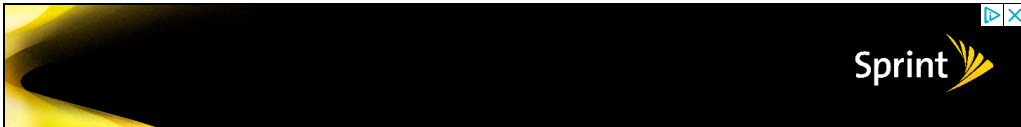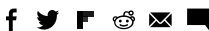# The FBI wants you to factory reset your router. Here's how to do it

The VPNFilter malware problem is getting worse. Here's how to safeguard your home network, and a list of the affected models.

BY **RICK BROIDA** / JUNE 6, 2018 6:48 PM PDT

The list of routers affected by VPNFilter has grown considerably.

Chris Monroe/CNET

Good news, everyone! Remember that FBI reboot-your-router warning in response to Russian malware VPNFilter? Turns out it's worse than originally thought, and a lot more people are going to need to do a lot more than just reboot their routers.

According to a new report from security firm Cisco Talos, the VPNFilter malware is "targeting more makes and models of devices than initially thought, and has additional capabilities, including the ability to deliver exploits to endpoints."

That means if you own one of the affected routers -- and that list has expanded to include models from Asus, D-Link, Huawei, Ubiquiti, Upvel and ZTE -- it's strongly recommended that you perform two key steps: upgrade the firmware and then factory-reset the router.

Ugh. This is going to suck. But we can get through it.

Step 1: Upgrade your router's firmware

In some ways this is the easier step, as it can often be done within the confines of your router's dashboard. Firmware is just the core software that operates the router, and updating it usually involves little more than a download and a few automated router restarts.
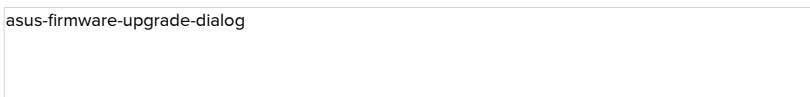
Of course, if you've never so much as looked at that dashboard, well, it may be time for a trip to the owner's manual -- or the router manufacturer's online help pages.

Because the firmware-update process varies from one make and model to another, here's a quick, generalized overview -- one that's based on upgrading an Asus WRT router.

Step i: Visit the Asus support site and download the most current firmware for your specific model.

Step ii: Open a browser window, type in **192.168.1.1** and press **Enter**. This will take you to the router's dashboard page -- but you may need a username and password to gain access. If you never changed the defaults, you should be able to find them in the instruction manual. (Often, the defaults are "admin" and "password," respectively.)

asus-firmware-upgrade-dialog

Updating your router's firmware may involve a screen like this.
Asus

Step iii: Click the **Administration** button (again, this is just for

Asus routers; on other models it might be Configuration or Firmware or the like), then the **Firmware Upgrade** tab.

Step iv: Click **Choose File** and locate the firmware file you downloaded in Step 1. Then click **Upload** to perform the update.

This may take a few minutes, and your router will likely restart at least once during the process. Needless to say, you'll lose all internet connectivity while this is happening.

And, again, this is just one example of the firmware-update process. It's a common one, but the steps may be different for your model.

Watch this: Russian hackers targeting your router: Here's what to...   1:23 📹
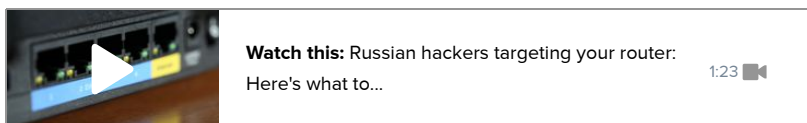
Step 2: Factory-reset your router

Now for the big hassle. You probably know that you can reboot or reset your router by pulling the power cord for a few seconds and then plugging it back in. But a *factory* reset is a little different. True to its name, it restores all the settings to their original, factory state, so once it's done, you get to have the fun of setting up your home network again.

