Germany: 5%
- UK: 3%
- Australia: 3%
- Japan: 3%
- India: 3%
- Malaysia: 3%
- France: 1%
- China: 1%
- Other: 7%
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@xxxxxx]
Sent: June-25-15 11:48 AM
To: XXXXX
Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:


http://xxxxxxxxxx.com/bitalo.html


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
'Key member' of DD4BC arrested in international crackdown

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.

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 increasing the level of damage in this form of extortion. How to stop?
Attacks: Amplification
DDOS REFLECTOR SOURCE PERCENTAGE BY IP COUNT - Q3 2016

- ntp: 60%
- sstdp: 18%
- chargen: 6%
- RPC: 5%
- sentinel: 5%
- qotd: 4%
- Ntp: 3%
- Others: 5%
Tools
Tools: Havij

Havij - Advanced SQL Injection Tool

Version 1.15 Free
Copyright © 2005-2011 By 3dm0x3

http://CTSaeTeam.com
http://forums.3dm0x3.com
info@3dm0x3.com  Check for update

Databases:
MySQL with error
MySQL no error
MySQL Blind (Pro Version)
MySQL Memcached (Pro Version)
MySQL InnoDB (Pro Version)
MySQL Access
MySQL Access Blind (Pro Version)

Status: In IDE

[Error Log]

Getting 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 correct?
Are you sure the 'GET' method is correct?
Tools: Donut
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
Tools: HOIC
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

```java
var loggedIn bool
var userInfo AccountInfo

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

this.conn.Write([]byte("\r\n\033[0m"))
this.conn.Write([]byte("[+] DDOS | Successfully hijacked connection\n\n"))
time.Sleep(250 * time.Millisecond)
this.conn.Write([]byte("[+] DDOS | Masking connection from utmp+wtmp...\n\n"))
time.Sleep(500 * time.Millisecond)
this.conn.Write([]byte("[+] DDOS | Hiding from netstat...\n\n"))
time.Sleep(150 * time.Millisecond)
this.conn.Write([]byte("[+] DDOS | Removing all traces of LD_PRELOAD...\n\n"))
```
// Set up passwords

add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x58\x4D\x4D\x56", "\x54\x48\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\x41", 5); // root xmhdipc
add_auth_entry("\x58\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x56", 5); // root default
add_auth_entry("\x58\x4D\x4D\x56", "\x4B\x57\x43\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\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
On November 21, 2016, Oracle announced that it has signed an agreement to acquire Dyn, the leading cloud-based Internet Performance and DNS provider that monitors, controls, and optimizes Internet applications and cloud services to deliver faster access, reduced page load times, and higher end-user satisfaction. The proposed transaction is subject to customary closing conditions. Until the transaction closes, each company will continue to operate independently.
Tools: WGET

Do.. not... look... behind... you.

Seriously.
Trends
Media Grandstanding

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

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
  - Bitcoin

- **180 Seconds**
  - $8.99 Monthly
  - N/A Lifetime
  - Bitcoin

- **3600 Seconds**
  - $44.99 Monthly
  - $120.00 Lifetime
  - Bitcoin

- **7200 Seconds**
  - $69.99 Monthly
  - $280 Lifetime
  - Bitcoin
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?
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.

<table>
<thead>
<tr>
<th>Website</th>
<th>Number of Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Myspace</td>
<td>359,420,698</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>164,611,595</td>
</tr>
<tr>
<td>Adobe</td>
<td>152,445,165</td>
</tr>
<tr>
<td>tumblr</td>
<td>65,469,298</td>
</tr>
<tr>
<td>Fling</td>
<td>40,767,652</td>
</tr>
<tr>
<td>Mate1</td>
<td>27,393,015</td>
</tr>
<tr>
<td>000webhost</td>
<td>13,545,468</td>
</tr>
<tr>
<td>R2Games</td>
<td>13,186,088</td>
</tr>
<tr>
<td>Gamigo</td>
<td>8,243,604</td>
</tr>
<tr>
<td>Heroes</td>
<td>8,089,103</td>
</tr>
<tr>
<td>Lifeboat</td>
<td>7,089,395</td>
</tr>
<tr>
<td>Nexus Mods</td>
<td>5,915,013</td>
</tr>
<tr>
<td>Acne.org</td>
<td>432,943</td>
</tr>
<tr>
<td>Xbox-Scene</td>
<td>432,552</td>
</tr>
<tr>
<td>Avast</td>
<td>422,959</td>
</tr>
<tr>
<td>PSX-Scene</td>
<td>341,118</td>
</tr>
<tr>
<td>Plex</td>
<td>327,314</td>
</tr>
<tr>
<td>Sumo Torrent</td>
<td>285,191</td>
</tr>
<tr>
<td>Seedpeer</td>
<td>281,924</td>
</tr>
<tr>
<td>MajorGeeks</td>
<td>269,548</td>
</tr>
<tr>
<td>myRepoSpace</td>
<td>252,751</td>
</tr>
<tr>
<td>Foxy Bingo</td>
<td>252,216</td>
</tr>
<tr>
<td>COMELEC (Philippines Voters)</td>
<td>228,605</td>
</tr>
<tr>
<td>Cannabis.com</td>
<td>227,746</td>
</tr>
</tbody>
</table>
Why this is a problem.
Passwords

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
File Inclusions

upload shell

Coded by Mr.MaGnO M -- 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

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
AND WITH THAT...

AKAMAI IS HIRING!

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.

See video
Thanks for listening!
Questions?

Dave Lewis
@gattaca
dave@akamai.com