FritzFrog

Threat: **Botnet**

Author: **Jeffrey Farnan** Date Originally Published: **December 18th, 2020**

1. SUMMARY

- FritzFrog is a fileless Peer2Peer Botnet which uses a hybrid method to communicate with its targets, while avoiding detection. A unique feature of FritzFrog is that it's fileless, using worm like features to assemble and execute payloads in memory. When a new target has been identified, runs a series of tasks to brute-force the new machine, when successfully breached, infects the system and adds it to the P2P network.

2. MALWARE FAMILY

- **Type** = Botnet.
- **Sub-type** = Worm.

- FritzFrog is a Botnet, which is a network of hijacked zombie computers which are remotely controlled by a Hacker. The Hacker than decides snoop around, steal data or infect the machine with other malware. The Botnet usually comes with a worm component which runs unseen in memory. The worms aim is to infect other machines on the network by brute-forcing its way onto other devices, adding machines to its network and remaining undetected.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = United States.
- **First seen date/period** = January 2020.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = December 15th, 2020.

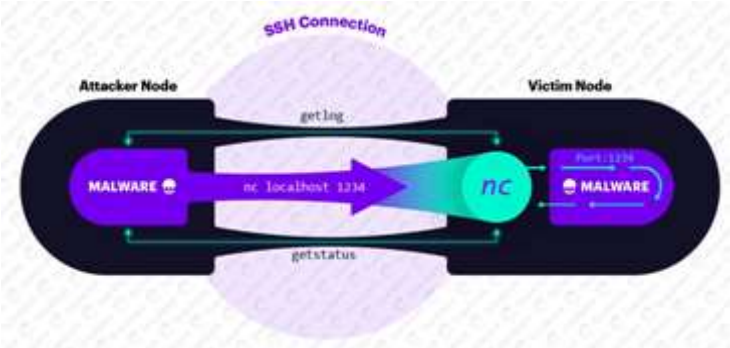
4. MALWARE HISTORY

- Guardicore Labs security researchers first spotted FritzFrog in January 2020, it is advanced Botnet with the capability to remain traceless on an infected machine. FritzFrog has been written from scratch using the Go language. Although not seen before researchers have discovered some resemblance to the Rakes P2P botnet that was discovered in 2016. This botnet uses the same techniques used by other botnets to gain access to remote machines, the difference with FritzFrog, is the sophisticated and stealthy way is goes about it. It has been observed brute-forcing millions of IP addresses, and over 500 servers targeting well known educational and finance organizations.

5. MALWARE DESCRIPTION

- FritzFrog is a fileless malware written in the Go language. It has many sophisticated features such as brute-force attacks on exposed SSH services, fileless execution in memory, a worm component which propagates across the network and a bespoke P2P protocol. The techniques used in its hybrid communication method:

- **Secure Shell Communication -** Firewalls can easily detect and block traffic on non-standard ports, such as port 1234. To evade detection, the attacker connects to the victim over SSH and runs netcat on the victim's machine, which in turn connects to the malware's server. Any command sent over SSH will be used as netcat's input, thus transmitted to the malware.



- **P2P and Encryption Communication -** FritzFrog has its own communications module, built with its own proprietary peer-to-peer (P2P) protocol, written from scratch, communications are done over an encrypted channel. FritzFrog attackers use an implemented encrypted command channel with 30 different commands. The data is encrypted using AES symmetric encryption and encoded in Base64. To slip under the radar, the malware runs malicious processes named ifconfig and nginx and listens on port 1234 for further instructions. The nodes constantly keep in contact with each other, to verify connectivity, exchange peers and targets and keep each other synced.
- **Transfer files and payloads -** FritzFrog has the ability to share files over the network both to infect new machines and run malicious payloads. It does this by creating a unique stealthy and fileless way to transfer files across the internet. To avoid detection, all its files are in memory and not on disk. The Files are split into blobs, or bulks of binary data, which are tracked and mapped by each blob's hash value.

When a node A wishes to receive a file from its peer, node B, it can query node B which blobs it owns using the command "getblobstats". Then, node A can get a specific blob by its hash, either by the P2P command "getbin" or over HTTP. When node A has all the needed blobs – it assembles the file and runs it.

6. POTENTIAL CUSTOMER DEFENSE

To prevent and detect a FritzFrog infection, it is advised that:

- All security software is updated regularly.
- Secure configurations are applied to all Client and Servers on the network.
- In security products make sure protection settings in all devices are tamper proof.
- All obsolete platforms are removed from the network.
- The network is continuously monitored, and any unusual activity is reported.
- Remote access is given to, and accept connections from authorized users, using strongly encrypted protocols.
- All Network Security Personal has the latest training and is kept up to data with security policies.

Research Sources:

- https://www.securityweek.com/fritzfrog-botnet-uses-proprietary-p2p-protocol
- https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/
- https://digital.nhs.uk/cyber-alerts/2020/cc-3602