Barbarians At The Gate(way)
Examination of actors, tools and defenses
#whoami

Dave Lewis
@gattaca
dave@akamai.com
OLD MAN YELLS AT CLOUD

Old man Abraham Silver, he's yelling at the cloud.

[Article text in a foreign language, possibly Hebrew or Yiddish, not legible]
It left me wanting...
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don’t waste your time. Nobody can recover your files without paying a decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78nGsdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail

   wowsmith123456@posteo.net. Your personal installation key:

   PqvrHJ-BCvRyd-iQu7E5-rJbEJZ-fBXAKX-tP3tWS-1t2FAd-M7T8jE-3Ggax-x-A6BchH

   If you already purchased your key, please enter it below:
### Address

<table>
<thead>
<tr>
<th>Address</th>
<th>3.63676946 BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1Mz753HMuxXTuR2R1t78mGSdzaAtNbBWX</td>
<td></td>
</tr>
</tbody>
</table>

### Summary

- **Total Received**: 3.63676946 BTC
- **Total Sent**: 0 BTC
- **Final Balance**: 3.63676946 BTC
- **No. Transactions**: 36

---

**$11,286**
What are the Panama Papers? A guide to history's biggest data leak

What is Mossack Fonseca, how big is it, and who uses offshore firms? Key questions about one of the biggest ever data leaks

- Kubrick to Cowell: Panama Papers expose offshore dealings of the stars
- How the world's rich and famous hide their money offshore
- All the Panama Papers revelations so far
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
THE HACKTIVISTS
THERE ARE STANDARD VILLAINS
AND THERE ARE
ARCH VILLAINS
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.
Web Application Attack Frequency, Q2 2017

- SQLi 51%
- LFI 33%
- XSS 9%
- RFI 2%
- PHPi 2%
- Other 2%
Types of Attacks

- SYN Floods
- UDP Floods
- ICMP Floods
- NTP Amplification
- HTTP Flood
Attacks: Volumetric
Your website can be overwhelmed...
10 Most Frequent Attack Vectors by Week

- ACK
- NTP
- SSDP
- UDP Fragment
- CharGen
- RIP
- SYN
- Other
- DNS
- SNMP
- UDP

Count

Average Number of DDoS Attacks Per Target

Top target organization DDoS attack count Q2 2017

558
Top 10 Target Countries for Web Application Attacks, Q2 2017

- USA: 200M
- United Kingdom: ~50M
- Brazil: ~30M
- Japan: ~20M
- Singapore: ~10M
- Sweden: ~10M
- Germany: ~10M
- India: ~10M
- China: ~10M
- Netherlands: ~10M

Number of Attacks
Hotel & Travel 7%
High Technology 8%
Media & Entertainment 9%
Financial Services 12%
Other 21%
Retail 43%
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@]
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


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.
'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 innovating on the methodology of this form of extortion. How secure?
From: Stealth Ravens [mailto:stealthravens@sigaint.org]
Sendt: Wednesday 11th January 2017 14:57
To:
Cc:

Subject: ddos attack

Hi!

If you dont pay 8 bitcoin until 17. january your network will be hardly ddosed! Our attacks are super powerfull. And if you dont pay until 17. january ddos attack will start and price to stop will double! We are not kidding and we will do small demo now on [IP address] to show we are serious. Pay and you are safe from us forever.

OUR BITCOIN ADDRESS: [BitCoin address]

Dont reply, we will ignore! Pay and we will be notify you payed and you are safe.

Cheers!
Attacks: Amplification
Tools: Havij

Havij - Advanced SQL Injection Tool

Version 1.15 Free
Copyright © 2009-2011
By r3dm0xv3

http://FTSecTeam.com
http://forum.lnetsec.com
info@ftsec.com
Check for update

Databases:
MySQL with error
MySQL no error
MySQL Blind (Pro Version)
MySQL false based (Pro Version)
MsAccess
MsAccess Blind (Pro Version)

Status: In idle

Setting to find string column
Finding string columns &
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.example.com/]
- Port: 80
- Threads: 1

Show received 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
Tools: LOIC

![LOIC Interface](image_url)

- Manual Mode
- F**king Hive Mind
- DAMN Overlord

1. Select your target
   - URL
   - IP

2. Ready?
   - Lock on
   - Unlock

3. Attack options
   - Timeout
   - HTTP Substrate
   - Append random chars to the URL
   - TCP/UDP message
   - Append random chars to the message
   - Use GET
   - Use UDP

4. Attack status
   - Kneeling
   - Connecting
   - Requesting
   - Downloading
   - Downloading
   - Resubmitting
   - Failed

IMMA CHARGIN MAH LAZER
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

```swift
var loggedIn bool
var userInfo AccountInfo
if loggedIn, userInfo = database.TryLogin(username, password); !loggedIn {
    this.conn.Write(nil, byte("\r\n\033[32;1mПроизошла неизвестная ошибка\r\n"))
    this.conn.Write(nil, byte("\033[31мнажмите любую клавишу для выхода. (any key)\033[0m"))
    buf := make([]byte, 1)
    this.conn.Read(buf)
    return
}
this.conn.Write(nil, byte("\r\n\033[0m"))
this.conn.Write(nil, byte("[+] DDOS | Successfully hijacked connection\r\n"))
time.Sleep(250 * time.Millisecond)
this.conn.Write(nil, byte("[+] DDOS | Masking connection from utmp+wtmp...\r\n"))
time.Sleep(500 * time.Millisecond)
this.conn.Write(nil, byte("[+] DDOS | Hiding from netstat...\r\n"))
time.Sleep(150 * time.Millisecond)
this.conn.Write(nil, byte("[+] DDOS | Removing all traces of LD_PRELOAD...\r\n"))
```
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", 6); // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x4F\x4B\x52\x41", 5); // root xmhdpic
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\x54\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

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?
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
Attack Density and Trends

- 100 Gbps
- 10 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

Jul 2015, Jan 2016, Jul 2016, Jan 2017
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.

- 711,477,622 Onliner Spambot accounts
- 593,427,119 Exploit.In accounts
- 457,962,538 Anti Public Combo List accounts
- 393,430,309 River City Media Spam List accounts
- 359,420,698 MySpace accounts
- 234,842,089 NetEase accounts
- 164,611,595 LinkedIn accounts
- 152,445,165 Adobe accounts
- 112,005,531 Badoo accounts
- 105,059,554 B2B USA Businesses
- 830,155 Pokémon Negro accounts
- 819,478 Warframe accounts
- 800,157 Onverse accounts
- 790,724 Brazzers accounts
- 777,387 Black Hat World accounts
- 776,125 Abandonia accounts
- 745,355 Android Forums accounts
- 738,556 WildStar accounts
- 735,405 MALL.cz accounts
- 707,432 Programming Forums accounts
- 699,793 mSpy accounts
Why this is a problem.
Passwords

http://pastebin.com/raw/JKiXaVxF
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

https://www.flickr.com/photos/scabeater/3279616674/sizes/o/
So, what to do?

- 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
STATE OF THE INTERNET.COM

STATEOFTHEINTERNET.COM
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!

Dave Lewis
@gattaca
dave@akamai.com