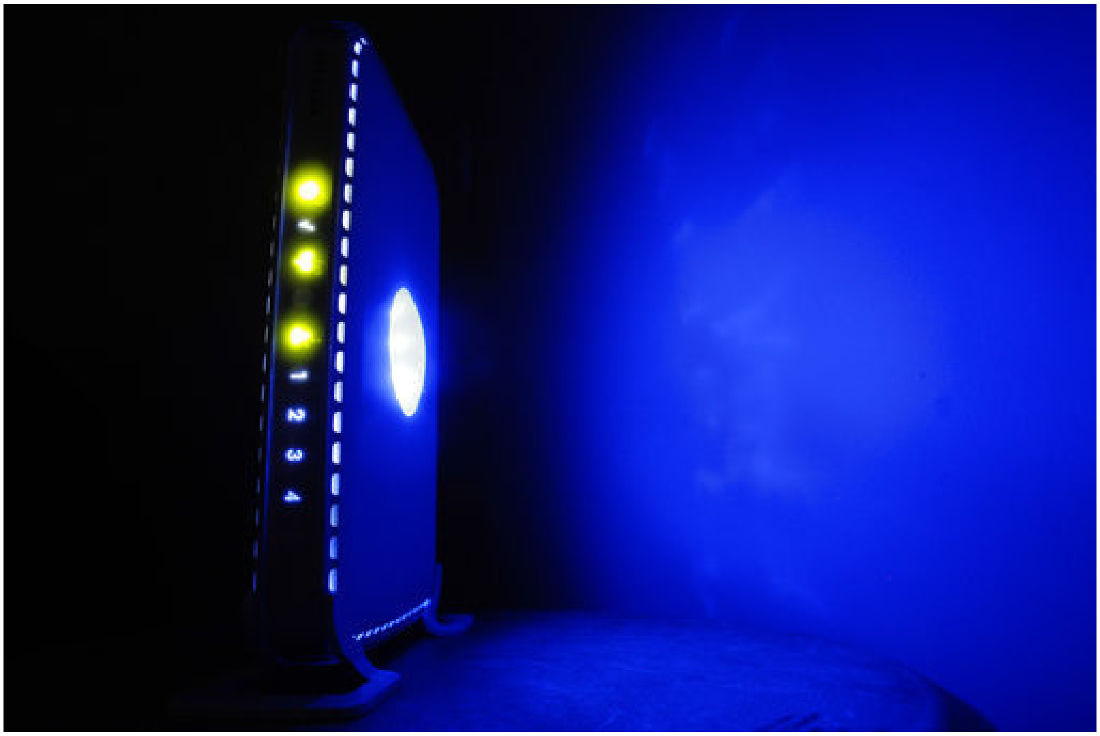
Q&A: Should you reboot your router like the FBI says?

May 30 2018, by The Associated Press



This July 27, 2008, file photo shows a, LED-illuminated wireless router in Philadelphia. Last week, the FBI recommended rebooting home and small office routers that could have been infected with disruptive malware, allegedly by sophisticated state-backed Russian hackers. An estimated half million routers and network-attached storage devices have been infected. But even the FBI admits this step will only "temporarily disrupt" the malware. (AP Photo/Matt Rourke, File)

Last week, the FBI recommended rebooting home and small office routers that could have been infected with disruptive malware, allegedly by sophisticated state-backed Russian hackers . An estimated half million routers and network-attached storage devices have been infected.

But even the FBI acknowledges this step will only "temporarily disrupt" the malware. Here are some questions and answers about the situation:

Q: How can I tell if my router is infected?

A: Short answer: You probably can't. Routers aren't very consumer-friendly, and most people lack the ability to get deep enough inside the device to tell if it's infected.

Q: If my router was infected and I reboot, is it safe?

A: No. Turning an infected router off and on again only removes some of the malware—such as elements that could snoop on your internet activity or even overwrite the basic code on your router, thus "bricking" it (that is, turning it into an inoperable brick). The core infection persists on reboot and there's no simple way to delete it.

The good news is that last week, the FBI seized of the command-and-control server that sends instructions to the infected routers, disrupting the zombie network that could be used to mount a crippling internet-based attack. The bad news is that the persistent malware is in listening mode, awaiting instructions. "So all the cards are still on the table," said Craig Williams of Cisco's Talos cyberthreat intelligence team, which identified the operation it calls VPNFilter.

Q: Why can't I completely remove the malware from my router?

This July 27, 2008, file photo shows an LED-illuminated wireless router in Philadelphia. Last week, the FBI recommended rebooting home and small office routers that could have been infected with disruptive malware, allegedly by sophisticated state-backed Russian hackers. An estimated half million routers and network-attached storage devices have been infected. But even the FBI admits this step will only "temporarily disrupt" the malware. (AP Photo/Matt Rourke, File)

A: For starters, routers are difficult for ordinary users to fiddle with. They have publicly known vulnerabilities that aren't easy for average users to patch and typically aren't equipped with anti-virus software packages or intrusion protection systems. That said, if you can update your router's "firmware" to the latest version—something you can often do via the router's phone app or web interface—you should. It may not fix the problem, but it won't hurt and may help.

Q: Which devices are affected and where can I learn more?

A: Cisco identified these companies as makers of affected devices: Linksys, Mikrotik, Netgear, TP-Link and QNAP. It said most of the infected routers are in Ukraine. You can find more details from Talos and the United States Computer Emergency Readiness Team . The FBI says it has nothing new to report beyond the announcement it put out Friday.

—-

Links:

FBI announcement: www.ic3.gov/media/2018/180525.aspx

Talos blog: blog.talosintelligence.com/2018/05/VPNFilter.html

U.S. CERT release: www.us-cert.gov/ncas/alerts/TA18-145A

Citation: Q&A: Should you reboot your router like the FBI says? (2018, May 30) retrieved 9 April 2024 from https://phys.org/news/2018-05-qa-reboot-router-fbi.html