Mirai Spawn Echobot Found Using Over 50 Different Exploits (CSB19-05)

SUMMARY

Echobot is one of the many botnets that were based on the Mirai botnet. Echobot is nearly identical to the Mirai malware. As part of the Mirai Botnet attack, Linux will be installed on the infected device, as well as various applications such as a Web proxy and software used to carry out DDoS attacks. Echobot carries out attacks on a wider variety of targets and has software designed to exploit a large number of vulnerabilities. Once the victim's device has been compromised, it becomes integrated into the Echobot botnet, an enormous group of infected devices that can be used in coordination to carry out many attacks.

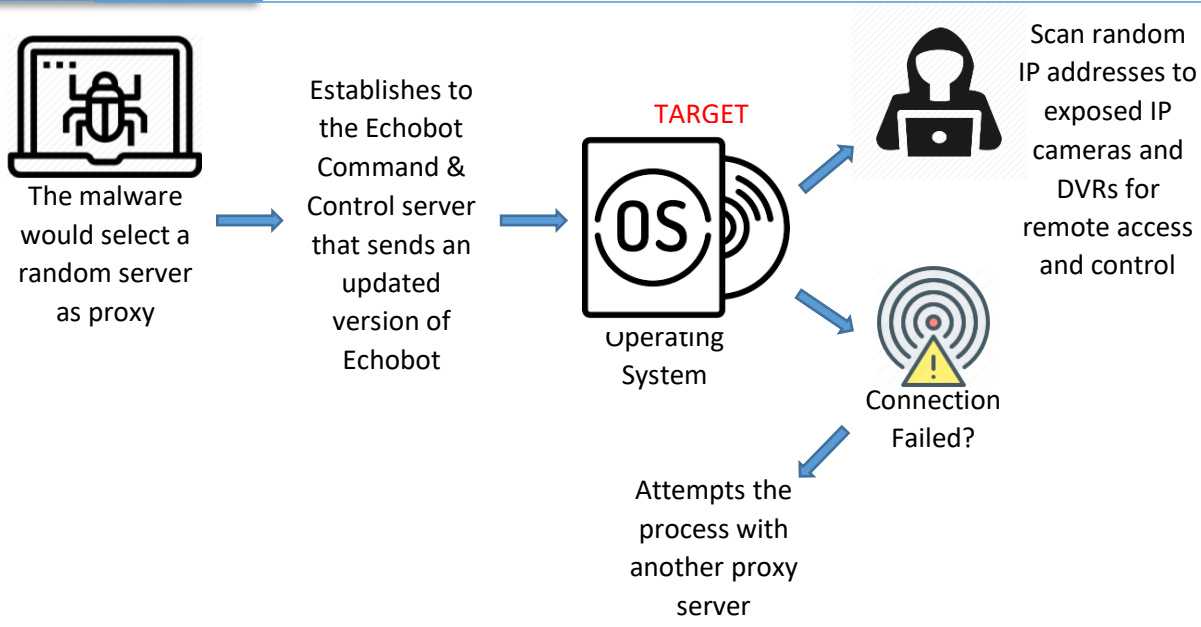
- Targeting IoT devices and enterprise apps;
- It can cause target vulnerabilities in commonly used enterprise software;
- Designed to exploit at least 26 different vulnerabilities to carry out its attack;
- Attempts to target vulnerabilities in software used in enterprise devices such as VMware NSX SD-WAN and Oracle WebLogic Server, apart from using common exploits in the Windows operating system and commonly used platforms;
- Designed to target businesses and higher-profile targets. However, home systems also are vulnerable;

Echobot added new exploits that are older and remained unpatched by the vendor.

Once a device has been compromised, it establishes a connection to the Echobot Command and Control server that sends an updated version of Echobot that is specific to the targeted system's operating environment

These botnets can be used for devastating attacks, leveraging the large number of infected devices. Some examples incorporate DDoS (Distributed Denial of Service) attacks, sending out massive quantities of spam email and money laundering operations. Computer users are advised to use strong security software, update all firmware and software, and use strong passwords, particularly on devices like routers that are commonly left unprotected relatively.

HOW IT WORKS



SECURITY RISKS

- Stealing of sensitive personal information and credentials;
- Can issue system commands, write, delete or read files or connect to databases.

MITIGATIONS

- Regularly updating devices, firmware, software and changing access credentials;
- Configuring the router's settings to deter potential intrusions;
- Disabling outdated and unused device components;
- Enabling the auto-update feature if the device allows it;
- Encrypting the connections that the devices use;
- Incorporating security tools that provide additional protection to home networks and devices connected to them; and
- Using only legitimate applications from trusted sources and stores.

REFERENCE

- https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-spawn-echobot-found-using-over-50-different-exploits;
- https://www.securityweek.com/new-mirai-variant-hides-cc-server-tor-network

LIST OF EXPLOITS USED BY MIRAI ECHOBOT:

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