

Internet routers running Tomato are under attack by notorious crime gang

advancedtomato.com

reader comments

58 with 46 posters participating

Share this story

Internet routers running the Tomato alternative firmware are under active attack by a self-propagating exploit that searches for devices using default credentials. When credentials are found and remote administration has been turned on, the exploit then makes the routers part of a botnet that's used in a host of online attacks, researchers said on Tuesday.

The Muhstik botnet came to light about two years ago when it started unleashing a string of exploits that attacked Linux servers and Internet-of-things devices. It opportunistically exploited a host of vulnerabilities, including the so-called critical Drupalgeddon2 vulnerability disclosed in early 2018 in the Drupal content management system. Muhstik has also been caught using vulnerabilities in routers that use Gigabit Passive Optical Network (GPON) or DD-WRT software. The botnet has also exploited previously patched vulnerabilities in other server applications, including the Webdav, WebLogic, Webuzo, and WordPress.

On Tuesday, researchers from Palo Alto Networks said they

recently detected Muhstik targeting Internet routers running Tomato, an open-source package that serves as an alternative to firmware that ships by default with routers running Broadcom chips. The ability to work with virtual private networks and provide advanced quality of service control make Tomato popular with end users and in some cases router sellers.

The exploits use already infected devices to scan the Internet for Tomato routers and, when found, to check if they use the default username and password of “admin:admin” or “root:admin” for remote administration. Here’s what the scanning activity looks like:

The exploit causes Tomato routers that haven’t been locked down with a strong password to join an IRC server that’s used to control the botnet. Remote administration is turned off by default in Tomato and DD-WRT, so exploits require this setting to be changed. The infection also causes the routers to scan the Internet for servers or devices running WordPress, Webuzo, or WebLogic packages that are vulnerable. The image below shows the execution flow of the new variant as it combines various modules that scan the Internet for vulnerable servers:

Attackers use the botnet to infect targets with multiple malicious payloads, including cryptocurrency miners and software for performing distributed denial-of-service attacks on other domains. Muhstik relies on multiple command-and-control domains and IP addresses, presumably for redundancy in the event one gets taken down. The Muhstik name comes from a keyword that pops up in the exploit code.

“The new Muhstik botnet variant demonstrates that IoT botnet keeps expanding the botnet size by adding new scanners and exploits to harvest new IoT devices,” Palo Alto Networks researchers Cong Zheng, Asher Davila, and Yang Ji wrote in a post titled Muhstik Botnet Attacks Tomato Routers to Harvest New IoT Devices. “Botnet developers are increasingly compromising IoT devices installed with the open source firmware, which often lack the security updates and maintenance patches necessary to keep devices safeguarded. End users should be cautious when installing open source firmware and must follow the security guidelines in the firmware manual.”

People looking for signs that their router has been infected should check logs for access to the following IP addresses or domains:

46.149.233[.]35
68.66.253[.]100
185.61.149[.]22
hxxp://y.fd6fq54s6df541q23sdxfg[.]eu/nvr
hxxp://159.89.156[.]190/.y/pty1
hxxp://159.89.156[.]190/.y/pty3
hxxp://159.89.156[.]190/.y/pty5
hxxp://159.89.156[.]190/.y/pty6
s.shadow.mods[.]net

Tuesday's blog post also provides the names and hash digests for seven files used in the router compromises. Although Muhstik has been known to exploit firmware vulnerabilities in GPON and DD-WRT, there's no indication the new variants are using any flaws in Tomato. That suggests that weak passwords are the sole means the botnet has for taking control of routers. People should make sure they have updated the default credentials with a strong password.

Post updated to note remote administration is turned off by default.

<https://arstechnica.com/?p=1646825>