THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

May 2022

Clueless Hackers Spent Months inside a Network and Nobody Noticed - but then a Ransomware Gang Turned Up

Danny Palmer | ZDNet | April 13, 2022

A series of poor cybersecurity decisions meant the victim didn't notice intruders on their network - until more sophisticated attackers arrived. Novice hackers who didn't know what they were doing spent months inside a government agency network without being detected – before higher-skilled attackers came in after them and launched a ransomware attack.

Analysis of the incident at an unspecified US regional government agency by cybersecurity researchers at Sophos found that the amateur intruders left plenty of indicators they were in the network. Yet despite a lack of subtly and leaving a trail behind, they weren't detected because what Sophos researchers describe as "strategic choices" made by the IT team that made life easy for them.

To read the full article, use link below:
https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/clueless-hackers-spent-months-inside-a-network-and-nobody-noticed-then-a-ransomware-gang-took-over/#ftag=CAD-00-10aag7e

Russia’s most cutthroat hackers infect network devices with new botnet malware

Dan Goodin | ARS Technica | February 23, 2022

Hackers for one of Russia’s most elite and brazen spy agencies have infected home and small-office network devices around the world with a previously unseen malware that turns the devices into attack platforms that can steal confidential data and target other networks.

Cyclops Blink, as the advanced malware has been dubbed, has infected about 1 percent of network firewall devices made by network device manufacturer WatchGuard, the company said on Wednesday. The malware is able to abuse a legitimate firmware update mechanism found in infected devices in a way that gives it persistence, meaning the malware survives reboots.

Like VPNFilter, but Stealthier

Cyclops Blink has been circulating for almost three years and replaces VPNFilter, the malware that in 2018 researchers found infecting about 500,000 home and small office routers. VPNFilter contained a veritable Swiss Army knife that allowed hackers to steal or manipulate traffic and to monitor some SCADA protocols used by industrial control systems. The US Department of Justice linked the hacks to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation, typically abbreviated as the GRU.

To read the full article use link below:
https://arstechnica-com.cdn.ampproject.org/c/s/arstechnica.com/information-technology/2022/02/russias-most-cut-throat-hackers-infect-network-devices-with-new-botnet-malware/?amp=1

State Hackers' New Malware Helped Them Stay Undetected for 250 Days

Bill Toulas | BleepingComputer | February 3, 2022

A state-backed Chinese APT actor tracked as 'Antlion' has been using a new custom backdoor called 'xPack' against financial organizations and manufacturing companies.

The malware has been used in a campaign against targets in Taiwan that researchers believe spanned for more than 18 months, between 2020 and 2021, allowing the adversaries to run stealthy cyber-espionage operations.

To read the full article use link below:

https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/state-hackers-new-malware-helped-them-stay-undetected-for-250-days/amp/

OFFICE OF RESEARCH SECURITY STAFF

DENISE SPILLER
Security Administrator
824-6444, denise.spiller@uah.edu

JANINE WILSON
Associate Security Administrator
824-3025, janine.wilson@uah.edu

APRIL MCMEANS
Assistant Security Administrator
824-6048, april.mcmeans@uah.edu

CAITLYN SCHOENIG
Program Coordinator
824-4717, caitlyn.schoenig@uah.edu

RYAN WILKINSON
Student Specialist II
824-4818, ryan.wilkinson@uah.edu

MADILYN GOLEMBECK
Student Specialist II
824-4818, meg0025@uah.edu