ID: 830708
Sample Name: 8lsvVMbYw7.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:19:55
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Linux Analysis Report 8lsvVMbYw7.elf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Warnings 4
Runtime Messages 4
Process Tree 5
Malware Threat Intel 5
Yara Signatures 5
Initial Sample 5
Memory Dumps 6
Snort Signatures 8
Joe Sandbox Signatures 9
AV Detection 10
Networking 10
System Summary 10
Persistence and Installation Behavior 10
Hooking and other Techniques for Hiding and Protection 10
Stealing of Sensitive Information 10
Remote Access Functionality 10
Mitre Att&ck Matrix 10
Malware Configuration 11
Behavior Graph 11
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 12
Public IPs 12
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 15
General 15
Static ELF Info 15
ELF header 15
Sections 16
Program Segments 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 17
TCP Packets 17
DNS Queries 17
DNS Answers 17
System Behavior 18
Analysis Process: 8lsvVMbYw7.elf PID: 6211, Parent PID: 6129 18
General 18
File Activities 18
File Read 18
Analysis Process: 8lsvVMbYw7.elf PID: 6213, Parent PID: 6211 18
General 18
Analysis Process: sh PID: 6213, Parent PID: 6211 18
General 18
File Activities 18
File Read 18
Analysis Process: sh PID: 6215, Parent PID: 6213 18
General 18
Analysis Process: rm PID: 6215, Parent PID: 6213 18
General 19
File Activities 19
File Deleted 19

File Read 19
Analysis Process: sh PID: 6216, Parent PID: 6213 19
General 19
Analysis Process: mkdir PID: 6216, Parent PID: 6213 19
General 19
File Activities 19
File Read 19
Directory Created 19
Analysis Process: sh PID: 6217, Parent PID: 6213 19
General 19
Analysis Process: mv PID: 6217, Parent PID: 6213 19
General 19
File Activities 19
File Read 19
File Moved 19
Analysis Process: sh PID: 6218, Parent PID: 6213 20
General 20
Analysis Process: chmod PID: 6218, Parent PID: 6213 20
General 20
File Activities 20
File Read 20
Permission Modified 20
Analysis Process: 8lsvVMbYw7.elf PID: 6219, Parent PID: 6211 20
General 20
Analysis Process: 8lsvVMbYw7.elf PID: 6221, Parent PID: 6219 20
General 20
File Activities 20
File Read 20
Directory Enumerated 20
Analysis Process: 8lsvVMbYw7.elf PID: 6222, Parent PID: 6219 20
General 20

Linux Analysis Report

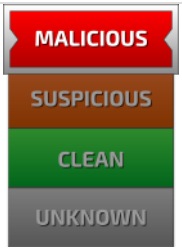
8lsvVMbYw7.elf

Overview

General Information

Sample Name:	8lsvVMbYw7.elf
Original Sample Name:	4db30b374297…
Analysis ID:	830708
MD5:	4db30b374297…
SHA1:	d4934ed96152…
SHA256:	7e4dadf93fbb7…
Tags:	32 elf mips mirai
Infos:	

Detection



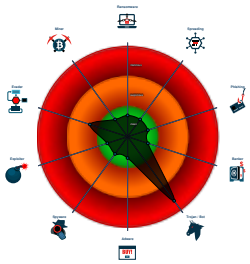
Mirai, Moobot

Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Moobot
- Snort IDS alert for network traffic
- Connects to many ports of the same…
- Uses known network protocols on n…
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…
- Uses the "uname" system call to qu…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830708
Start date and time:	2023-03-20 16:19:55 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Sample file name:	8lsvVMbYw7.elf
Original Sample Name:	4db30b3742977f4175543bcc258bba08.elf
Detection:	MAL
Classification:	mal92.troj.linELF@0/0@2/0

Warnings

Runtime Messages

Command:	/tmp/8lsvVMbYw7.elf
PID:	6211
Exit Code:	0
Exit Code Info:	

