

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Virus & Threats](#)



New 'Enemybot' DDoS Botnet Targets Routers, Web Servers

By [Ionut Arghire](#) on April 15, 2022

Share

Tweet

推荐 0



A recently identified DDoS botnet has targeted several router models and various types of web servers by exploiting known vulnerabilities, Fortinet warns.

Dubbed [Enemybot](#), the botnet appears to be the work of Keksec, an established cybercrime group that specializes in DDoS attacks and cryptocurrency mining.

The malware was built using the source code of the [Gafgyt \(Bashlite\) botnet](#) - which leaked in 2015 - with some modules borrowed from the infamous [Mirai](#) botnet, including the scanner module and a bot killer module.

Enemybot employs several obfuscation techniques meant not only to prevent analysis, but also to keep it hidden from other botnets, and connects to a command and control (C&C) server on the Tor network.

The new botnet targets numerous architectures used within Internet of Things (IoT) products and can also target x86, which increases its chances of infection.

[READ: [Fast-Growing Golang-Based 'Kraken' Botnet Emerges](#)]

To spread, Enemybot attempts to compromise devices using known combinations of usernames and passwords, by running shell commands on Android devices with an exposed Android Debug Bridge port (5555), and by targeting roughly 20 known router vulnerabilities.

The most recent of the targeted security holes is CVE-2022-27226, a remote code execution issue that impacts iRZ mobile routers, and which was made public on March 19, 2022. Enemybot, Fortinet points out, is the first botnet to target devices from this vendor.

The threat also targets the now infamous Apache Log4j remote code execution [vulnerabilities](#) disclosed last year (CVE-2021-44228 and CVE-2021-45046), as well as a couple of path traversal issues in Apache HTTP server (CVE-2021-41773 and CVE-2021-42013).

Enemybot also attempts to exploit vulnerabilities in TOTOLINK routers and Seowon routers, as well as older flaws in ThinkPHP, D-Link routers, NETGEAR products, Zhone routers, and ZyXEL devices.

[READ: [FBI Disables "Cyclops Blink" Botnet Controlled by Russian Intelligence Agency](#)]

Once a vulnerability has been successfully exploited, the malware runs a shell command to download a shell script from a URL that is dynamically updated by the C&C. The script is responsible for downloading the actual Enemybot binary compiled for the target device's architecture.

After a successful infection, the malware connects to its C&C server and awaits instructions. Based on received commands, it can perform DNS amplification attacks and various types of DDoS assaults, sniff traffic, and spread to other devices via brute force attacks.

"This mix of exploits targeting web servers and applications beyond the usual IoT devices, coupled with the wide range of supported architectures, might be a sign of Keksec testing the viability of expanding the botnet beyond low-resource IoT devices for more than just DDoS attacks. Based on their previous botnet operations, using them for cryptomining is a big possibility," Fortinet notes.

Related: [Abcbot DDoS Botnet Linked to Older Cryptojacking Campaign](#)

Related: [Spring4Shell Vulnerability Exploited by Mirai Botnet](#)

Related: [Russia-Linked Cyclops Blink Botnet Attacking ASUS Routers](#)

Share

Tweet

推荐 0



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Juniper Networks Patches Vulnerabilities in Contrail Networking, Junos OS](#)
[Conti Ransomware Gang Claims Cyberattack on Wind Turbine Giant Nordex](#)
[New 'Enemybot' DDoS Botnet Targets Routers, Web Servers](#)
[Google Patches Third Actively Exploited Chrome Zero-Day of 2022](#)
[Cloud Security Startup DoControl Raises \\$30 Million](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

sponsored links

[2022 Singapore/APAC ICS Cyber Security Conference](#)

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

[2022 CISO Forum: September 13-14 - A Virtual Event](#)