Home and Office Router Security

The United States Computer Emergency Readiness Team (US-CERT) recently sent out an alert identifying that foreign cyber actors have compromised thousands of home and office routers worldwide. The actors used VPNFilter malware to target small office/home office (SOHO) routers. The malware is able to collect intelligence, exploit local area network (LAN) devices and block actor-configurable network traffic.

The malware can render a device inoperable and has destructive functionality across routers and network-attached storage devices (phones, laptops, tablets, etc.). The VPNFilter malware can impact sensitive or proprietary information, disrupt regular operations, including financial losses incurred to restore systems and files, as well as potential harm to an organization's reputation.

To temporarily disrupt the malware, it is recommended by the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) that owners of small/home office routers reboot their routers and networked devices.

To reboot or power cycle, switch off and unplug the power from your modem/router. Leave the router unplugged for at least 30 seconds. Plug the power back into the router and verify your internet connection. Rebooting affected devices will cause non-persistent portions of the malware to be removed from the system.

The DHS and FBI encourage SOHO routers to report information concerning suspicious or criminal activity to their local FBI office or the FBI's 24/7 CyberWatch (CyWatch). CyWacth can be contacted by phone at 855-292-3937 or by email at CyWatch@fbi.gov.

For more information on this alert, please visit www.us-cert.gov to view the full release.