Killed:	False
Standard Output:	done.
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 8lsvVMbYw7.elf (PID: 6211, Parent: 6129, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/8lsvVMbYw7.elf
  - 8lsvVMbYw7.elf New Fork (PID: 6213, Parent: 6211)
  - sh (PID: 6213, Parent: 6211, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv /tmp/8lsvVMbYw7.elf bin/watchdog; chmod 777 bin/watchdog"
    - sh New Fork (PID: 6215, Parent: 6213)
    - rm (PID: 6215, Parent: 6213, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/watchdog
    - sh New Fork (PID: 6216, Parent: 6213)
    - mkdir (PID: 6216, Parent: 6213, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6217, Parent: 6213)
    - mv (PID: 6217, Parent: 6213, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/8lsvVMbYw7.elf bin/watchdog
    - sh New Fork (PID: 6218, Parent: 6213)
    - chmod (PID: 6218, Parent: 6213, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/watchdog
  - 8lsvVMbYw7.elf New Fork (PID: 6219, Parent: 6211)
    - 8lsvVMbYw7.elf New Fork (PID: 6221, Parent: 6219)
    - 8lsvVMbYw7.elf New Fork (PID: 6222, Parent: 6219)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	**http://** osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Name	Description	Attribution	Blogpost URLs	Link
MooBot		No Attribution	**http://** https://blog.netlab.360.com/ddos-botnet-moobot-en/https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/https://otx.alienvault.com/pulse/6075b645942d5adf9bb8949bhttps://unit42.paloaltonetworks.com/moobot-d-link-devices/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.moobot

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
8lsvVMbYw7.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
8lsvVMbYw7.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
8lsvVMbYw7.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x11834:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11848:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1185c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11870:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11884:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11898:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118ac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118d4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118fc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11910:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11924:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11938:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1194c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11960:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11974:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11988:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1199c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F

Memory Dumps

Source	Rule	Description	Author	Strings
6211.1.00007f3790400000.00007f3790414000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6211.1.00007f3790400000.00007f3790414000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6211.1.00007f3790400000.00007f3790414000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x11834:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11848:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1185c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11870:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11884:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11898:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118ac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118d4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118fc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11910:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11924:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11938:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1194c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11960:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11974:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11988:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1199c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Process Memory Space: 8lsvVMbYw7.elf PID: 6211	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x5dce:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5de2:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5df6:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e0a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e1e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e32:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e46:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e5a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e6e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e82:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5e96:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5eaa:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5ebe:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5ed2:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5ee6:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5efa:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5f0e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5f22:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5f36:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5f4a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x5f5e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 93.94.199.119

Timestamp:	192.168.2.2393.94.199.11953672372152835222 03/20/23-16:21:16.976524
SID:	2835222
Source Port:	53672
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 94.187.107.90

Timestamp:	192.168.2.2394.187.107.9039438372152835222 03/20/23-16:21:34.558345
SID:	2835222
Source Port:	39438
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 203.6.74.105

Timestamp:	192.168.2.23203.6.74.10537918372152835222 03/20/23-16:21:45.948271
SID:	2835222
Source Port:	37918
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.23 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.238.8.8.843281532023883 03/20/23-16:20:44.511900
SID:	2023883
Source Port:	43281
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response - Source IP: 156.224.24.249 - Destination IP: 192.168.2.23

Timestamp:	156.224.24.249192.168.2.2356999477962030489 03/20/23-16:21:24.722739
SID:	2030489
Source Port:	56999
Destination Port:	47796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response - Source IP: 156.224.24.249 - Destination IP: 192.168.2.23

Timestamp:	156.224.24.249192.168.2.2356999478062030489 03/20/23-16:22:44.755597
SID:	2030489
Source Port:	56999
Destination Port:	47806
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.234.43.110

