FritzFrog – New Fileless P2P Botnet Malware

Date: 02/09/2020

Shikha Sangwan

The newly discovered malware which is attacking SSH servers of mainly government organisations, banks, medical centres, telecommunication companies and educational institutions is a fileless botnet malware named **FritzFrog.** It is spreading all over the world since January. It is a peer-to-peer (P2P) botnet having miner characteristics which also spreads over network.

OVERVIEW

It was first discovered by Guardicore Labs in January 2020. It is a RAT which attacks on SSH servers by brute forcing and establish a backdoor. It is written in GO programming language. It does not have a centralised command and control server. It is distributed among different nodes on the network. These types of botnets are very hard to take down than centralised botnets. The malware is an ELF 64-bit LSB executable file.

THREAT ASSESSMENT

When we execute the malware, it deletes itself from the directory and creates a process in `/temp/` directory. It is a fileless malware and executes in the memory. The process in the /temp then starts performing malicious activities. It connects to C&C servers and fires `sshd` command which OpenSSH Daemon process. It attacks to other SSH servers in the network. It forms a backdoor in the system by adding a SSH RSA key in the system. It mines for cryptocurrency in the system by using CPU Mining method in which it utilizes processors to mine for cryptocurrency. The infection flow is shown in the diagram below:

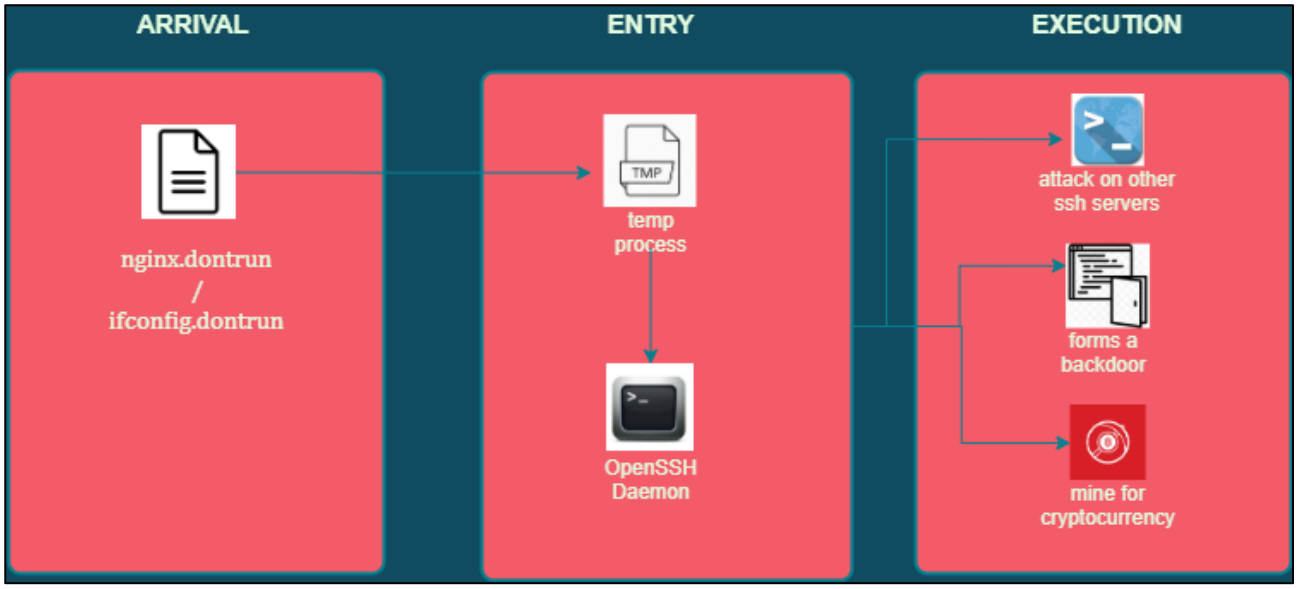

Figure 1 infection flow

After connecting to command and control server and it starts listening on the port "**1234**". It receives commands for execution and starts the process 'sshd'.

```
COMMAND    PID          USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd       791          root    3u  IPv4  20294      0t0  TCP *:ssh (LISTEN)
sshd       791          root    4u  IPv6  20296      0t0  TCP *:ssh (LISTEN)
```

Figure 2 OpenSSH Daemon

- **Attack on other SSH servers**

It adds itself to the p2p network and connects with the other peers in the network. Every node in the network has the ability to target systems and to communicate with each other over an encrypted channel. It attacks other SSH servers and propagate itself. Then it starts receiving and sending data from other peers in the network through SSH. All the packets sent and received between the ssh servers are encrypted. They keep communicating with each other to keep the network alive. It connects to more than hundreds of IPs through SSH.