Before you get started, make sure to write down the name and password of each Wi-Fi network currently configured on your router. You might have just one; I've seen houses that had five. You'll want to note these so you can recreate them verbatim after the factory reset.

Why is that important? Because if your current "SmithLAN" network becomes "Smith LAN" after the reset (just because you forgot and added a space this time), now you'll have to manually reconnect every device in your house to that "new" network. Hassle city.

The actual reset should be pretty easy. On some Linksys routers, for example, there's a small reset button on the unit itself. You press and hold it for 10 seconds and that's it. Alternately, you may be able to sign into the dashboard and execute the reset from there. In the aforementioned Asus example, in Step 3, you'd click the **Restore/Save/Upload** tab and then the **Restore** button.

Again, consult your router manual (or router's website) for the correct factory-reset steps for your model.

Here are links to the support directories for some of the affected routers (the complete list is in the next section):

- Asus support
- D-Link support
- TP-Link support
- Linksys support
- Netgear support

When it's done, you'll have to venture into the dashboard and recreate your networks. Thankfully, with your firmware upgraded and any trace of VPNFilter eradicated, you *should* be safeguarded from future attacks -- of this particular malware, anyway.

Which routers are affected?

Courtesy of Cisco Talos, here's a current list of the models that can be affected by VPNFilter. Those identified as new weren't included in the original report.

Asus

- RT-AC66U (new)
- RT-N10 (new)
- RT-N10E (new)
- RT-N10U (new)
- RT-N56U (new)
- RT-N66U (new)

D-Link

- DES-1210-08P (new)
- DIR-300 (new)
- DIR-300A (new)
- DSR-250N (new)
- DSR-500N (new)
- DSR-1000 (new)

- DSR-1000N (new)

Huawei

- HG8245 (new)

Linksys

- E1200
- E2500
- E3000 (new)
- E3200 (new)
- E4200 (new)
- RV082 (new)
- WRVS4400N

Mikrotik

- CCR1009 (new)
- CCR1016
- CCR1036
- CCR1072
- CRS109 (new)
- CRS112 (new)
- CRS125 (new)
- RB411 (new)
- RB450 (new)
- RB750 (new)
- RB911 (new)
- RB921 (new)
- RB941 (new)
- RB951 (new)
- RB952 (new)
- RB960 (new)
- RB962 (new)
- RB1100 (new)
- RB1200 (new)

- RB2011 (new)
- RB3011 (new)
- RB Groove (new)
- RB Omnitik (new)
- STX5 (new)

Netgear

- DG834 (new)
- DGN1000 (new)
- DGN2200
- DGN3500 (new)
- FVS318N (new)
- MBRN3000 (new)
- R6400
- R7000
- R8000
- WNR1000
- WNR2000
- WNR2200 (new)
- WNR4000 (new)
- WNDR3700 (new)
- WNDR4000 (new)
- WNDR4300 (new)
- WNDR4300-TN (new)
- UTM50 (new)

Qnap

- TS251
- TS439 Pro
- Other QNAP NAS devices running QTS software

TP-Link

- R600VPN
- TL-WR741ND (new)

- TL-WR841N (new)

Ubiquiti

- NSM2 (new)

- PBE M5 (new)

Upvel

- Unknown models (new)

ZTE

- ZXHN H108N (new)

READ MORE:

Best VPN services for 2018

Best ID monitoring services for 2018

SHARE YOUR VOICE   TAGS

[💬 48 comments]   [Security]   [Networking]   [ZTE]   [Asus]

Malware   Cisco   Huawei   Linksys

D-Link   Netgear

⌄ **Next Article:** Why Apple's in no rush to sell you a 5G iPhone ⌄

CNET Magazine

Check out the fall issue of CNET Magazine to learn about Blockchain, discover the latest innovation in beekeeping and find out how to take the jet lag out of long-distance travel. You can also get glimpses into the future of supersonic jets, augmented hearing devices and a Star Trek-style holodeck.

Read Now!

Download the CNET app / About CNET / Sitemap / Privacy Policy / Ad Choice / Terms of Use / Mobile User Agreement / Help Center