Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 25, 2018

Alert Number
I-052518-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

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

FOREIGN CYBER ACTORS TARGET HOME AND OFFICE ROUTERS AND NETWORKED DEVICES WORLDWIDE

SUMMARY

The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices. Foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office and home office routers. The malware is able to perform multiple functions, including possible information collection, device exploitation, and blocking network traffic.

TECHNICAL DETAILS

The size and scope of the infrastructure impacted by VPNFilter malware is significant. The malware targets routers produced by several manufacturers and network-attached storage devices by at least one manufacturer. The initial infection vector for this malware is currently unknown.

THREAT

VPNFilter is able to render small office and home office routers inoperable. The malware can potentially also collect information passing through the router. Detection and analysis of the malware's network activity is complicated by its use of encryption and misattributable networks.

DEFENSE

The FBI recommends any owner of small office and home office routers reboot the devices to temporarily disrupt the malware and aid the potential identification of infected devices. Owners are advised to consider disabling remote management settings on devices and secure with strong passwords and encryption when enabled. Network devices should be upgraded to the latest available versions of firmware.