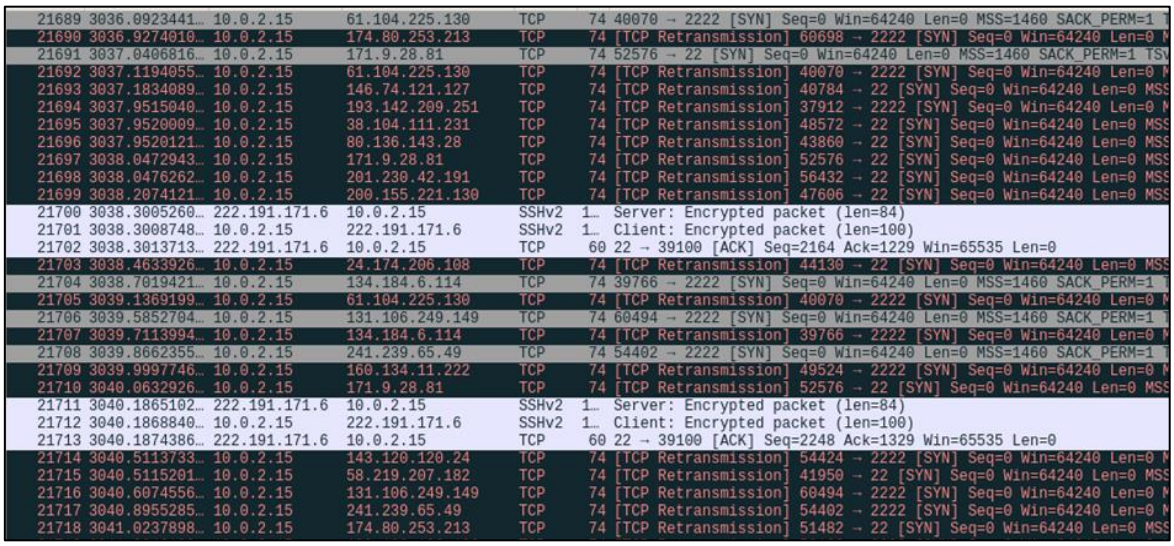

Figure 3 Connecting to other SSH servers in the network

The commands that are sent over the network are AES128 encrypted.

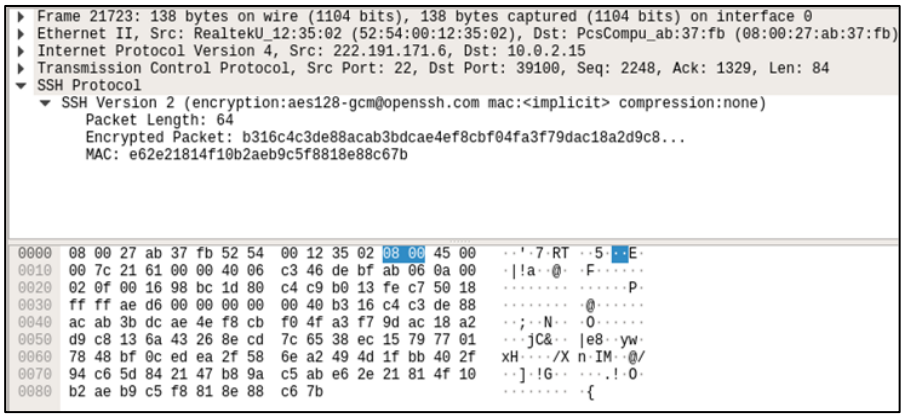

Figure 4 Encrypted Communication

- **Backdoor**

It drops a public SSH-RSA key to the "**`/root/.ssh/authorized_keys`**" which forms a **backdoor** in the victim machine which allow the attacker to run commands to get the system information and to access the machine even if the password is changed. This backdoor helps attacker to regain access to the victim even if the malware is removed.

The file that is dropped is : `9DA18D38B6DD4C4AA84642378D63FA89`

The Backdoor intends to collect the system information like cpu usage, logs, process status and mac address.(as shown in the image below)

