Sophisticated FritzFrog P2P Botnet Returns After Long Break

securityweek.com/sophisticated-fritzfrog-p2p-botnet-returns-after-long-break

By Eduard Kovacs on February 14, 2022

Tweet

RSS

A sophisticated botnet named FritzFrog has returned after a long break with new capabilities, and researchers believe it may be linked to Chinese threat actors.

FritzFrog is a Golang-based malware that can be compiled to run on various architectures and it operates completely in memory. The FritzFrog botnet uses a proprietary peer-to-peer (P2P) architecture for command and control (C&C) communications — the bots don't get commands from a central server, but from any other device on its network.

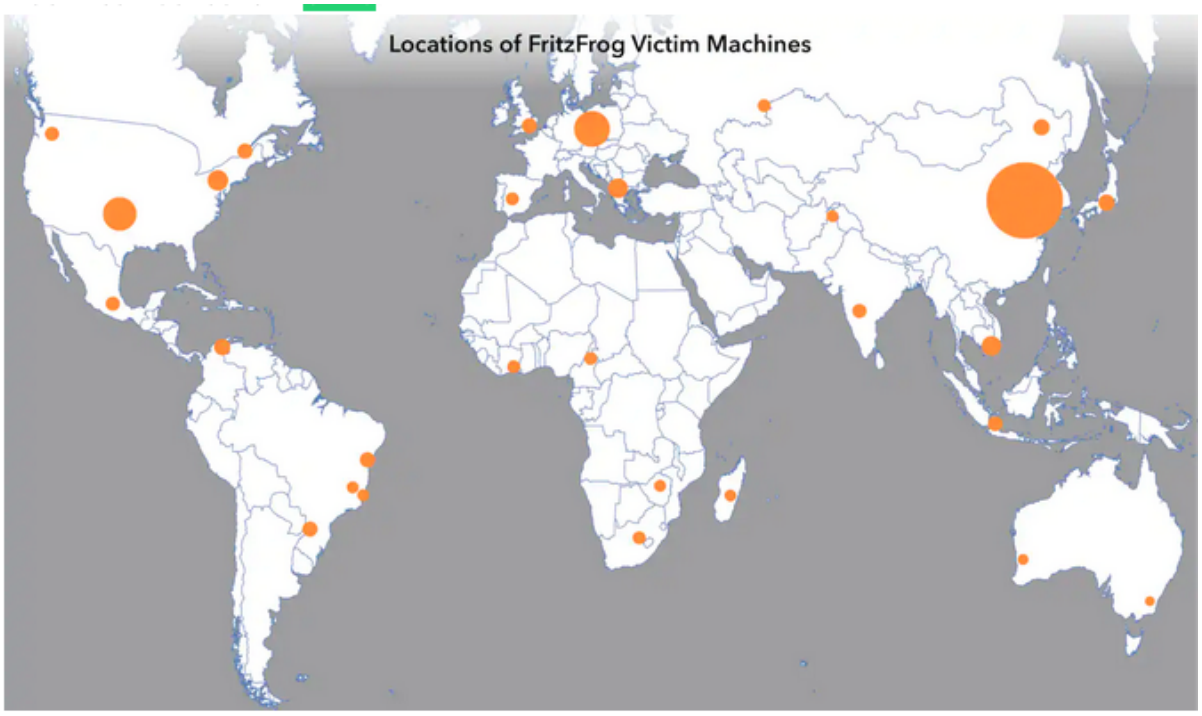
FritzFrog has targeted SSH servers — it uses a simple brute-force technique to obtain their credentials — and once it has established an SSH session, it drops the malware and executes it.

The malware then waits for commands from its operators, including for transferring files, running scripts and binary payloads, deploying a cryptocurrency miner, and eliminating other miners from the compromised system. It also starts scanning IP addresses to spread further.

FritzFrog emerged in January 2020 and it was detailed by micro-segmentation technology startup Guardicore in August 2020. Shortly after Guardicore's warning, the botnet seemed to disappear. However, it returned in December 2021 with new capabilities and many attack attempts — attacks peaked at 500 per day.

Akamai, which acquired Guardicore in 2021, warned last week that at least 1,500 hosts had been infected. The content delivery and security giant said the botnet has been seen targeting cloud instances, routers, and data center servers around the world.

A large concentration of victims has been seen in China, Central Europe and the United States. Targeted sectors include healthcare, higher education and government, and the list of victims singled out by Akamai includes a European TV network, a Russian healthcare equipment manufacturer, and East Asian universities.



According to Akamai, FritzFrog is often updated and there is some indication that its developers might be preparing to target WordPress servers. The company's researchers also noticed that FritzFrog contains functionality for creating a Tor proxy chain that would help it become more resilient. However, the Tor proxy chain functionality has yet to be used by the malware.

Other changes observed by Akamai include the use of a public Secure Copy Protocol (SCP) library that the malware leverages to copy itself to a compromised server, and a hardcoded blocklist for ensuring that the malware avoids systems with low resources and certain IP addresses — for instance, ones that may be botnet sinkholes.

The SCP library used by FritzFrog appears to have been developed by someone in China, and the cryptocurrency mining activity has been linked to wallets previously tied to Chinese threat actors. In addition, roughly one-third of the infected systems appear to be located in China.

"These points of evidence, while not damning, lead us to believe a possible link exists to an actor operating in China, or an actor masquerading as Chinese," Akamai said.

The company has shared indicators of compromise (IOCs), as well as a free tool that can be used to detect the presence of FritzFrog on SSH servers.

Related: Mirai Botnet Starts Exploiting OMIGOD Flaw as Microsoft Issues More Guidance

Related: Mirai-Based 'Manga' Botnet Targets Recent TP-Link Vulnerability

Related: Massive Android Botnet Hits Smart TV Ad Ecosystem

Tweet

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

Exploitation of VMware Vulnerability Imminent Following Release of PoC
FBI: Higher Education Credentials Sold on Cybercrime Forums
Google Announces New Chrome and Chrome OS Security Features for Enterprises
Cloud Security Firm Lacework Lays Off 20% of Workforce
VMware to Absorb Broadcom Security Solutions Following $61 Billion Deal
2022 CISO Forum: September 13-14 - A Virtual Event

Virtual Event Series - Security Summit Online Events by SecurityWeek

2022 Singapore/APAC ICS Cyber Security Conference]

2022 ICS Cyber Security Conference | USA [Hybrid: Oct. 24-27]

Tags:

- NEWS & INDUSTRY
- Virus & Threats
- Virus & Malware
- Malware
- Cybercrime