

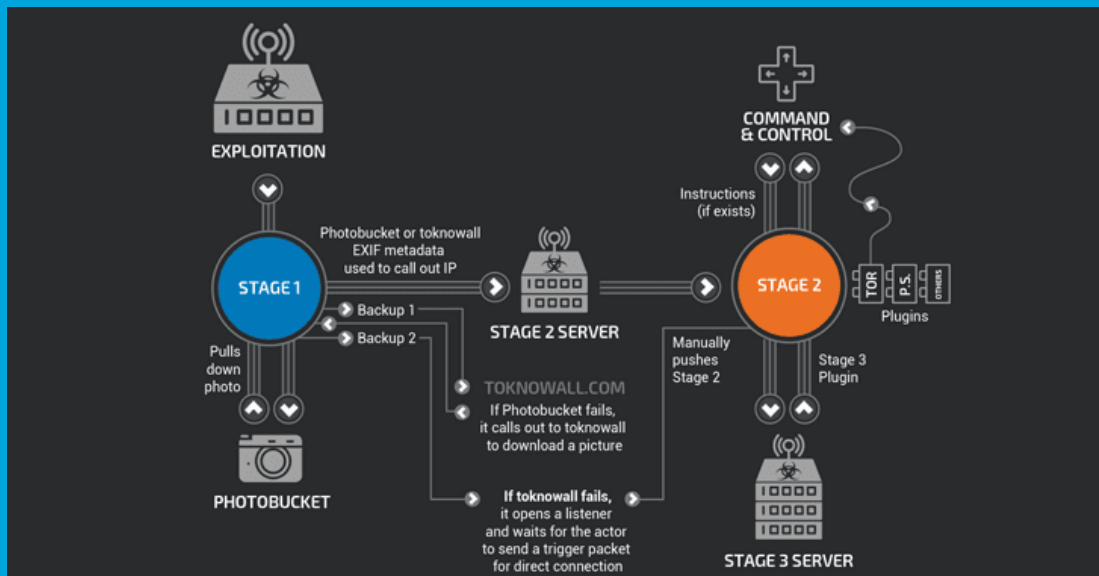


Security Newsletter

28 May 2018

[Subscribe to this newsletter](#)

VPNFilter: FBI Seizes botnet army of 500,000 hacked routers



More than half a million routers and storage devices in dozens of countries have been infected with a piece of highly sophisticated IoT botnet malware, likely designed by Russia-baked state-sponsored group. Cisco's Talos cyber intelligence unit have discovered an advanced piece of IoT botnet malware, dubbed VPNFilter, that has been designed with versatile capabilities to gather intelligence, interfere with internet communications, as well as conduct destructive cyber attack operations.

VPNFilter is a multi-stage, modular malware that can steal website credentials and monitor industrial controls or SCADA systems, such as those used in electric grids, other infrastructure and factories. The malware communicates over Tor anonymizing network and even contains a killswitch for routers, where the malware deliberately kills itself.

The US Federal Bureau of Investigation (FBI) has obtained court orders and has taken control of the command and control servers of a massive botnet of over 500,000 devices, known as the VPNFilter botnet. The FBI confirmed that the botnet has been created and was under the control of a famous Russian cyber-espionage unit known under different names, such as APT28, Sednit, Fancy Bear, Pawn Storm, Sofacy, Grizzly Steppe, STRONTIUM, Tsar Team, and others. A report authored by the Estonian Foreign Intelligence Service claims APT28 is a unit of the Russian Military's Main Intelligence Directorate (abbreviated GRU). With the domain firmly in its grasp, the FBI is now asking users across the world who own affected routers and NAS devices to reset their equipment.

[Read More](#)

[Even More](#)

SpectreNG: Google and Microsoft Reveal New Spectre Attack



Security researchers from Google and Microsoft have found two new variants of the Spectre attack that affects processors made by AMD, ARM, IBM, and Intel. AMD, ARM, IBM, Intel, Microsoft, Red Hat and Ubuntu have published security advisories at the time of writing, containing explanations of how the bugs work, along with mitigation advice.

The bugs —referred to in the past weeks as SpectreNG— are related to the previous Meltdown and Spectre bugs discovered last year and announced at the start of 2018. Both Google and Microsoft researchers discovered the bug independently. The bugs work similarly to the Meltdown and Spectre bugs, a reason why they were classified as "variant 3a" and "variant 4" instead of separate vulnerabilities altogether.













The researchers also claims that one of the vulnerabilities is much more dangerous than the original Spectre. In theory, attackers could launch exploit code from within a virtual machine, which could then attack the host or other VMs. Unfortunately, these attacks could even sidestep Intel's Software Guard Extensions (SGX), which are designed to protect the most sensitive passwords and encryption keys.

[Read More](#)

[Even More](#)

GDPR: Request your personal data from 100+ companies.

Where do you want to request your data from?

 Tinder	 Facebook	 Uber	 Lyft
 DoorDash	 GrubHub	 LinkedIn	 Slack
			

Hundreds of companies store & process information about you. In many cases, you're entitled to this data, as well as information on how it's being used & shared. MyDataRequest.com read these companies' privacy policies to figure out how you can get this data about you.

Depending on where you live, you may be subject to certain regulations that entitle you to access certain types of personal data. You can use their templates to make these requests.

In the EU: People in the EU can access personal data based on the EU Data Protection Directive. These rights will be extended by the General Data Protection Regulation (GDPR) that came into effect on May 25, 2018.

[Read More](#)

Cutting room floor

- [Backdoor Account Found in D-Link DIR-620 Routers](#)
- [Amazon asked to stop selling facial recognition technology to police](#)
- [Google Chrome Has a Built-In Password Generator. Here's how to use it!](#)
- [Hijack of Amazon's internet domain service used to reroute web traffic for two hours unnoticed](#)
- [Microsoft to Block Flash in Office 365](#)
- [Comcast is \(update: was\) leaking the names and passwords of customers' wireless routers](#)
- [Sunder: User-friendly graphical interface for cryptographic secret sharing.](#)
- [Data of Over 200 Million Japanese Sold on Underground Hacking Forum](#)
- [CT is coming, are you ready?](#)
- [GPON Routers Attacked With New Zero-Day](#)
- [Electron patches patch after security researcher bypassed said patch](#)
- [The AWS Bucket List for Security](#)
- [Brain Food botnet infected 5,000+ websites with malicious PHP scripts in past 4 months](#)
- [Firefox 63 to Get Improved Tracking Protection That Blocks In-Browser Miners](#)
- [Microsoft EnclaveDB can defend against malicious database admins, compromised OS](#)

#Tech and #Tools

- [WPA3: Technical Details and Discussion](#)
- [Analysis and mitigation of speculative store bypass \(CVE-2018-3639\)](#)
- [Announcing CERT Tapioca 2.0 for Network Traffic Analysis](#)
- [CVE-2018-5175: Universal CSP strict-dynamic bypass in Firefox](#)
- [Compromising Thousands of Websites Through a CDN](#)
- [An Analysis of Cloudflare's Email Address Obfuscation](#)
- [Kerberoasting, exploiting unpatched systems – a day in the life of a Red Teamer](#)
- [CobaltSplunk: Use Splunk as a central log database and analysis system for offensive infrastructure logs.](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>

If you no longer wish to receive this newsletter, you can [unsubscribe from this list](#).