The Virgin Islands Consortium

FBI Urging Residents To Reboot Routers To Stop Russian-Linked Malware

Technology / **Published On May 31, 2018 11:25 AM /**

Staff May 31, 2018

The F.B.I. has made an urgent request to anybody with internet routers, asking Americans both on the mainland and in U.S. territories to turn them off and back on in an effort to thwart a sophisticated malware system linked to Russia that has infected hundreds of thousands of internet routers.

The bureau announced on Friday that the malware is capable of disabling devices, blocking web traffic and collecting information that passes through home and office routers.

Router owners were advised to disable remote management settings on devices and secure with strong passwords and encryption when enabled. Network devices should be upgraded to the latest available versions of firmware.

The F.B.I. said the size and scope of the infrastructure impacted by malware is significant. It targets routers produced by several manufacturers and network-attached storage devices by at least one manufacturer. The initial infection vector for this malware is currently unknown, according to the bureau.

The U.S. Department of Justice said last week that hundreds of thousands of routers were already under the control of the Sofacy Group, which is also known as A.P.T. 28 and Fancy Bear and believed to be directed by Russia's military intelligence agency, which hacked the Democratic National Committee ahead of the 2016 presidential election, according to American and European intelligence agencies.

"The FBI will not allow malicious cyber actors, regardless of whether they are state-sponsored, to operate freely," said FBI Special Agent in Charge Bob Johnson. "These hackers are exploiting vulnerabilities and putting every American's privacy and network security at risk. Although there is still much to be learned about how this particular threat initially compromises infected routers and other devices, we encourage citizens and businesses to keep their network equipment updated and to change default passwords."

An analysis by Talos, the threat intelligence division for the tech giant Cisco, estimated that at least 500,000 routers in at least 54 countries had been infected by the malware, which the F.B.I. and cybersecurity researchers are calling VPNFilter, according to The New York Times. Among the affected networking equipment it found during its research were devices from manufacturers including Linksys, MikroTik, Netgear and TP-Link.

The Times said the analysis by Talos noted significant similarities between VPNFilter's computer code and "versions of the BlackEnergy malware -- which was responsible for multiple large-scale attacks that targeted devices in Ukraine."