Timestamp:	192.168.2.23197.234.43.11049508372152835222 03/20/23-16:22:30.124421
SID:	2835222
Source Port:	49508
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.36.73.52	
Timestamp:	192.168.2.2341.36.73.5245328372152835222 03/20/23-16:21:23.129262
SID:	2835222
Source Port:	45328
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1) - Source IP: 192.168.2.23 - Destination IP: 156.224.24.249	
Timestamp:	192.168.2.23156.224.24.24947806569992030490 03/20/23-16:21:34.964696
SID:	2030490
Source Port:	47806
Destination Port:	56999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.39.71.73	
Timestamp:	192.168.2.23197.39.71.7358096372152835222 03/20/23-16:22:16.668019
SID:	2835222
Source Port:	58096
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 86.71.8.242	
Timestamp:	192.168.2.2386.71.8.24242520372152835222 03/20/23-16:22:02.177570
SID:	2835222
Source Port:	42520
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1) - Source IP: 192.168.2.23 - Destination IP: 156.224.24.249	
Timestamp:	192.168.2.23156.224.24.24947796569992030490 03/20/23-16:20:45.109110
SID:	2030490
Source Port:	47796
Destination Port:	56999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 192.107.143.159	
Timestamp:	192.168.2.23192.107.143.159478963721528352222 03/20/23-16:22:19.853858
SID:	2835222
Source Port:	47896
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.23 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.238.8.8.846438532023883 03/20/23-16:21:34.369876
SID:	2023883
Source Port:	46438
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Sets full permissions to files and/or directories

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Yara detected Moobot

Remote Access Functionality

Yara detected Mirai

Yara detected Moobot

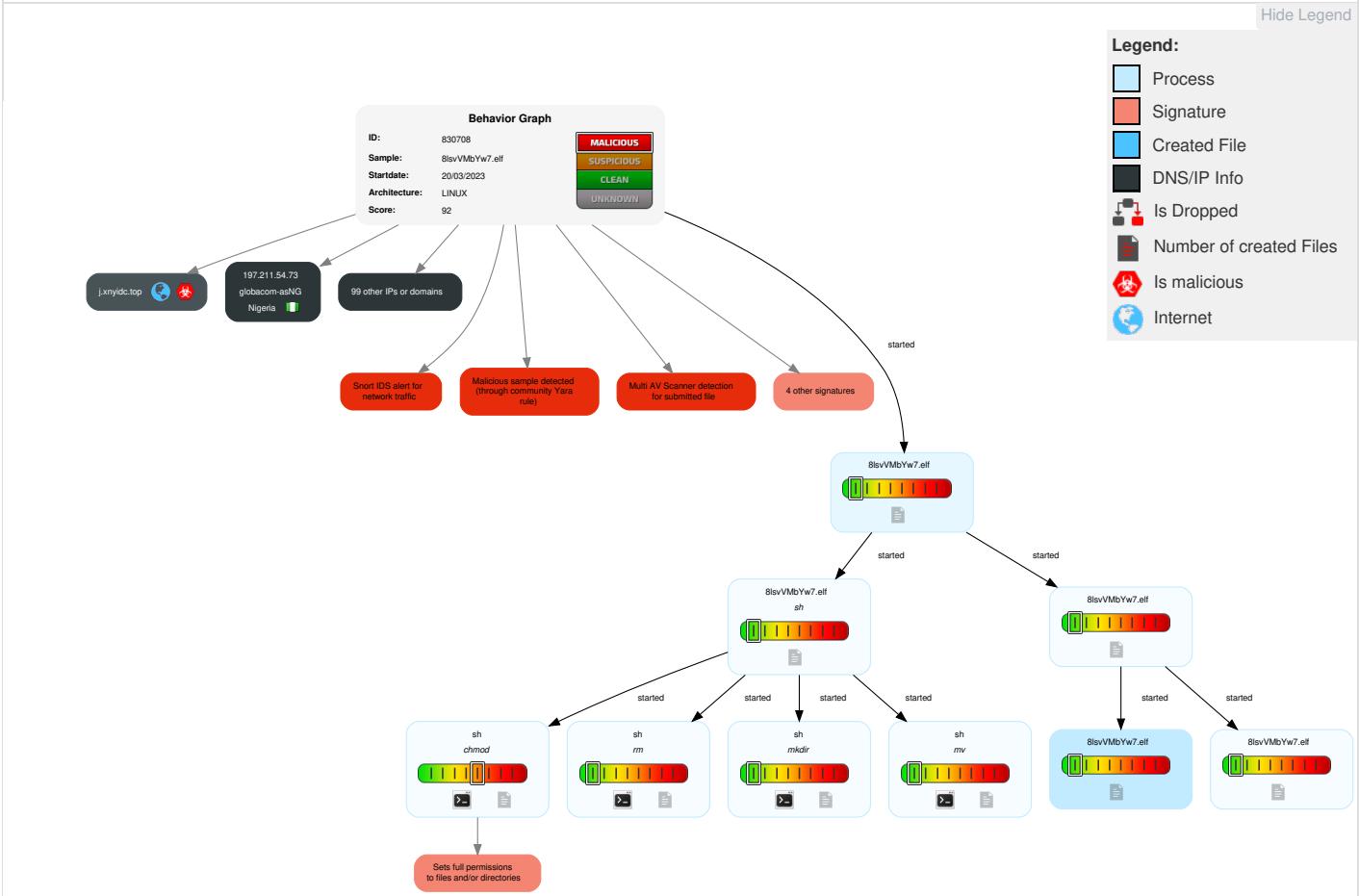
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	Path Interception	2 File and Directory Permissions Modification	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 File Deletion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
8lsvVMbYw7.elf	61%	Virustotal		Browse
8lsvVMbYw7.elf	64%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
j.xnyidc.top	13%	Virustotal		Browse

URLs

No Antivirus matches

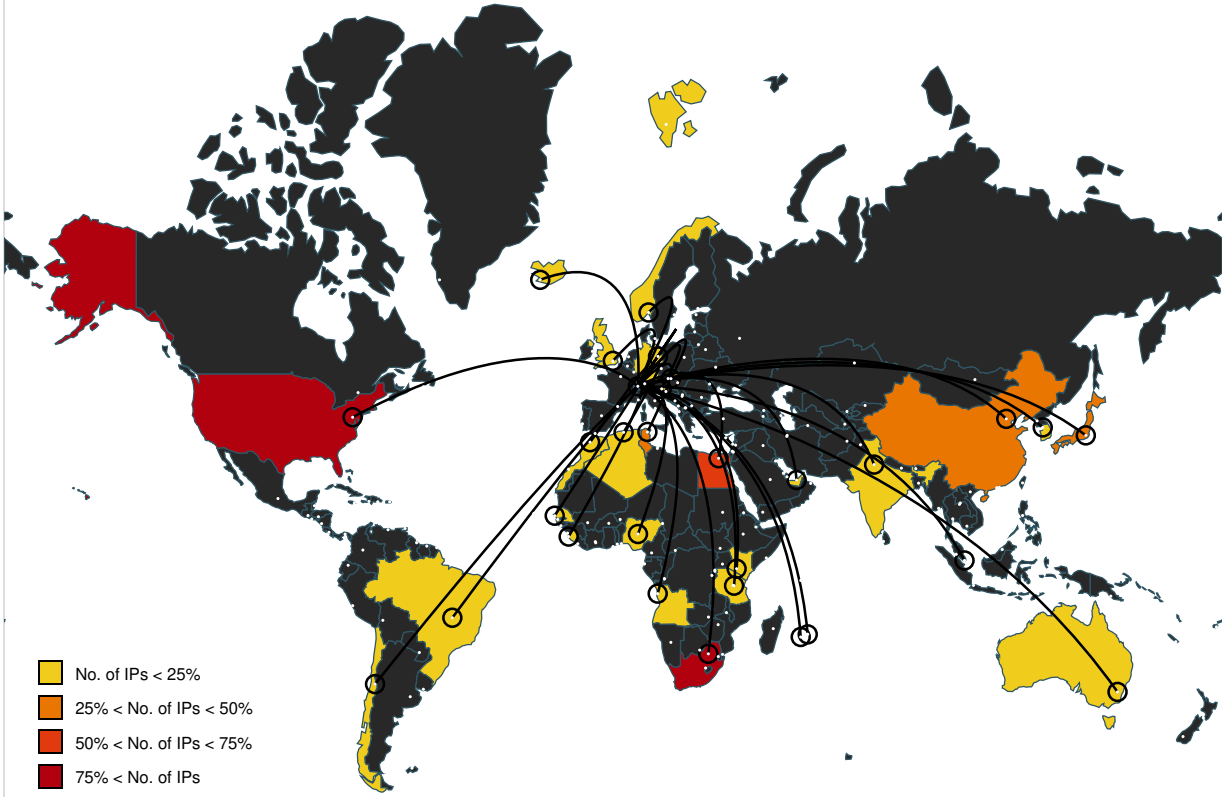
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
j.xnyidc.top	156.224.24.249	true	true	• 13%, Virustotal, Browse	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.122.249.23	unknown	South Africa		16637	MTNNS-ASZA	false
197.216.246.226	unknown	Angola		11259	ANGOLATELECOMAO	false
41.215.59.33	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
108.47.210.80	unknown	United States		5650	FRONTIER-FRTRUS	false
86.2.184.216	unknown	United Kingdom		5089	NTLGB	false
197.187.29.137	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
197.164.30.176	unknown	Egypt		24863	LINKdotNET-ASEG	false
163.159.243.10	unknown	Slovenia		15435	KABELFOONDELTAFiberNederlandNL	false
85.3.140.152	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
157.163.19.152	unknown	Germany		22192	SSHENETUS	false
157.114.152.203	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
197.215.104.9	unknown	Sierra Leone		37164	ZAIN-SL	false
41.165.220.194	unknown	South Africa		36937	Neotel-ASZA	false
41.51.170.24	unknown	South Africa		37168	CELL-CZA	false
157.155.254.125	unknown	Australia		17983	COLESMYER-AS-APColesMyerAU	false
41.213.144.200	unknown	Reunion		37002	ReunicableRE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.26.73.179	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
197.225.163.192	unknown	Mauritius		23889	MauritiusTelecomMU	false
203.117.207.148	unknown	Singapore		4657	STARHUB-INTERNETStarHubLtdSG	false
41.83.144.208	unknown	Senegal		8346	SONATEL-ASAutonomousSystemEU	false
41.76.254.8	unknown	Nigeria		37286	NG-ICT-FORUMNG	false
197.5.202.118	unknown	Tunisia		5438	ATI-TN	false
117.90.147.24	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
157.139.31.146	unknown	United States		20252	JSIWMCUS	false
70.43.200.100	unknown	United States		7029	WINDSTREAMUS	false
197.211.54.73	unknown	Nigeria		37148	globacom-asNG	false
124.245.211.133	unknown	Japan		7671	MCNETNTTSmartConnectCorporationJP	false
93.213.159.141	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
134.61.198.10	unknown	Germany		47610	RWTH-ASDE	false
107.118.129.135	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
157.175.206.68	unknown	United States		16509	AMAZON-02US	false
197.136.212.68	unknown	Kenya		36914	KENET-ASKE	false
197.240.178.142	unknown	unknown		37705	TOPNETTN	false
41.12.83.171	unknown	South Africa		29975	VODACOM-ZA	false
143.20.10.228	unknown	United States		264008	LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR	false
197.69.35.16	unknown	South Africa		16637	MTNNS-ASZA	false
197.173.143.31	unknown	South Africa		37168	CELL-CZA	false
157.215.57.56	unknown	United States		4704	SANNETRakutenMobileIncJP	false
41.224.199.212	unknown	Tunisia		37492	ORANGE-TN	false
53.174.9.169	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
157.220.249.137	unknown	United States		4704	SANNETRakutenMobileIncJP	false
144.177.101.154	unknown	Norway		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
157.37.64.93	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
96.195.150.65	unknown	United States		7922	COMCAST-7922US	false
197.12.117.173	unknown	Tunisia		37703	ATLAXTN	false
197.46.218.171	unknown	Egypt		8452	TE-ASTE-ASEG	false
106.90.178.87	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
121.166.75.153	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
197.180.156.79	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.17.21.185	unknown	Tunisia		37693	TUNISIANATN	false
157.120.215.120	unknown	Japan		9604	FSI-ASFUJISOFTINCORPORATEDJP	false
197.204.213.186	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.179.230.74	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
41.231.153.146	unknown	Tunisia		5438	ATI-TN	false
166.204.123.155	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
41.130.176.218	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.99.166.220	unknown	South Africa		3741	ISZA	false
197.165.117.160	unknown	Egypt		24863	LINKdotNET-ASEG	false
61.199.88.126	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.42.18.29	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
186.236.123.240	unknown	Brazil		53131	GBTECNOLOGIAEMONITORAMENTOEIRELIBR	false
41.121.55.46	unknown	South Africa		16637	MTNNS-ASZA	false
157.148.116.57	unknown	China		136958	UNICOM-GUANGZHOU-IDCChinaUnicomGuangdongIPnetworkCN	false
186.65.237.188	unknown	Chile		27680	TELEFONICAMOVILDECHILESACL	false
39.150.131.210	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
41.205.215.93	unknown	Morocco		36925	ASMediMA	false
68.179.215.229	unknown	United States		10430	WA-K20US	false
157.139.31.134	unknown	United States		20252	JSIWMCUS	false
151.253.220.12	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
197.73.232.47	unknown	South Africa		16637	MTNNS-ASZA	false
197.96.225.174	unknown	South Africa		3741	ISZA	false
13.59.33.208	unknown	United States		16509	AMAZON-02US	false
41.3.151.154	unknown	South Africa		29975	VODACOM-ZA	false
197.227.254.209	unknown	Mauritius		23889	MauritiusTelecomMU	false
197.239.252.138	unknown	unknown		36974	AFNET-ASCI	false
98.178.75.120	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
41.44.168.31	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.217.104.40	unknown	Nigeria		37340	SpectranetNG	false
197.222.122.211	unknown	Egypt		37069	MOBINILEG	false
41.108.245.6	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.15.56.36	unknown	South Africa		29975	VODACOM-ZA	false
157.121.53.53	unknown	United States		2514	INFOSPHERENTTPCCommunicationsIncJP	false
157.146.115.27	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
197.122.223.222	unknown	Egypt		36992	ETISALAT-MISREG	false
41.3.83.208	unknown	South Africa		29975	VODACOM-ZA	false
41.36.233.3	unknown	Egypt		8452	TE-ASTE-ASEG	false
131.124.97.114	unknown	United States		15329	UNASSIGNED	false
197.200.106.225	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.37.88.95	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
41.216.98.181	unknown	Mauritius		37006	LiquidTelecommunicationRwandaRW	false
39.147.18.97	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
197.202.209.139	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.227.53.36	unknown	Australia		4704	SANNETRakutenMobileIncJP	false
197.109.110.86	unknown	South Africa		37168	CELL-CZA	false
178.40.173.81	unknown	Slovakia (SLOVAK Republic)		6855	SK-TELEKOMSK	false
187.60.245.182	unknown	Brazil		28161	PiernetTelecomBR	false
157.157.39.30	unknown	Iceland		6677	ICENET-AS1IS	false
197.193.180.204	unknown	Egypt		36992	ETISALAT-MISREG	false
157.101.52.55	unknown	Japan		27947	TelconetSAEC	false
41.83.26.215	unknown	Senegal		8346	SONATEL-ASAutonomousSystemEU	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.442327939522003
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	8lsvVMbYw7.elf
File size:	84780
MD5:	4db30b3742977f4175543bcc258bba08
SHA1:	d4934ed96152dfae36f4b9421b5f5b602f9ed6fe
SHA256:	7e4dadf93fbb7a01b55eadacbb40ae8d5e95f5b9592e55f0fb2340d89fc78f17
SHA512:	5d7111eb62f6758cdf57839190d451713a146931e0ce63975f02de2ab51d69f0122a59b9982138a2a62893e1256622822e73b1eaa077f1d0e45a74c53f0e0935
SSDEEP:	768:2ty6IP7M/kq0INRhfuN2Eo9tl/de2YIwHKRH0I84EH6UTC7ZDYovZ73x/nL8y8QP:Rakdn2Eo3ePu5GTCRYo99Be037WQ/
TLSH:	C883A51E7E228FADF76D823147B74E25A69833C627E1D641E16CD6012E6034E641FFE8
File Content Preview:	.ELF.....@.`...4..H.....4. ...(.....@...@....6`..6`.....@..E@..E@.....+.....dt.Q.....<...'..\...!'.....<...'..8...!... ....'9... .....<...'.....!.....'9.

