EXCLUSIVE

PHOTO ILLUSTRATION BY ELIZABETH BROCKWAY/THE DAILY BEAST

EXCLUSIVE

GOTCHA

Exclusive: FBI Seizes Control of Russian Botnet

The FBI operation targets a piece of sophisticated malware linked to the same Russian hacking group that hit the Democratic National Committee in 2016.

KEVIN POULSEN 05.23.18 6:25 PM ET

EXCLUSIVE

PHOTO ILLUSTRATION BY ELIZABETH BROCKWAY/THE DAILY BEAST

FBI agents armed with a court order have seized control of a key server in the Kremlin's global botnet of 500,000 hacked routers, The Daily Beast has learned. The move positions the bureau to build a comprehensive list of victims of the attack, and short-circuits Moscow's ability to reinfect its targets.

The FBI counter-operation goes after "VPN Filter," a piece of sophisticated malware linked to the same Russian hacking group, known as Fancy Bear, that breached the Democratic National Committee and the Hillary Clinton campaign during the 2016 election. On Wednesday security researchers at Cisco and Symantec separately provided new details on the malware, which has turned up in 54 countries including the United States.

VPN Filter uses known vulnerabilities to infect home office routers made by Linksys, MikroTik, NETGEAR, and TP-Link. Once in place, the malware reports back to a command-and-control infrastructure that can install purpose-built plug-ins, according to the researchers. One plug-in lets the hackers eavesdrop on the victim's Internet traffic to steal website credentials; another targets a protocol used in industrial control networks, such as those in the electric grid. A third lets the attacker cripple any or all of the infected devices at will.

The FBI has been investigating the botnet since at least August, according to court records, when agents in Pittsburgh interviewed a local resident whose home router had been infected with the Russian malware. "She voluntarily relinquished her router to the agents," wrote FBI agent Michael McKeown, in an affidavit filed in federal court. "In addition, the victim allowed the FBI to utilize a network tap on her home network that allowed the FBI to observe the network traffic leaving the home router."

That allowed the bureau to identify a key weakness in the malware. If a victim reboots an infected router, the malicious plugins all disappear, and only the core malware code survives. That code is programmed to connect over the Internet to a command-and-control infrastructure set up by the hackers. First it checks for particular images hosted on Photobucket.com that held hidden information in the metadata. If it can't find

> **“One plug-in lets the hackers eavesdrop on the victim’s Internet traffic; another targets a protocol used in the electric grid. A third lets the attacker cripple any or all of the infected devices at will.”**

On Tuesday, FBI agents in Pittsburg asked federal Magistrate Judge Lisa Pupo Lenihan in Pittsburgh for an order directing the domain registration firm Verisign to hand the ToKnowAll[.]com address over to the FBI, in order to “further the investigation, disrupt the ongoing criminal activity involving the establishment and use of the botnet, and assist in the remediation efforts,” according to court records. Lenihan agreed, and on Wednesday the bureau took control of the domain.

The move effectively kills the malware’s ability to reactivate following a reboot, said Vikram Thakur, technical director at Symantec, who confirmed to the Daily Beast that the domain was taken over by law enforcement on Wednesday, but didn’t name the FBI. “The payload itself is non-persistent and will not survive if the router is restarted,” Thakur added. “That payload will vanish.”

RELATED IN TECH

Russian Troll Farm Hacked Teen Girls to Attack America

Exclusive: U.S. Government Can’t Get Rid of Russian Software

Google Just Made Things a Lot Easier for Censors

In other words, average consumers have the ability to stop Russia’s latest cyber attack by rebooting their routers, which will now reach out to the FBI instead of Russian intelligence. According to the court filings, the FBI is collecting the Internet IP addresses of every compromised router that phones home to the address, so agents can use the information to clean up the global infection.

“One of the things they can do is keep track of who is currently infected and who is the victim now and pass that information to the local ISPs,” said Thakur. “Some of the ISPs have the ability to remotely restart the router. The others might even send out letters to the home users urging them to restart their devices.”

The court order only lets the FBI monitor metadata like the victim’s IP address, not content. As a technical matter, Thakur said there’s no danger of the malware sending the FBI a victim’s browser history or other sensitive data. “The threat capability is purely to ask for additional payloads,” he said. “There is no data that is leaked from these routers to the domain that is now controlled by an agency.”