The FBI Is Telling Everyone to Reboot Their Internet Router - What You Need to Know

May 29, 2018 - The FBI is warning that hundreds of thousands of internet routers across the country have been infected with malware called VPNfilter. They believe the malware to be the product of Russian hackers. The agency is telling anyone responsible for a router in a home or business network that they should immediately reboot their router to get rid of the threat. But not all routers manufacturers have been impacted and a simple reboot might not do the trick for routers that have been.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Routers manufactured by Linksys, Mikrotik, QNAP and TP-Link are known to have been infected so far. For the most part, impacted routers have been running older firmware with factory default passwords and user names. Cisco has released what it believes to be a complete list of the devices affected that you can find here.

Neither the router manufacturers nor the FBI currently know how the routers became infected but they do have some idea of what VPNfilter can do. It can steal website logon information and it can destroy the router.

While the FBI is simply telling people to reboot their router, according to a posting on KrebsOnSecurity.com, Cisco is warning that a reboot may not do the trick. They are telling people to update the firmware on their routers and then do a factory reset.

Doing a reset is a simple process. On most routers, it can be accomplished by simply pressing a button. Getting your network up and running again after a factory resent isn't so simple though. It means that you have to completely reconfigure your router and the equipment connected to it. If you are a technical novice, you should seriously consider hiring someone to do this for you.

If you own one of the routers on the list, we're advising that you do a factory reset of your router. Not doing so could result in giving criminals access to any websites that you sign onto, including banks and brokerages. In the case of businesses, banking losses may not be covered under federal law. And in the case of consumer bank accounts, losses will only be covered if reported within certain time frames.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS