

New Echobot Botnet Variant Uses Over 50 Exploits to Propagate

By Ionut Ilascu

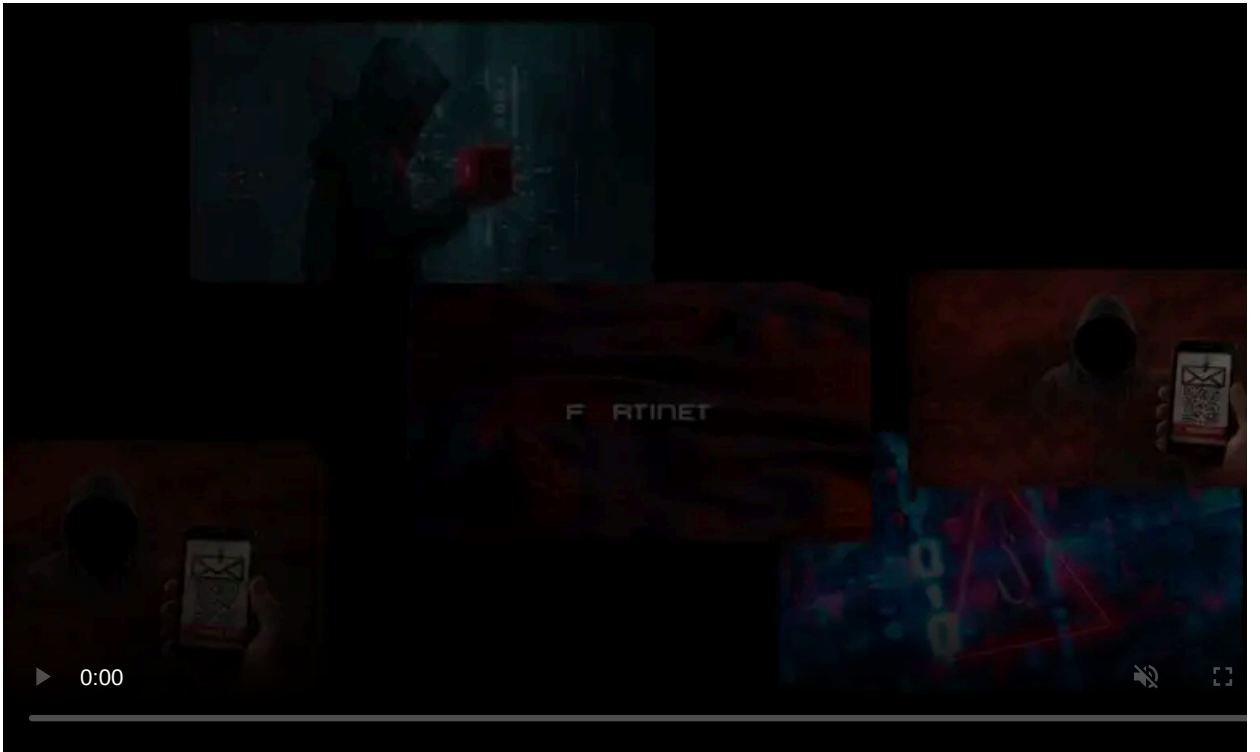
Published: 2019-08-06 · Archived: 2026-04-05 22:31:45 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

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.

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.

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.

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.

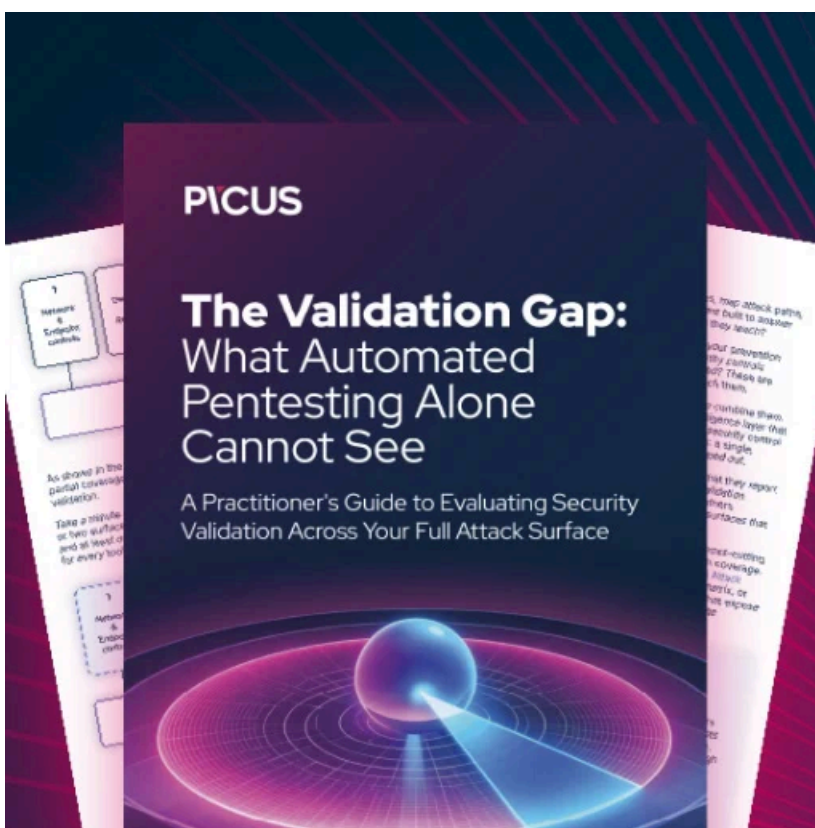
It is unclear what the author of this variant is trying to achieve, but their endeavor definitely shows how easily one can pick up malicious code and adapt it to their own needs.

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

Asustor ADM 3.1.2RHG1	Remote Code Execution
Ubiquiti 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



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/>