# HNS Evolves From IoT to Cross-Platform Botnet

Catalin Cimpanu

By
Catalin Cimpanu

- July 6, 2018
- 10:37 AM
- 0

A botnet discovered at the start of the year and named Hide 'N Seek (HNS) has expanded from infecting Internet of Things (IoT) devices and is now also targeting cross-platform database solutions as well.

This is an important development in the botnet's evolution, which also passed a significant milestone in May when it became the first IoT malware that was capable of surviving device reboots.

## HNS now targets more devices

Now, the Netlab research team at Qihoo 360 says that HNS has expanded beyond the scope of routers and DVRs and is now also targeting database applications running on server operating systems.

According to Netlab researchers, the botnet is now capable of infecting the following types of devices, with the following types of exploits:

1. TPLink-Routers RCE
2. Netgear RCE
3. (new) AVTECH RCE

4. (new) CISCO Linksys Router RCE
5. (new) JAW/1.0 RCE
6. (new) OrientDB RCE
7. (new) CouchDB RCE

As a side-effect for adding more payloads, HNS is also noisier now, as it needs to scan more ports to find new hosts to infect. Experts say they've seen HNS bots initiating scans on ports:

| | |
|---|---|
| **23** | Telnet |
| **80** | HTTP Web Service |
| **2480** | OrientDB |
| **5984** | CouchDB |
| **8080** | HTTP Web Service |

... but also **random ports**

But HNS was easy to spot anyway because it's only the second major IoT botnet besides Hajime known to use a P2P structure, so security researchers would have an easy time identifying it regardless.

## HNS testing coinminer payload

HNS is not the first botnet to target OrientDB servers, which have become quite the favorite among various botnets. For example, DDG, a botnet discovered last year, which is still alive today, has targeted OrientDB servers in the past with cryptocurrency-mining malware.

In fact, it appears that HNS operators might have learned something from the DDG crew because Netlab says HNS has also started dropping a coinminer payload on some of the infected systems.

Fortunately, for the time being, it appears that these deployments have all failed, as the additional coinminer payload failed to start and generate funds for the HNS operators.

But if they manage to get it up and running, they'll be in for some profits, as the DDG gang collected well over $1 million from their coinmining last year.

*The Netlab team has published an in-depth analysis of the changes in HNS compared to its previous variant spotted back in January.*

### Related Articles:

New cryptomining malware builds an army of Windows, Linux bots

Microsoft detects massive surge in Linux XorDDoS malware activity

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

Popular NFT marketplace Rarible targeted by scammers and malware

Emotet botnet switches to 64-bit modules, increases activity

- Botnet
- Coinminer
- CryptoCurrency
- 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

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: