CyberAlert

June 4, 2018

Cyber Alert – Consider Resetting (or, at a minimum, Rebooting) Your Routers to Disable Latest Malware

Risk Management Question: How can law firms and businesses protect against the latest Russian-developed malware threat affecting more than 500,000 routers?

The Issue: Malware allegedly developed by a Russian state-sponsored hacking group has infected over 500,000 routers according to the FBI and other intelligence reports.

The malware, called VPNFilter, allows hackers to collect personal information such as passwords and log-in information. In addition, the malware can wipe the infected device's firmware with a single click. The device and your network connection then are rendered useless. The malware works in 3 stages. Stage 1 loads the malware; Stage 2 allows hackers to execute commands and steal data, and Stage 3 involves the installation of plugins that permit the malware to perform additional nefarious tasks.

The FBI has seized control of the domain the hackers had planned to use to provide instructions to the infected routers, ToKnowAll[.]com, and urged users to reboot routers to help diffuse the threat. Rebooting a router will remove Stage 2 and Stage 3 components of VPNFilter if it was infected, however Stage 1, the malware itself will remain after a reboot.

While there is a published list of routers known to be infected, there is no guarantee that those on the list are the only infected ones, and there is no way to tell if a router is infected.

Risk Management Solution: Law firms and businesses should consider resetting (or at a minimum rebooting) their network routers in light of the FBI alert. The only way to fully remove the malware from an infected router is to reset it to its original settings. You can find the steps to do so in this article: https://is.gd/aUhDOE.

It is also a wise practice to stay as current as possible on software, firmware and other applications used by your Firm, as newer versions typically will close vulnerabilities found in older versions. And when you install a newer version, don't forget to remove the older version which can still be exploited if it is replaced but not removed from your system.


Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com


Anthony E. Davis
212-471-1100
adavis@hinshawlaw.com


Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com


Lauren N. Kus
312-704-3000
lkus@hinshawlaw.com