Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 May 2018

PIN Number
20180523-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide

Summary

Cybersecurity researchers have identified that foreign cyber actors compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office/home office (SOHO) routers. The VPNFilter malware uses modular functionality to collect intelligence, exploit LAN devices, and block actor-configurable network traffic. Specific characteristics of VPNFilter have only been observed in the BlackEnergy malware, specifically BlackEnergy versions 2 and 3.

The FBI is recommending any owner of SOHO routers power cycle (reboot) the device to temporarily disrupt the malware and aid in the potential identification of infected devices by a non-profit security organization working with the FBI, pursuant to legal process.

Threat

The size and scope of this infrastructure impacted by VPNFilter malware is significant. The persistent VPNFilter malware linked to this infrastructure targets a variety of SOHO routers and network-attached storage devices. The initial exploit vector for this malware is currently unknown.

The malware uses modular functionality on SOHO routers to collect intelligence, exploit LAN devices, and block actor-configurable network traffic. The malware can render a device inoperable, and has destructive functionality across routers, network-attached storage devices, and CPU architectures running embedded Linux. The command and control mechanism implemented by the malware uses a combination of SSL with client-side certificates for authentication and TOR protocols, complicating network traffic detection and analysis.

Mitigation

The FBI is recommending any owner of SOHO routers power cycle (reboot) the device to temporarily disrupt the malware and aid in the potential identification of infected devices by a non-profit security organization working with the FBI, pursuant to legal process.

Network device management interfaces, such as Telnet, SSH, Winbox and HTTP should be turned off for WAN interfaces and secured with strong passwords and encryption when enabled. Network devices should be upgraded to the latest available versions of firmware, which often contain patches for vulnerabilities.

Rebooting affected devices will cause non-persistent portions of the malware to be removed from the system. Network defenders should ensure that first-stage malware is removed from the devices, and/or appropriate network-level blocking is in place prior to rebooting affected devices. This will ensure that second stage malware is not downloaded again after reboot.

While the paths at each stage of the malware can vary across device platforms, processes running with the name 'vpnfilter' are almost certainly instances of the second stage malware. Terminating these processes, and removing associated processes/persistent files that execute the second stage malware would likely remove this malware from targeted devices.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@fbi.gov. 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.

Administrative Note

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey