New Roboto botnet emerges targeting Linux servers running Webmin

By Written by Catalin Cimpanu, ContributorContributor Nov. 20, 2019 at 8:51 a.m. PT

Archived: 2026-04-05 16:47:34 UTC

See als

-

A cybercrime group is enslaving Linux servers running vulnerable Webmin apps into a new botnet that security researchers are currently tracking under the name of Roboto.

The botnet's appearance dates back to this summer and is linked to the disclosure of a major security flaw in a web app installed on more than 215,000 servers -- which is the perfect cannon fodder to build a botnet on top.

Back in August, the team behind Webmin, a web-based remote management app for Linux systems, disclosed and patched a vulnerability that allowed attackers to run malicious code with root privileges and take over older Webmin versions.

Because of the security flaw's easy exploitation and the vast number of vulnerable systems, attacks against Webmin installs began days after the vulnerability was disclosed.

The new Roboto botnet

In a report published today [Chinese, English], the Netlab team at Chinese cyber-security vendor Qihoo 360 said that one of those early attackers was a new botnet they are currently tracking under the name of Roboto.

For the past three months, this botnet has continued to target Webmin servers.

Per the research team, the botnet's primary focus seems to have been expansion, with the botnet growing in size, but also in code complexity.

Currently, the botnet's main feature appears to be a DDoS capability. On the other hand, while the DDoS capability is in the code, Netlab says they've never seen the botnet conduct any DDoS attacks, and the botnet operators seem to be have been primarily focused over the past months on growing the botnet in size.

According to Netlab, the DDoS feature could launch attacks via vectors such as ICMP, HTTP, TCP, and UDP. But besides DDoS attacks, the Roboto bot that's installed on hacked Linux systems (via the Webmin flaw) can also:

- Function as a reverse shell and let the attacker run shell commands on the infected host
- Collect system, process, and network info from the infected server
- Upload collected data to a remote server
- Run Linux system() commands
- Execute a file downloaded from a remote URL
- Uninstall itself

Another rare P2P botnet

But there's nothing special in the above features, as many other IoT/DDoS botnets come with similar functions -- considered basic features of any modern botnet infrastructure.

The thing that's unique to Roboto is, however, its internal structure. Bots are organized in a peer-to-peer (P2P) network, and relay commands that they receive from a central command and control (C&C) server commands from one another, rather than each bot connecting to the main C&C.

Per Netlab, most bots are zombies, relaying commands, but some are also selected to prop up the P2P network or work as scanners to search for other vulnerable Webmin systems, to expand the botnet further.


Roboto
Image: Netlab

The P2P structure is of note because P2P-based communications are rarely seen in DDoS botnets, and the only ones known to use P2P are the Hajime [1, 2, 3, 4] and Hide'N'Seek botnets.

If the Roboto operators don't shut down the botnet on their own, taking it down will be a very hard task. Efforts to take down the Hajime botnet have failed in the past, and according to a source, the botnet is still going strong, with 40,000 infected bots on a daily average, and sometimes peaking at 95,000.

If Roboto will ever reach that size remains to be determined, but the botnet is not larger than Hajime, according to sources.

The world's most famous and dangerous APT (state-developed) malware

---

Source: https://www.zdnet.com/article/new-roboto-botnet-emerges-targeting-linux-servers-running-webmin