Botnet of Thousands of MikroTik Routers Abused in Glupteba, TrickBot Campaigns

thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html

March 23, 2022

Vulnerable routers from MikroTik have been misused to form what cybersecurity researchers have called one of the largest botnet-as-a-service cybercrime operations seen in recent years.

According to a new piece of research published by Avast, a cryptocurrency mining campaign leveraging the new-disrupted Glupteba botnet as well as the infamous TrickBot malware were all distributed using the same command-and-control (C2) server.

"The C2 server serves as a botnet-as-a-service controlling nearly 230,000 vulnerable MikroTik routers," Avast's senior malware researcher, Martin Hron, said in a write-up, potentially linking it to what's now called the Mēris botnet.

The botnet is known to exploit a known vulnerability in the Winbox component of MikroTik routers (CVE-2018-14847), enabling the attackers to gain unauthenticated, remote administrative access to any affected device. Parts of the Mēris botnet were sinkholed in late September 2021.

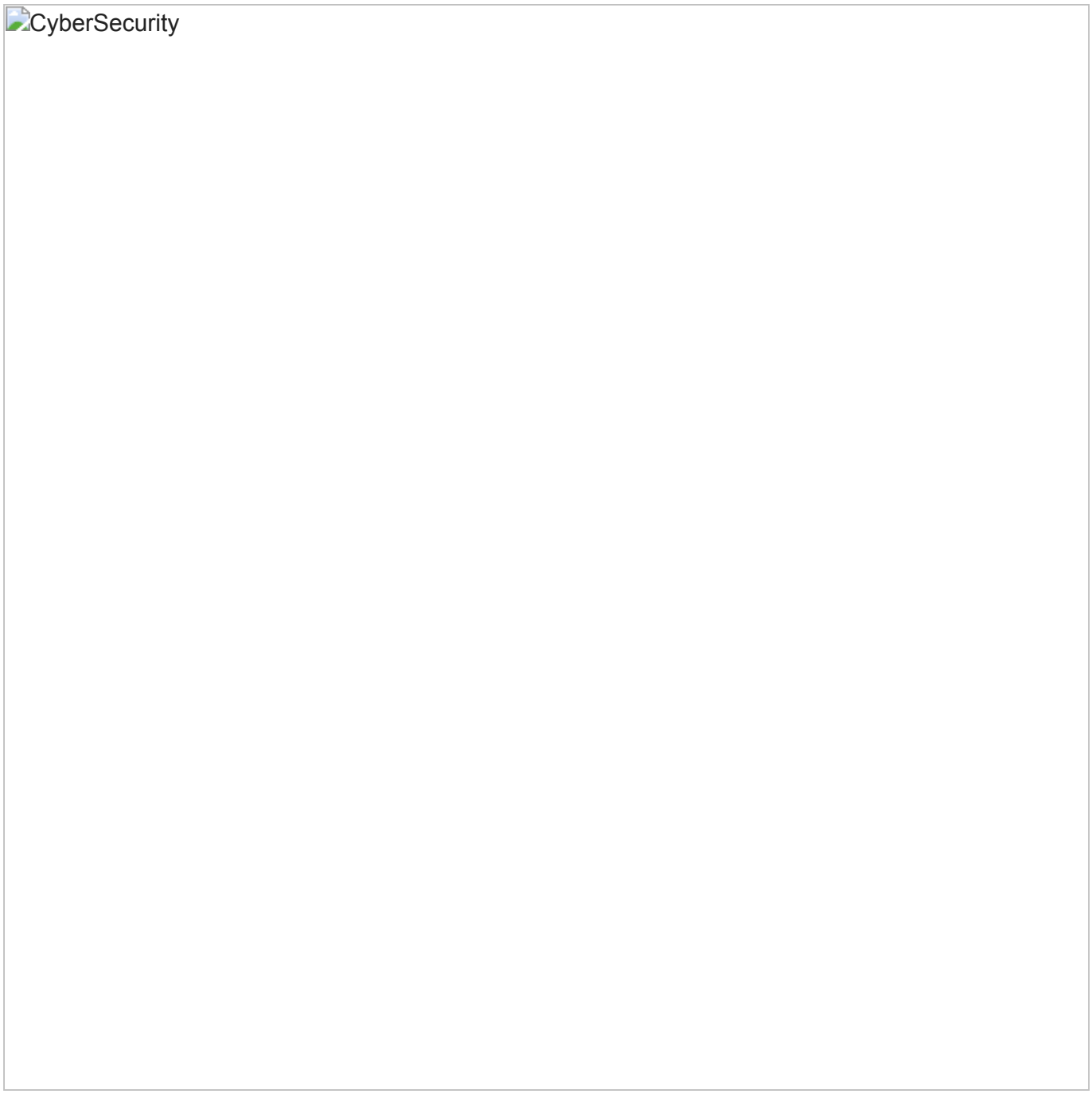
"The CVE-2018-14847 vulnerability, which was publicized in 2018, and for which MikroTik issued a fix for, allowed the cybercriminals behind this botnet to enslave all of these routers, and to presumably rent them out as a service," Hron said.

In attack chain observed by Avast in July 2021, vulnerable MikroTik routers were targeted to retrieve the first-stage payload from a domain named bestony[.]club, which was then used to fetch additional scripts from a second domain "globalmoby[.]xyz."

Interesting enough, both the domains were linked to the same IP address: 116.202.93[.]14, leading to the discovery of seven more domains that were actively used in attacks, one of which (tik.anyget[.]ru) was used to serve Glupteba malware samples to targeted hosts.

"When requesting the URL https://tik.anyget[.]ru I was redirected to the https://routers.rip/site/login domain (which is again hidden by the Cloudflare proxy)," Hron said. "This is a control panel for the orchestration of enslaved MikroTik routers," with the page displaying a live counter of devices connected into the botnet.

But after details of the Mēris botnet entered public domain in early September 2021, the C2 server is said to have abruptly stopped serving scripts before disappearing completely.



The disclosure also coincides with a new report from Microsoft, which revealed how the TrickBot malware has weaponized MikroTik routers as proxies for command-and-control communications with the remote servers, raising the possibility that the operators may have used the same botnet-as-a-service.

In light of these attacks, it's recommended that users update their routers with the latest security patches, set up a strong router password, and disable the router's administration interface from the public side.

"It also shows, what is quite obvious for some time already, that IoT devices are being heavily targeted not just to run malware on them, which is hard to write and spread massively considering all the different architectures and OS versions, but to simply use their legal and built-in capabilities

to set them up as proxies," Hron said. "This is done to either anonymize the attacker's traces or to serve as a DDoS amplification tool."

Update: Latvian company MikroTik told The Hacker News that the number "was only true before we released the patch in [the] year 2018. After patch was released, the actual affected number of devices is closer to 20,000 units that still run the older software. Also, not all of them are actually controlled by the botnet, many of them have a strict firewall in place, even though running older software."

When reached out to Avast for comment, the cybersecurity company confirmed that the number of affected devices (~230,000) reflected the status of the botnet prior to its disruption. "However, there are still isolated routers with compromised credentials or staying unpatched on the internet," the company said in a statement.

(The headline of the article has been corrected to take into account the fact that the number of affected MikroTik routers is no longer more than 200,000 as previously stated.)

SHARE □ □ □ □ □
SHARE □