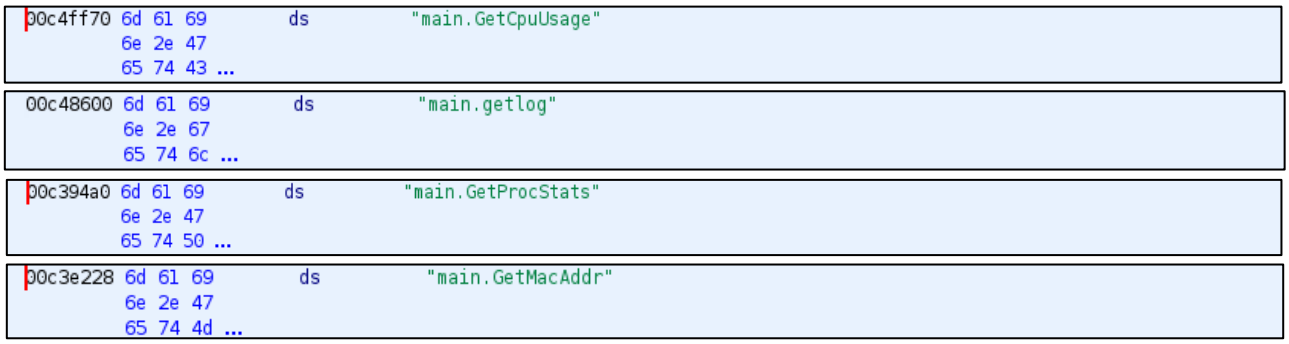

Figure 5 Collecting System Information

The malware doesn't leave any traces on the disk and it makes more difficult to detect it. It shows a pattern of evasion also. It deletes log files, execute sleep command and uses "**uname**" system call to query kernel version information.

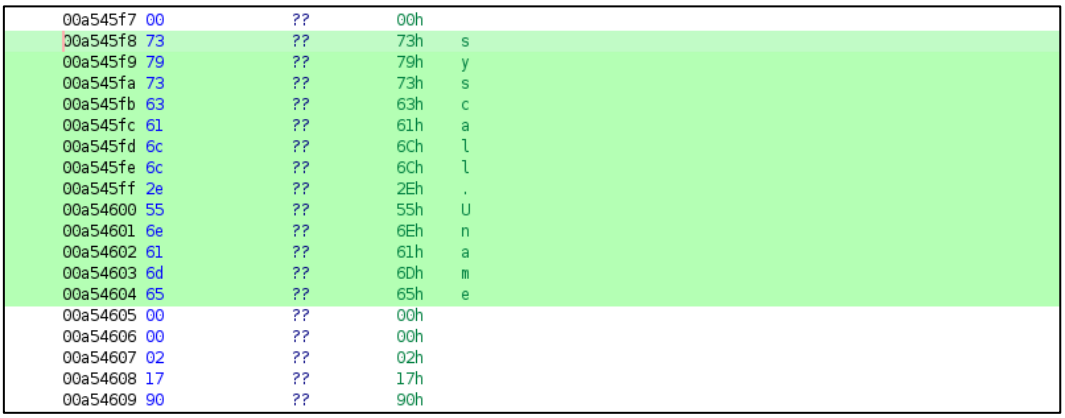

Figure 6 uname system call command

- **Cryptocurrency Mining**

The main goal of the malware is to mine for cryptocurrency. It executes "`free`" command used for querying memory usage, reads cpu information from `/proc` and `/sys` which is an indicative of miner or an evasive malware.

The commands that are used:

/usr/bin/free
/proc/cpuinfo
/sys/devices/system/cpu/online

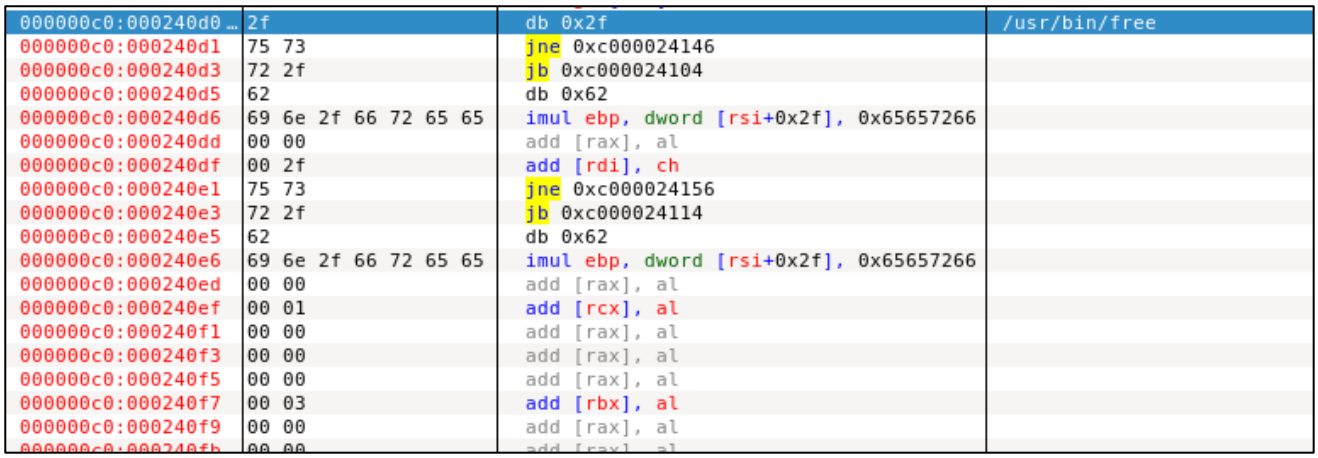

Figure 7 executing "free" command (Address:000240d0)

