# NEWS BRIEF

## FBI Urges Consumers to Reset Their Routers to Prevent a Malware Attack

Recently, researchers at Talos—a cyber intelligence unit of Cisco—warned consumers of malware (malicious software) that specifically targets networking devices. The malware, which is known as VPNFilter, impacts an estimated 500,000 routers worldwide, particularly targeting devices from the following manufacturers:

- Linksys
- MikroTik
- Netgear
- QNAP
- TP-Link

### VPNFilter Could Collect Your Information Without Your Knowledge

Once on your equipment, the malware could stop your router from working, collect information from any systems that run through it and even block network traffic. Experts are concerned over the scope of the attack, as anyone owning a router from the affected manufacturers could be at risk, including businesses and individuals.

Agencies like the FBI have also expressed concern over VPNFilter, as this particular brand of malware can be used in espionage attacks on military, security and other government organizations.

### Reduce Your Risk by Resetting Your Router

Unfortunately, there's no simple way to tell if your router is infected. To protect yourself, it is recommended that you:

- Reset your router to disrupt the malware. This can be done by simply turning the router off and on or holding the reset button down on your device. For further protection, you may want to consider doing a factory reset of your router.
- Install any firmware updates. These updates are typically found on the manufacturer's website. You may need to search by your router's model number, which can be found on the back of the device.
- Create a new, secure password for your router.
- Disable remote management settings.

For help performing any of the above steps, contact your router manufacturer or click the links provided in this News Brief.

---

CONSULTATIVE INSURANCE GROUP