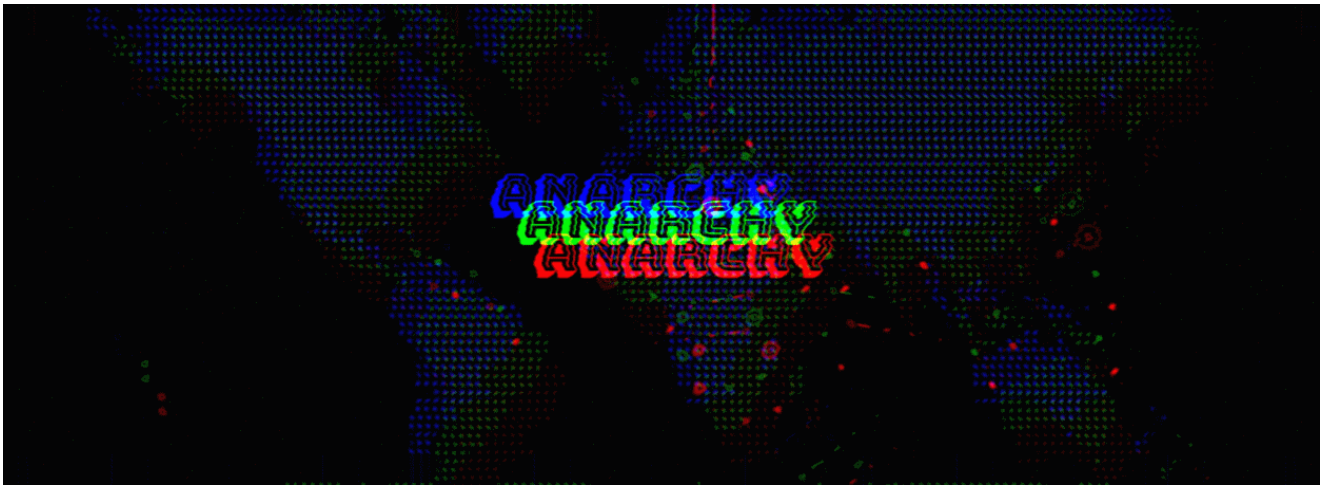
Router Crapfest: Malware Author Builds 18,000-Strong Botnet in a Day

bleepingcomputer.com/news/security/router-crapfest-malware-author-builds-18-000-strong-botnet-in-a-day/

Catalin Cimpanu

By
Catalin Cimpanu

- July 19, 2018
- 07:33 AM
- 0



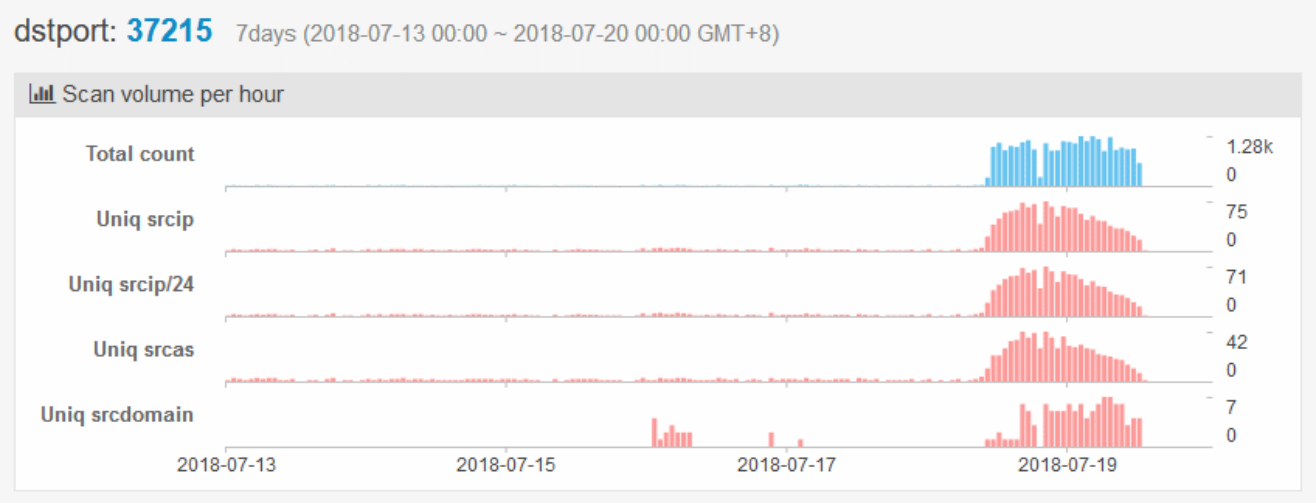
A malware author has built a huge botnet comprised of over 18,000 routers in the span of only one day.

This new botnet has been spotted yesterday by security researchers from NewSky Security, and their findings have been confirmed today by Qihoo 360 Netlab, Rapid7, and Greynoise.

Botnet built with one exploit only

The botnet has been built by exploiting a vulnerability in Huawei HG532 routers, tracked as CVE-2017-17215.

Scans for this vulnerability, which can be exploited via port 37215, started yesterday morning, July 18, according to data collected by Netlab's NetScan system.



By late in the evening, NewSky security researcher Ankit Anubhav says the botnet had already gathered 18,000 routers.

Anubhav told *Bleeping Computer* the botnet author reached out to him to brag about his actions, even sharing a list with the IP addresses of all of the botnet's victims.

Botnet author is a known threat actor

The botnet herder identified himself with the pseudonym "Anarchy." Answering inquiries from both Anubhav and Bleeping Computer, Anarchy did not provide a reason why he created the botnet.

But Anubhav believes Anarchy may actually be a hacker who previously identified as Wicked, which Anubhav interviewed on NewSky's blog and Fortinet featured in a report here.

Wicked/Anarchy is a well-known malware author who, in the past, has created variations of the Mirai IoT malware. These variations and their respective botnets were known as Wicked, Omni, and Owari (Sora), and had been previously used for DDoS attacks.

Botnet will also target Realtek routers

But the real problem here is not a malware author doing what he does best. The problem is the relative ease with which Anarchy built a gigantic botnet within one day.

He didn't do it with a zero-day or some vulnerability that had not been exploited before. He did so with a high-profile vulnerability that many botnets have exploited before.

CVE-2017-17215 is a well-known exploit that has been abused by at least two versions of the Satori botnet [1, 2], and many of the smaller Mirai-based offshoots. You'd think that by now users would have patched devices or ISPs would have blocked incoming connections on port 37215.

But Anarchy is not done yet. The botnet author told Anubhav that he also plans to target CVE-2014-8361, a vulnerability in Realtek routers exploitable via port 52869.

"Testing has already started for the Realtek exploit during the night," Anubhav told *Bleeping Computer* in a private conversation today. [*Update: Both Rapid7 and Greynoise are confirming that scans for Realtek have gone through the roof today*.]

It's both hilarious and sad that somebody can nowadays build a huge DDoS botnet in less than a day. This only shows the real sad state of SOHO router security.

IOCs, courtesy of NewSky Security and CERT Tunisia:

SHA-256: 61440574aafaf3c4043e763dd4ce4c628c6c92fb7d7a2603076b3f60f2813f1b [Source]

C2: hxxp://104.244.72.82 [Source]

Related Articles:

Honeypot experiment reveals what hackers want from IoT devices

New EnemyBot DDoS botnet recruits routers and IoTs into its army

Mirai malware now delivered using Spring4Shell exploits

Beastmode botnet boosts DDoS power with new router exploits

Cisco urges admins to patch IOS XR zero-day exploited in attacks

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.