SEQURETEK

FritzFrog

OVERVIEW

FitzFrog botnet written in GOlang is using secure and encrypted Peer-to-Peer communication protocol to distribute malware and take control of device nodes. Encrypted communication makes the botnet difficult to detect and enables it to propagate across multiple infected SSH servers.

OVERVIEW

- A sophisticated modular, multi-threaded and **file-less, Golang-Based** peer-to-peer botnet FritzFrog is **actively targeting SSH servers** of governmental offices, educational institutions, medical centers, banks and telecom companies since January 2020.
- FritzFrog successfully breached **500 servers** by infecting well-known universities in the U.S. and Europe, and a railway company.
- FritzFrog botnet has worm functionality and spreading over SSH to **mine Monero** crypto-currency.
- The botnet has decentralized P2P infrastructure that evenly **distributes control among all its nodes**, so there is **no single point-of-failure** and no command-and-control server (C2). P2P communication is done over an encrypted channel, using AES for symmetric encryption and the Diffie-Hellman protocol for key exchange.
- Routers and IoT devices with exposed SSH on internet are vulnerable to FritzFrog.

TECHNICAL DETAILS OF FRITZFROG P2P NETWORK

Target	Machine in target queue will scan and try to brute-force it
Deploy	Machine successfully breached and queued for malware infection
Owned	Machine successfully infected and will be added to the P2P network

Figure 1: FritzFrog Network machine states

- FritzFrog attackers uses **brute-force attack** to breach SSH server' credentials.
- After successful breach **malware creates a backdoor** in the form of **public SSH-RSA key**, backdoor enable attacker to access victim machines even if the password is changed.
- FritzFrog malware starts running the UPX-packed malware, which erase itself after execution. The malware process **runs under the names ifconfig and nginx**, to minimize suspicion.

- FritzFrog is listening on **port 1234 for commands**. The first commands which a new victim receives are responsible for **syncing the victim with the database of network peers and brute-force targets.**
- After this, the new victim becomes part of the P2P network and start contributing its CPU power to propagate to new SSH servers. It is also capable of receiving and executing commands from other peers in the network.
- To evade detection on port 1234, attacker connects to the victim over SSH and **runs a netcat client** on the victim machine, therefore any **command sent over SSH will be used as netcat's input** and transmitted to the malware.
- The Fritzfrog attackers implemented an encrypted command channel and before sending, the data is encrypted using AES symmetric encryption and encoded in Base64. Nodes uses Diffie-Hellman for key exchange protocol.
- The nodes in the FritzFrog Peer-to-peer network constantly ping each other to verify connectivity, exchange peers and targets and keep each other synced. The targets are evenly distributed, such that no two nodes in the network attempt to brute-force the same target machine in order to find new victim.

INDICATORS OF COMPROMISE

IP Addresses

100.0.197.18	115.143.66.28	139.198.191.245	163.172.43.70
102.131.59.246	118.25.62.164	139.199.163.77	166.168.111.151
103.127.80.9	120.24.243.109	14.54.245.109	167.86.73.135
103.21.76.18	121.155.49.93	14.54.245.220	175.24.57.194
103.39.209.157	121.156.203.3	140.207.83.149	176.139.8.11
104.47.156.119	121.201.61.205	142.44.196.234	176.99.12.209
106.75.7.111	122.225.18.194	145.14.157.171	178.22.123.208
107.172.90.18	122.51.48.52	148.70.167.224	18.27.197.252
107.187.122.10	123.30.149.92	148.70.242.55	187.189.63.82
109.244.35.20	123.57.138.150	150.165.60.105	190.221.81.6
111.161.72.176	124.119.89.249	154.126.56.85	190.88.251.27
112.217.225.61	124.124.44.156	156.155.179.14	192.144.239.96
113.15.114.151	13.235.253.205	161.139.68.245	195.154.179.3
114.217.179.49	13.90.45.216	162.252.57.102	195.91.184.205

