Internet Crime Complaint Center (IC3)

Published: 2025-05-07 · Archived: 2026-04-05 13:40:31 UTC

The Federal Bureau of Investigation (FBI) is issuing this announcement to inform individuals and businesses about proxy services taking advantage of end of life routers that are susceptible to vulnerabilities. When a hardware device is *end of life*, the manufacturer no longer sells the product and is not actively supporting the hardware, which also means they are no longer releasing software updates or security patches for the device. Routers dated 2010 or earlier likely no longer receive software updates issued by the manufacturer and could be compromised by cyber actors exploiting known vulnerabilities.

End of life routers were breached by cyber actors using variants of TheMoon malware botnet. Recently, some routers at end of life, with remote administration turned on, were identified as compromised by a new variant of TheMoon malware. This malware allows cyber actors to install proxies on unsuspecting victim routers and conduct cyber crimes anonymously.

Proxies and Router Vulnerabilities

A proxy server is a system or router that provides a gateway between users and the Internet. It is an intermediary between end-users and the web pages they visit online. A proxy is a service that relays users' Internet traffic while hiding the link between users and their activity.

Cyber actors use proxy services to hide their identities and location. When actors use a proxy service to visit a website to conduct criminal activity, like stealing cryptocurrency or contracting illegal services, the website does not register their real IP address and instead registers the proxy IP.

TheMoon Malware

TheMoon malware was first discovered on compromised routers in 2014 and has since gone through several campaigns. TheMoon does not require a password to infect routers; it scans for open ports and sends a command to a vulnerable script. The malware contacts the command and control (C2) server and the C2 server responds with instructions, which may include instructing the infected machine to scan for other vulnerable routers to spread the infection and expand the network.

Tips to Protect Yourself

Commonly identified signs of malware infections on routers include overheating devices, problems with connectivity, and changes to settings the administrator does not recognize.

The FBI recommends individuals and companies take the following precautions:

- If the router is at end of life, replace the device with an updated model if possible.
- Immediately apply any available security patches and/or firmware updates for your devices.

- Login online to the router settings and disable remote management/remote administration, save the change, and reboot the router.
- Use strong passwords that are unique and random and contain at least 16 but no more than 64 characters. Avoid reusing passwords and disable password hints.
- If you believe there is suspicious activity on any device, apply any necessary security and firmware updates, change your password, and reboot the router.

Victim Reporting and Additional Information

If you suspect you are a victim of a proxy service or your personal information has been compromised:

- File a complaint with the FBI Internet Crime Complaint Center (IC3), www.ic3.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting organization; designated point of contact.
- Contact your account provider immediately to regain control of your accounts, change passwords, and place alerts on your accounts for suspicious login attempts and/or transactions.
