Barbarians At The Gate(way)
Examination of actors, tools and defenses
MYSTERY SOLVED!
WE FOUND HIM!
OLD MAN YELLS AT CLOUD
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.

Browse OR Start a Project for Free
Actors: Bored Kids

Can I has milk?
AND

BORED TEENS
HACKTIVISTS

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: 47.06%
- XSS: 7.84%
- Shellshock: 5.85%
- PHPi: 1.60%
- RFI: 1.36%
- Other: 1.43%
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%
Types of Attacks

- SYN Floods
- UDP Floods
- ICMP Floods
- NTP Amplification
- HTTP Flood
Attacks: Volumetric
Your website can be overwhelmed...
Multi-Vector DDoS Attacks, Q2 2015 – Q1 2016

- **Q2 2015**
  - Single Vector: 26%
  - Two Vectors: 56%
  - Three Vectors: 4%
  - Four Vectors: 4%
  - Five to Eight Vectors: 2%

- **Q3 2015**
  - Single Vector: 32%
  - Two Vectors: 51%
  - Three Vectors: 4%
  - Four Vectors: 3%
  - Five to Eight Vectors: 5%

- **Q4 2015**
  - Single Vector: 35%
  - Two Vectors: 45%
  - Three Vectors: 3%
  - Four Vectors: 3%
  - Five to Eight Vectors: 3%

- **Q1 2016**
  - Single Vector: 42%
  - Two Vectors: 41%
  - Three Vectors: 12%
  - Four Vectors: 3%
  - Five to Eight Vectors: 2%
DDoS Attack Vector Frequency, Q1 2016

- **ACK**: 3.63%
- **CHARGEN**: 11.34%
- **DNS**: 18.26%
- **NTP**: 11.70%
- **SSDP**: 6.70%
- **SYN**: 6.66%
- **TCP Anomaly**: 2.10%
- **UDP Floods**: 6.32%
- **UDP Fragment**: 27.35%
- **Other**: 3.38%

Additional vectors:
- **FIN** (0.64%)
- **FIN PUSH** (0.02%)
- **ICMP** (0.60%)
- **NetBIOS** (0.13%)
- **RESET** (0.69%)
- **RIP** (0.24%)
- **RPC** (0.18%)
- **SNMP** (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: 283

Average Number by Quarter:
- Q2 2015: 14
- Q3 2015: 17
- Q4 2015: 24
- Q1 2016: 29
Attacks: Application Layer
## Application Layer DDoS

<table>
<thead>
<tr>
<th>Application Layer DDoS</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%
Top 10 Source Countries for Web Application Attacks, Q1 2016

- US: 43%
- Brazil: 12%
- Netherlands: 8%
- China: 8%
- Romania: 7%
- Russia: 6%
- UK: 6%
- Germany: 4%
- Ukraine: 3%
- India: 3%

THE US IS THE TOP APPLICATION ATTACK SOURCE
Top 10 Target Countries for Web Application Attacks, Q1 2016

- US: 60%
- Brazil: 9%
- UK: 6%
- India: 5%
- Canada: 4%
- Netherlands: 3%
- Australia: 3%
- China: 2%
- Japan: 1%
- Singapore: 1%
- Other: 7%
Web Application Attacks by Industry, Q1 2016

- Retail: 43.42%
- Hotel & Travel: 12.99%
- Financial Services: 12.11%
- High Technology: 9.43%
- Media & Entertainment: 7.22%
- Public Sector: 3.25%
- Software as a Service: 3.09%
- Business Services: 2.38%
- Other: 6.10%
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@xxxxxxxx]

Sent: June-25-15 11:48 AM

To: XXXXX

Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:


http://xxxxxxxxxxxx.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 rascal 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 innovating on the hardwars and this form of extortion by extorting...
Attacks: Amplification
Reflection-Based DDoS Attacks, Q1 2015–Q1 2016
Tools
Tools: Havij
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

<table>
<thead>
<tr>
<th>Target</th>
<th>Power</th>
<th>Booster</th>
<th>Status</th>
</tr>
</thead>
</table>

**HIGH ORBIT ION CANNON**

- HIGH ORBIT ION CANNON
- STANDING BY

**FIRE TEH LAZER!**

<table>
<thead>
<tr>
<th>Threads</th>
<th>Output</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 2 &gt;</td>
<td>0 bytes</td>
<td>+ -</td>
</tr>
</tbody>
</table>
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

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

Seriously.
Trends

TO THE WORLD'S GREATEST MOM,
FROM YOUR LOVING BOY.
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?
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?
<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>27.24%</td>
</tr>
<tr>
<td>US</td>
<td>17.12%</td>
</tr>
<tr>
<td>Turkey</td>
<td>10.24%</td>
</tr>
<tr>
<td>Brazil</td>
<td>8.60%</td>
</tr>
<tr>
<td>South Korea</td>
<td>7.47%</td>
</tr>
<tr>
<td>India</td>
<td>6.67%</td>
</tr>
<tr>
<td>Spain</td>
<td>6.32%</td>
</tr>
<tr>
<td>Thailand</td>
<td>5.65%</td>
</tr>
<tr>
<td>Japan</td>
<td>5.55%</td>
</tr>
<tr>
<td>Russia</td>
<td>5.14%</td>
</tr>
</tbody>
</table>
Q4 2015 DDoS Attacks > 100 Gbps

- Gaming
- Software & Technology

<table>
<thead>
<tr>
<th>Date</th>
<th>Gaming</th>
<th>Software &amp; Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. 8</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>Dec. 9</td>
<td>203</td>
<td></td>
</tr>
<tr>
<td>Dec. 23</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>Dec. 24</td>
<td>135</td>
<td></td>
</tr>
<tr>
<td>Dec. 30</td>
<td>309</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

```plaintext
upload shell

Coded by Mr.MagnoM -- CodersLeeT Team
greetz: Ulzr1z - Salinnas - Jje covers - w413x3y3 - 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

/*.HACKMIAMI 0x7E0 */
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
THANKS FOR LISTENING

고맙습니다  QUESTIONS?
Questions?
Thanks

Dave Lewis
@gattaca
dave@akamai.com