196.189.91.162	222.154.86.51	5.26.221.186	69.85.84.10
198.100.146.76	23.254.217.214	50.250.21.164	71.62.129.30
198.54.62.248	3.122.60.196	51.75.31.39	73.144.18.16
209.126.106.161	3.127.255.82	52.175.252.75	73.254.114.94
210.5.88.89	31.206.240.54	52.231.188.167	78.5.170.222
211.110.184.22	34.92.90.235	54.93.55.80	80.211.245.21
218.146.128.93	35.229.239.179	57.100.69.129	81.130.146.18
218.151.100.195	39.106.111.11	59.24.153.124	81.170.214.154
218.151.35.193	45.143.136.213	59.26.132.133	82.64.138.80
218.93.239.44	45.249.92.58	60.172.206.11	85.95.191.56
220.135.59.164	45.32.122.40	60.253.116.46	89.238.5.94
220.179.231.188	45.32.128.117	62.117.12.62	90.249.10.17
220.77.145.80	45.84.196.108	62.210.73.82	90.249.102.111
221.142.135.128	46.101.2.179	66.130.210.106	90.249.182.105
221.176.177.194	46.97.44.18	68.84.68.139	90.249.196.75
221.182.207.107	47.100.108.185	68.97.74.52	94.191.15.40

Hash Values

001EB377F0452060012124CB214F658754C7488CCB82E23EC56B2F45A636C859

041BC20CA8AC3161098CBC976E67E3C0F1B672AD36ECBE22FD21CBD53BCAA742

0AB8836EFCAA62C7DAAC314E0B7AB1679319B2901578FD9E95EC3476B4C1A732

103B8404DC64C9A44511675981A09FD01395EE837452D114F1350C295357C046

2378E76ABA1AD6E0C937FB39989217BF0DE616FDAD4726C0F4233BF5414CDE86

23E390E6531623C1E9E09B1EAF807D501D1A01E45184B7D3FFC4EEED955B0C6D

30C150419000D27DAFCD5D00702411B2B23B0F5D7E4D0CC729A7D63B2E460A01

3205603282A636979A55AA1E1BE518CD3ADCBBE491745D996CEB4B5A4DECE0C5

39AB194DC7A7BA65615A30D99ED8845EE00AD19F2AC1236FBD71A671F7FA4C5A

453468B86856665F2CC0E0E71668C0B6AAC8B14326C623995BA5963F22257619

5FB29FB0136978B9CCF60750AF09CEC74A257A0CA9C47159CA74DBBA21FBCC59

6FE6808B9CFE654F526108EC61CB5211BB6601D28E192CADF06102073B54F69C

7745B070943E910E8807E3521AC7B7A01401D131BF6C18A63433F8177ED539A6

7F18E5B5B7645A80A0D44ADF3FECDAFCBF937BFE30A4CFB965A1421E034996DD

8C094313B1D4236AE3F630D93E8037B0A9D38DF716D5D7AED5B871DEA0DC1445

90B61CC77BB2D726219FD00AE2D0ECDF6F0FE7078529E87B7EC8E603008232D5
9384B9E39334479194AACB53CB25ACE289B6AFE2E41BDC8619B2D2CAE966B948
985FFEE662969825146D1B465D068EA4F5F01990D13827511415FD497CF9DB86
D1E82D4A37959A9E6B661E31B8C8C6D2813C93AC92508A2771B2491B04EA2485
D9E8D9187FDD5A6682CC3B55076FE48BC8743487EB4731F669A7D591D3015CE5

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- **Preventive Actions**
  - Block the IoCs in the corresponding security devices.
  - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
  - Use strong SSH password and public key authentication.
  - If possible change routers' and IoT devices' SSH port.
  - Disable SSH access if the service is not needed.

- **Corrective Actions**
  - If infected, Remove FritzFrog's public key from the authorized_keys file to remove backdoor.