UC SANTA BARBARA

THE Current

June 6, 2018

Sonia Fernandez

Better Safe than Sorry

If you haven't already done so, reboot your router now. Better yet, reset it back to factory settings and/or update its firmware settings. The added security is worth any temporary inconvenience.

"Your router is one of the most important things in your house or small business," said Sam Horowitz, UC Santa Barbara's chief information security officer, "so you need to factory reset, or upgrade it or update the firmware to wipe the malware out completely."

This advice comes direct from the FBI, following reports that the agency had intercepted malware with ties to Russia — and that over half a million routers had likely been infected. This malicious code known as VPNFilter can snoop into your private files and monitor your web traffic. It may also turn your router into a zombie, which, when networked with other compromised routers, could launch a large-scale Distributed Denial of Service (DDoS) attack. As a safety precaution, anyone unsure about the vulnerability of their router, regardless of make or model, should perform the reset or upgrade.

"How this originally happened, we don't know,"Horowitz said. Campus wireless networks are not vulnerable to VPNFilter and ETS is working to address any issues found in the departments that operate vulnerable routers. However, due to the unprecedented potential for mayhem, Horowitz sent an urgent memo to the campus community — in the same way the FBI urged the general public to power down their home and small office routers — in an effort to thwart the spread of the malware.

Not every brand of router, and not all routers made by those manufacturers found to have the malware (including Netgear, Linksys and TP-Link), have been infected. Those more likely to have been compromised have either not had their firmware updated or their passwords changed since they were set up. Many of the more recent models may have an autoupdate function, but those that have been in use for a couple of years likely do not, according to Horowitz. VPNFilter is thought to have been crawling the web for at least that long.

“The software itself is interesting,” Horowitz said. “It has three parts. The first part is the part that somehow or other infects your router and has a permanent foothold in your router.” That foothold allows for the second stage of the attack, in which other malicious code and programs can be downloaded, uploaded and executed through the router. “It’s basically a remote control back door for your router,” Horowitz said.

Stage three further enhances this activity. Researchers at Talos, the security branch of Cisco Systems, have discovered that aside from the plugins and extensions that allow for the snooping and traffic monitoring, there also is a “kill” function that can turn your router into a brick. One dead router is painful enough for a family sharing a network at home; a network of these with exposed sensitive information or disrupted access to the internet can wreak havoc for a small business.

The FBI, said Horowitz, was able to take control of the “command-and-control” infrastructure that initiates the downloading and execution of plugins and programs, but the power-down maneuver is only a quick and possibly temporary fix. To remove the persistent malware, the “inside man” that opens the door to further infection, routers should be reset back to factory settings, or have their firmware updated. Accomplishing the former is usually done via a button on the router, or the tried-and-true paperclip-in-the-hole maneuver. The latter will require visiting the manufacturer’s website and downloading updated firmware. And don’t forget to reset your passwords.

This latest attack highlights the vulnerability of routers, which, once they are up and running, most consumers don’t pay much attention to. The inconvenience and relative labor-intensiveness of manually checking for and downloading firmware is often why routers have become vulnerable to these kinds of attacks.

“The router isn’t just a router; there’s a Linux-based computer in there,” Horowitz said. In addition, one router typically has access to several computers, not to

mention the growing population of wearables, voice assistants, smartphones and other devices in the Internet of Things. While VPNFilter has not (yet) been found to be able to access all these devices, there have certainly been instances where similar malware was deployed to commandeer internet-enabled gadgets, such as the Mirai malware, which created a network or remotely controlled “bots” (a “botnet”) that in late 2016 attacked webcams and routers.

One non-router device, the QNAP digital storage device, has been found to be similarly vulnerable to VPNFilter, said Horowitz.

It is not yet clear if this incident is the end of the VPNFilter attack, but if enough people observe the security measures, the malware’s reach will be restricted.

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.