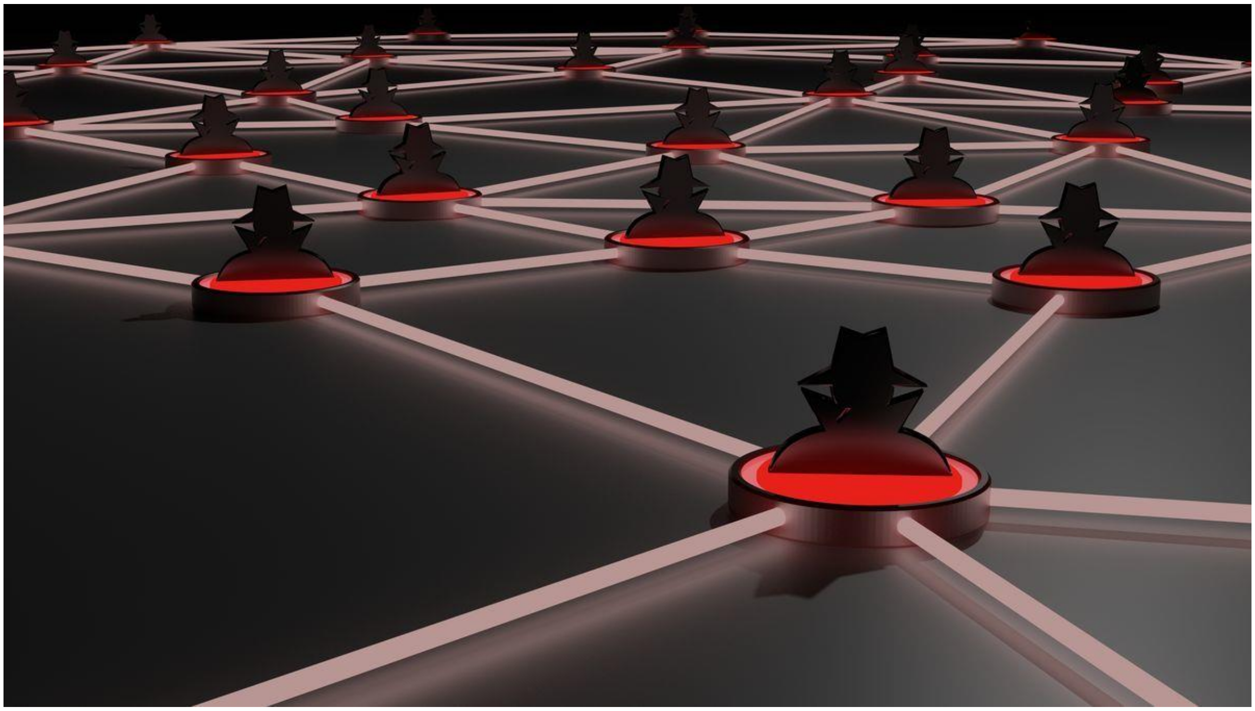
Hoaxcalls Botnet Exploits Symantec Secure Web Gateways



The fast-moving botnet has added an exploit for an unpatched bug in an unsupported version of the security gateway.

Cyberattackers are targeting a post-authentication remote code-execution vulnerability in Symantec Secure Web Gateways as part of new Mirai and Hoaxcalls botnet attacks.

Hoaxcalls first emerged in late March, as a variant of the Gafgyt/Bashlite family; it's named after the domain used to host its malware, Hoaxcalls.pw. Two new Hoaxcalls samples showed up on the scene in April, incorporating new commands from its command-and-control (C2) server. These included the ability to proxy traffic, download updates, maintain persistence across device restarts, prevent reboots and launch a larger number of distributed denial-of-service (DDoS) attacks.

It also incorporated a new exploit for infiltrating devices – an unpatched vulnerability impacting the ZyXEL Cloud CNM SecuManager that was disclosed in March. Now, researchers at Palo Alto Networks' Unit 42 division have observed that same version of the botnet exploiting a second unpatched bug, this time in Symantec Secure Web Gateway version 5.0.2.8, which is a product that became end-of-life (EOL) in 2015 and end-of-support-life (EOSL) in 2019.

The Symantec bug was disclosed in March. Since it affects older versions of the gateway, it will remain unpatched.

“On April 24, I observed samples of the same botnet incorporating an exploit targeting the EOL’d Symantec Secure Web Gateway v5.0.2.8, with an HTTP request in the format: POST /spywall/timeConfig.php HTTP/1.1,” said Unit 42 researcher Ruchna Nigam, in a Thursday post. “Some samples reach out to a URL for a public file upload service (plexle[.]us) where the post-exploitation payload is hosted. The URL contacted for the update serves a shell script that downloads and executes binaries from attacker-controlled URLs.”

Meanwhile, Nigam also saw a Mirai variant campaign in May spreading using that same vulnerability; oddly, the malware itself lacks any DDoS capabilities, according to the researcher. As such, the binary seems to be a first-stage loader.

“Samples of this campaign surfaced early May, built on the Mirai source code, and are packed with a modified version of UPX by using a different 4-byte key with the UPX algorithm,” according to Nigam. “Another deviation from the Mirai source-code is the use of all of ten 8-byte keys that are cumulatively used for a byte-wise string encryption scheme.”

The vulnerability as mentioned is a post-authentication bug, meaning that the exploit is only effective for authenticated sessions. It’s also no longer present in the latest version of the Symantec Web Gateway, version 5.2.8, so updated devices are protected.

Researchers at Radware previously noted that Hoaxcalls operators seem very quick to weaponize newly discovered bugs, like the ZyXel vulnerability. Unit 42’s Nigam came to a similar conclusion:

“The use of the exploit in the wild surfaced only a few days after the publication of the vulnerability details, highlighting the fact that the authors of this particular botnet have been pretty active in testing the effectiveness of new exploits as and when they are made public,” according to the researcher.

Reference:

https://threatpost.com/hoaxcalls-botnet-symantec-secure-web-gateways/155806/?web_view=true