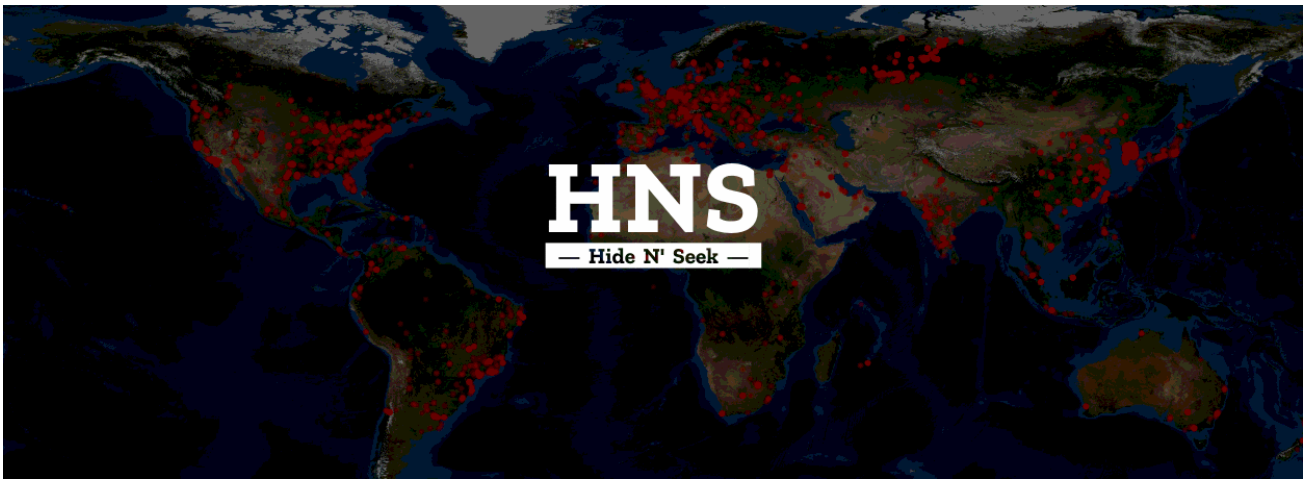
New HNS IoT Botnet Has Already Amassed 14K Bots

bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/

Catalin Cimpanu

By
Catalin Cimpanu

- January 24, 2018
- 12:22 PM
- 1



A new botnet is growing around the world, feeding off unsecured IoT devices, mainly IP cameras, and getting ready to do some harm.

Discovered by security researchers from Bitdefender, the new botnet is called Hide 'N Seek (HNS), and according to experts, the botnet first appeared on January 10, died off for a few days, and came back strong over the weekend, on January 20.

In all this time, the botnet grew from an initial list of 12 compromised devices to over 14,000 bots, as of writing.

Not Mirai related

Unlike all the Internet of Things (IoT) botnets that have appeared in recent weeks, HNS is not another modification of the Mirai IoT malware source code that was leaked online last year.

In fact, according to Bogdan Botezatu, Bitdefender senior e-threat analyst, the HNS botnet is more similar to Hajime rather than Mirai.

"It is the second known IoT botnet to date, after the notorious Hajime botnet, that has a decentralized, peer-to-peer architecture," Botezatu says. "However, if in the case of Hajime, the P2P functionality was based on the BitTorrent protocol, here we have a custom-built P2P communication mechanism."

According to an analysis Botezatu authored today, each bot contains a list of IPs of other infected bots, a list that can be updated in real-time, as the botnet grows and bots are lost or gained.

HNS bots relay instructions and commands from one another, similar to the basics of the P2P protocol. Botezatu says an HNS bot can receive and execute several types of commands, such as "data exfiltration, code execution and interference with a device's operation."

No DDoS function (yet)

Surprisingly, Bitdefender experts did not find a DDoS function, meaning the botnet is intended to be deployed as a proxy network, similar to how most IoT botnets have been weaponized in the past year after DDoS functions drew too much attention and led to the downfall of many aggressive botnets.

The botnet spreads via dictionary brute-force attacks against devices with open Telnet ports. Just like its unique P2P bot management protocol, this spreading mechanism is also heavily customized. Botezatu explains below:

The bot features a worm-like spreading mechanism that randomly generates a list of IP addresses to get potential targets. It then initiates a raw socket SYN connection to each host in the list and continues communication with those that answer the request on specific destination ports (23 2323, 80, 8080). Once the connection has been established, the bot looks for a specific banner ("buildroot login:") presented by the victim. If it gets this login banner, it attempts to log in with a set of predefined credentials. If that fails, the botnet attempts a dictionary attack using a hardcoded list.

Once a session is established with a new victim, the sample will run through a "state machine" to properly identify the target device and select the most suitable compromise method. For example, if the victim has the same LAN as the bot, the bot sets up TFTP server to allow the victim to download the sample from the bot. If the victim is located on the internet, the bot will attempt a specific remote payload delivery method to get the victim to download and run the malware sample. These exploitation techniques are preconfigured and are located in a memory location that is digitally signed to prevent tampering. This list can be updated remotely and propagated among infected hosts.
The good news is that just like all IoT malware, HNS cannot establish persistence on infected devices, meaning the malware is automatically removed with every device reboot.

This makes managing the HNS botnet a 24-hour job, with the botnet needing constant supervision from its creator in order to ensure the botnet continues to add new bots before the old ones die off.

HNS still under development

In addition, because it's a new arrival on the IoT malware scene, HNS is also in a state of constant change, as its operator(s) explores new spreading and bot management techniques.

As many of these "new" botnets have had a tendency to disappear after a few weeks, let's hope HNS' author gets bored and abandons his "experiment."

A 14K botnet is nothing to ignore. If we learned anything from the ProxyM botnet is that you don't need tens of thousands of infected devices to run a profitable botnet. Four-five thousands are enough.

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

- Botnet
- IoT
- Malware

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.

- Previous Article
- Next Article

Comments

C0bra - 4 years ago

-
-

14K bots in 2 weeks. Wow. I really hope he gets bored indeed.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: