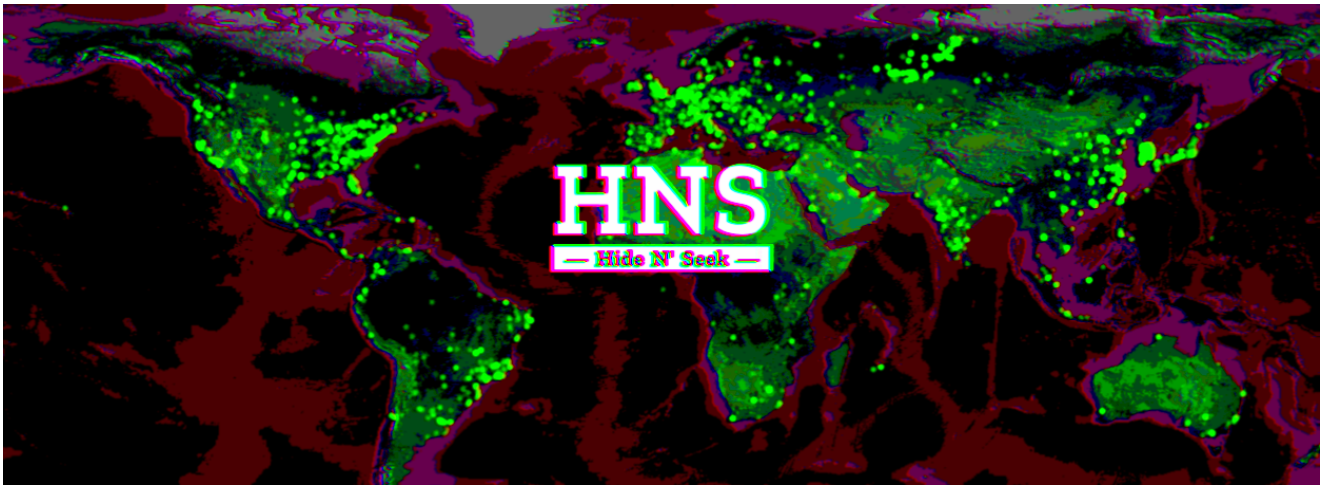
"Hide and Seek" Becomes First IoT Botnet Capable of Surviving Device Reboots

bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/

Catalin Cimpanu

By
Catalin Cimpanu

- May 8, 2018
- 05:20 PM
- 0



Security researchers have discovered the first IoT botnet malware strain that can survive device reboots and remain on infected devices after the initial compromise.

This is a major game-changing moment in the realm of IoT and router malware. Until today, equipment owners could always remove IoT malware from their smart devices, modems, and routers by resetting the device.

The reset operation flushed the device's flash memory, where the device would keep all its working data, including IoT malware strains.

"Hide and Seek" malware copies itself to /etc/init.d/

But today, Bitdefender researchers announced they found an IoT malware strain that under certain circumstances copies itself to /etc/init.d/, a folder that houses daemon scripts on Linux-based operating systems —like the ones on routers and IoT devices.

By placing itself in this menu, the device's OS will automatically start the malware's process after the next reboot.

The malware strain that achieved something that even the Mirai strain couldn't is called Hide and Seek (HNS) —also spelled Hide 'N Seek.

HNS botnet has evolved considerably in the past few months

Bitdefender experts first spotted the HNS malware and its adjacent botnet in early January, this year, and the botnet grew to around 32,000 bots by the end of the same month. Experts say HNS has infected 90,000 unique devices from the time of discovery until today.

Crooks used two exploits to create their initial botnet, which was unique from other IoT botnets active today because it used a custom P2P protocol to control infected systems.

Now, experts have found new HNS versions that have added support not only for two other exploits [1, 2] but also for brute-force operations.

What this means is that HNS infected devices will scan for other devices that have an exposed Telnet port and attempt to log into that device using a list of preset credentials.

Researchers say that HNS authors have also had time to fine-tune this brute-forcing scheme, as the malware can identify at least two types of devices and attempt to log into those systems using their factory default credentials, instead of blindly guessing passwords.

Furthermore, the HNS codebase also received updates, and the bot now has ten different binaries for ten different device architectures.

Not all HNS bots are boot persistent

But HNS is not capable of gaining boot permission on all infected devices. According to Bitdefender senior e-threat analyst Bogdan Botezatu, "in order to achieve persistence, the infection must take place via Telnet, as root privileges are required to copy the binary to the init.d directory."

The security expert also adds that the HNS botnet is still a work-in-progress, and the malware still doesn't support launching DDoS attacks.

Nonetheless, the functions to steal data and execute code on infected devices are still there, which means the botnet supports a plugin/module system and could be expanded at any point with any type of malicious code.

Related Articles:

Microsoft detects massive surge in Linux XorDDoS malware activity

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Emotet botnet switches to 64-bit modules, increases activity

New stealthy BotenaGo malware variant targets DVR devices

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.