Botnet Echobot spreads across a wide range, specifically targeting Oracle and VMware applications

A relatively new botnet named Echobot has contributed to 26 dangerous exploits, while using exploits as a tool to spread quickly.

A relatively new botnet named Echobot has contributed to 26 dangerous exploits, while using exploits as a tool to spread quickly. According to statistics, most of the exploits codes that Echobot contributes to are for IoT devices that have not been updated with security patches. However, many enterprise applications Oracle WebLogic and VMware SD-Wan are among the targets - a point to be particularly careful about.

Echobot is based on Mirai malware, which is like hundreds of other botnets that appear after the source of a malware is made public. It was first revealed **(https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-Exloits-target-additable-iot-devices/)** earlier this month by researchers Secure security at Palo Alto Networks. Experts have found this botnet at the time of 'only' part of 18 exploits worldwide.

1. Telegram has just suffered heavy DDoS, but no significant damage was recorded

Echobot Botnet is spreading rapidly around the world

IoT devices become the main target

Popular security researcher Larry Cashdollar of Akamai's network security intelligence response group (SIRT) observed a new version of Echobot botnet, adding a new series of exploits to help it expand. spread.

"I have counted a total of 26 independent exploits that are being used to spread this botnet. Most of these are command execution vulnerabilities that are well known in other networked devices. each other, "said Larry Cashdollar.

1. Shade ransomware, the nightmare of 5 years ago is showing signs of returning

ECHOBOT	NEW ECHOBOT
ADM	ADM
ASUS	AirOS
BELKIN	ASMAX
Blackbox	ASUS
DELL	BELKIN
DREAMBOX	Blackbot
GEUTEBRUCK	DD-WRT
HOOTOO	DELL
NETGEAR	D-LINK
NUUO	DREAMBOX
ORACLE	GEUTEBRUCK
REALTEK	HOOTOO
SUPERSIGN	LINKSYS
UMOTION	NETGEAR
VERALITE	NUUO
VMWARE	ORACLE
WEPRESENT	REALTEK
WIFICAM	SEOWONINTECH
	SUPERSIGN
	UMOTION
	VERALITE
	VMWARE
	WEPRESENT
	WIFICAM
	YEALINK
	ZEROSHELL

Target of Echobot variant

The goals of the latest Echobot variant include networked storage devices (NAS), routers (routers), network video recorders (NVRs), IP cameras, IP phones and presentation systems. wireless presentation systems.

The old holes that have been around for decades have been exploited again

Larry Cashdollar and colleagues are having difficulty identifying the vulnerabilities used by this botnet, because some of them have been publicly discovered, but there are no designated tracking numbers. specific for each case.

Cashdollar's team overcame the problem by contacting MITER and thanks to the organization reallocating the vector identification number, he found the CVE symbols missing.

This effort plays an extremely useful role not only for the research of Cashdollar and his colleagues, but also for other experts when finding vulnerabilities exploited in nature because the CVE number is a system. Standard classification is used by the infosec community.

Cashdollar has also compiled a list with the errors used by the new Echobot variant as follows:

Affects	CVE
Asustor NAS appliance	CVE-2018-11510
ASUS Wireless-N300 ADSL Modem Router	CVE-2018-15887
Belkin Wemo UPnP Remote Code Execution (Crockpot)	CVE-2019-12780
Blackbox	CVE-2019-3929
Dell (Quest) KACE Command Injection	CVE-2018-11138
Open Dreambox Command Injection	CVE-2017-14135
Geutebruck Command Injection	CVE-2017-5173
Hootoo HT-05 Remote Code Execution	CVE-2018-20841
Netgear ReadyNAS Remote Command Execution	CVE-2017-18377
NUUO NVRmini devices Remote Command Execution	CVE-2018-14933
Oracle WebLogic Remote Code Execution Vulnerability	CVE-2019-2725
Realtek Miniigd UPnP SOAP Command Execution	CVE-2014-8361
LG SuperSign EZ CMS Remote Code Execution	CVE-2018-17173
Schneider Electric U.Motion Builder Remote Code Execution	CVE-2018-7841
MiCasaVerde VeraLite Remote Code Execution	CVE-2016-6255
VMware NSX SD-WAN Edge Command Injection	CVE-2018-6961
Barco wePresent WiPG-1000P Command Injection	CVE-2019-3929
Wireless IP Camera (P2P) WIFICAM	CVE-2017-18377
Ubiquity Nanostation5 (Air OS) - Remote Command Execution	CVE-2010-5330
ASMAX Ar-804gu Command Injection Vulnerability	CVE-2009-5156
DD-WRT Command Injection	CVE-2009-2765
D-Link UPnP SOAP Command Injection	CVE-2013-7471
Linksys WAG54G2 Web Management Console Injection Vulnerability	CVE-2009-5157
Linksys WAG54G2 Web Management Console Injection Vulnerability	CVE-2009-5157
Seowonintech Command Injection	CVE-2016-10760
Yealink VoIP Phone SIP-T38G - Remote Command Execution	CVE-2013-5758
ZeroShell 'cgi-bin/kerbynet' Remote Command Execution Vulnerability	CVE-2009-0545

list with vulnerabilities used by new Echobot variants

1. Microsoft warned about malicious spam campaigns using vulnerabilities in Office and Wordpad

One important aspect this researcher warns is that the author (s) of the botnet expanded the target list beyond the IoT device range, and added exploits targeting Oracle WebLogic. VMware SD-WAN server and network software, which is used to provide cloud services, private data storage centers, and SaaS-based enterprise applications - play a critical role with many organizations and businesses.

In addition, the team also noted the phenomenon of old security vulnerabilities that have been around for decades that have been exploited by this botnet, suggesting that malware authors are completely unaware. mind the age of the vulnerability, provided they still have excellent performance for devices that have not been patched.

This shows that many vulnerable systems are still being used, and most likely they become good prey for Echobot background updates not timely security patches.

1. GoldBrute botnet campaign is trying to hack 1.5 million RDP servers worldwide

Research by Larry Cashdollar and colleagues revealed more information about Echobot only using the same attack code originating from Mirai, and the most obvious difference is in the exploits that are helping it. spread quickly around the world.

Larry Cashdollar noticed that the command and control servers (C2 Server) were set for domains akumaiotsolutions [.] Pw and akuma Pw, although they were completely non-resolving to IP addresses.