FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

07 May 2025

FLASH Number

FLASH-20250507-001

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Cyber Criminal Services Target End-of-Life Routers to Launch Attacks and Hide Their Activities

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with 5Socks and Anyproxy cyber criminal services' targeting malware that affects end-of-life (EOL) routers. Threat actors exploit known vulnerabilities to compromise EOL routers, install malware, and use the routers in a botnet they control to launch coordinated attacks or sell access to the devices as proxy services. The FBI recommends users replace compromised devices with newer models or prevent infection by disabling remote administration and rebooting the router.

Technical Details

Overview

EOL routers were manufactured and produced many years ago and are no longer supported by their respective vendors with software updates or patches to fix known vulnerabilities. Threat actors are aware of these vulnerabilities and exploit them through various methods to install malware, set up a botnet, and sell proxy services.

The threat actors have successfully exploited known vulnerabilities in routers exposed to the Internet through remote management software that comes pre-installed on the devices. The threat actors use these known vulnerabilities to gain access to the devices and install malware. The malware allows the threat actors to maintain persistent access to the routers and to use them in a botnet controlled by the threat actors.

The botnets are used in various ways; such as launching coordinated attacks or selling access to the devices. With the 5Socks and Anyproxy network, criminals are selling access to compromised routers as proxies for customers to purchase and use. The proxies can be used by threat actors to obfuscate their identity or location.

List of Devices Vulnerable to Compromise

- E1200
- E2500
- E1000
- E4200
- E1500
- E300
- E3200
- WRT320N
- E1550
- WRT610N
- E100
- M10
- WRT310N

Distribution

The malware is distributed by targeting vulnerable devices connected to the Internet with remote administration turned on. Even with the remote administration password protected, the threat actors are able to bypass this authentication and gain shell access to the routers.

Exploitation

The threat actors use the device's known vulnerabilities to upload the malware, which ultimately allows the threat actor to gain root access to the device and make configuration changes. Chinese cyber actors are also among those who have taken advantage of known vulnerabilities in end of life routers and other edge devices to establish botnets used to conceal hacking into US critical infrastructures.

Persistence

The threat actors gain persistent access through the malware once installed. This allows the actor to communicate with the device on a regular basis (every 60 seconds to five minutes) to ensure it remains compromised and is available for use by customers.

Communication

The malware communicates with a command and control (C2) server through a two-way handshake between the server and the router that does regular check-ins with the devices and also opens ports to make them available to users as proxy servers.

Indicators

Since the malware is router-based, it is difficult for an end user to know if their device is compromised due to the inability of anti-virus tools to scan these devices. Below is a list of files associated with the malware's router exploitation campaign:

Hash	Name
661880986a026eb74397c334596a2762	0_forumdisplay-php_sh_gn-37-sh
62204e3d5de02e40e9f2c51eb991f4e8	1_banana.gif_to_elf_t
9f0f0632b8c37746e739fe61f373f795	2_multiquote_off.gif_to_elf_gn-p_forward-hw-data- to-exploit-server
22f1f4c46ac53366582e8c023dab4771	3_collapse_tcat_gif_sh_s3-sh
cffe06b0adcc58e730e74ddf7d0b4bb8	4_message_gif_to_elf_k
084802b4b893c482c94d20b55bfea47d	5_viewpost_gif_to_elf_s
e9eba0b62506645ebfd64becdd4f16fc	6_vk_gif_to_elf_b
41e8ece38086156959804becaaee8985	7_slack_gif_DATA
1f7b16992651632750e7e04edd00a45e	8_share_gif_DATA
2667a50869c816fa61d432781c731ed2	banana.gif-upx
0bc534365fa55ac055365d3c31843de7	message.gif-upx

Recommended Mitigations:

The FBI recommends users identify if any of the devices vulnerable to compromise are part of their networking infrastructure. If so, these devices should be replaced with newer models that remain in their vendor support plans to prevent further infection. Alternatively, a user can prevent infection by disabling remote administration and rebooting the device. Please refer to the specific instructions for your router for information on how to disable remote management.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Administrative Note

This product is marked **TLP:CLEAR**. Subject to standard copyright rules, the information in this product may be shared without restriction.