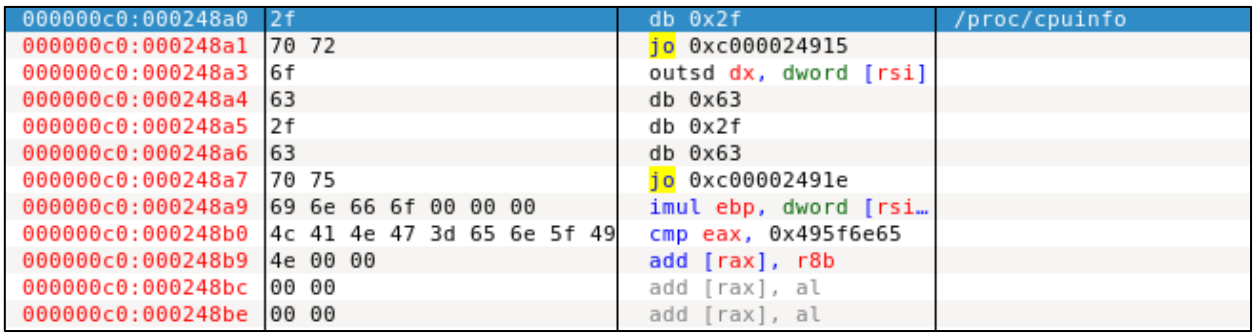

Figure 8 Getting CPU information from process (Address: 000248a0)

The files accessed and opened by the malware in the system are:

/etc/ld.so.cache
/lib/x86_64-linux-gnu/libselinux.so.1
/lib/x86_64-linux-gnu/libc.so.
/lib/x86_64-linux-gnu/libpcre.
/lib/x86_64-linux-gnu/libdl.so
/lib/x86_64-linux-gnu/libc-2.2
/lib/x86_64-linux-gnu/libpcre.
/lib/x86_64-linux-gnu/libdl-2.
/etc/passwd
/etc/ssh/ssh_host_rsa_key
/etc/protocols
/lib/x86_64-linux-gnu/libpthre
/proc/filesystems
/usr/lib/locale/locale-archive
/lib/charset.alias
/usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
/run/systemd/netif/state
/etc/locale.alias
/dev/null

/usr/lib/ssl/openssl.cnf
/etc/hosts.allow
/etc/hosts.deny

SUBEXSECURE PROTECTION

SubexSecure detects the FritzFrog botnet malware as '**SS_Gen_FrtizFrog_ELF_A**'.

IOCs:

The malware connects to the SSH servers of the following Ips:

183.87.208.152	116.184.30.162
176.222.5.159	145.70.221.30
136.2.40.72	60.122.215.91
19.151.44.110	170.126.250.222
159.96.206.208	208.238.243.246
13.187.25.44	84.17.181.87
85.109.55.87	100.151.4.85
170.197.175.149	156.159.7.4
153.84.219.105	214.191.177.90
11.98.68.40	197.105.100.17
66.221.90.76	64.110.190.60
61.166.113.28	105.39.175.239
251.3.141.32	148.82.203.251
223.106.189.110	

e6f7c7a083135ed8e97eb5c03725a1ed
100bff2f4ee4d88b005bb016daa04fe6
3a371a09bfcba3d545465339f1e1d481
d4e533f9c11b5cc9e755d94c1315553a
ae747bc7fff9bc23f06635ef60ea0e8d
c947363b50231882723bd6b07bc291ca
b2e0eede7b18253dccd0d44ebb5db85a
819b0fdb2b9c8a440b734a7b72522f12
aa55272ad8db954381a8eab889f087cf
3fe7b88a9ba6c5acee4faae760642b78
76fe4fdd628218f630ba50f91ceba852
8f0cb7af15afe40ed85f35e1b40b8f38
682ac123d740321e6ba04d82e8cc4ed8
97cfb3c26a12e13792f7d1741309d767
799c965e0a5a132ec2263d5fea0b0e1c

MITRE ATT&CK TECHNIQUES USED:

MITRE ID	MITRE TECHNIQUE NAME
T1210	Exploitation of Remote Services
T1021.004	SSH
T1110	Brute Force
T1098.004	SSH Authorized Keys
T1464	Jamming or Denial of Service
T1518.001	Security Software Discovery
T1082	System Information Discovery
T1003	OS Credential Dumping
T1564.001	Hidden Files and Directories
T1070	Indicator Removal on Host
T1070.004	File Deletion
T1059	Command and Scripting Interpreter

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 centres 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 centres 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, analysed, 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 flavours 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.