Issued 5/30/18

Reboot Your Router to Disable Russian Linked Malware

The FBI is warning the public to reboot the routers they have in their home or office to disrupt a malware that may have infected as many as 500,000 routers in 54 countries.

According to investigators, the VPNFilter malware was created by the same Russian-linked hackers who infiltrated the Democratic National Committee ahead of the 2016 U.S. presidential election. The bureau said it was able to take down a website that was controlling the malware before the second phase could be unleashed. The malware is capable of collecting personal information that passes through the infected routers, block web traffic and disable the devices. The FBI said rebooting routers will disrupt the malware and help the bureau identify which networking devices were affected.

So far, the routers affected were manufactured by Linksys, Mikrotik, Netgear, QNAP and TP-Link.

Follow these steps to reboot your router:
1. Turn off the device.
2. Unplug the router from the electrical outlet.
3. Leave the device unplugged for at least 30 seconds.
4. Plug the router back into the electrical outlet and power the device on.
5 Check to see if your internet connection was re-established.

As an additional security measure, the FBI suggests you update your router's firmware and set a new password.