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	

ELF header	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x115d0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x4116f0	0x116f0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x411750	0x11750	0x1f10	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x454000	0x14000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x454008	0x14008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x454014	0x14014	0x44	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x454060	0x14060	0x3a0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x454400	0x14400	0x498	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x454898	0x14898	0x1c	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x4548c0	0x14898	0x2250	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x9c6	0x14898	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x14898	0x64	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x13660	0x13660	5.5801	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x14000	0x454000	0x454000	0x898	0x2b10	3.8882	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

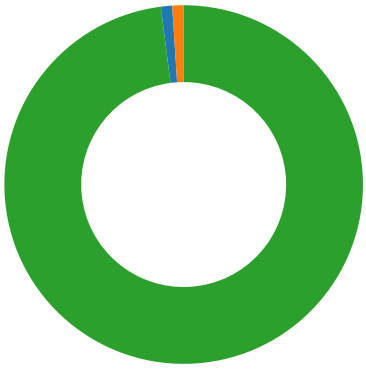
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2393.94.199.119536723721528352220 3/20/23-16:21:16.976524	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53672	37215	192.168.2.23	93.94.199.119
192.168.2.2394.187.107.9039438372152835222 03/20/23-16:21:34.558345	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39438	37215	192.168.2.23	94.187.107.90
192.168.2.23203.6.74.10537918372152835222 03/20/23-16:21:45.948271	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37918	37215	192.168.2.23	203.6.74.105
192.168.2.238.8.8.843281532023883 03/20/23-16:20:44.511900	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	43281	53	192.168.2.23	8.8.8.8
156.224.24.249192.168.2.2356999477962030489 03/20/23-16:21:24.722739	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	47796	156.224.24.249	192.168.2.23

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
156.224.24.249192.168.2.235699947806203048903/20/23-16:22:44.755597	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	47806	156.224.24.249	192.168.2.23
192.168.2.23197.234.43.1104950837215283522203/20/23-16:22:30.124421	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49508	37215	192.168.2.23	197.234.43.110
192.168.2.2341.36.73.5245328372152835222 03/20/23-16:21:23.129262	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45328	37215	192.168.2.23	41.36.73.52
192.168.2.23156.224.24.2494780656999203049003/20/23-16:21:34.964696	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	47806	56999	192.168.2.23	156.224.24.249
192.168.2.23197.39.71.735809637215283522203/20/23-16:22:16.668019	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58096	37215	192.168.2.23	197.39.71.73
192.168.2.2386.71.8.2424252037215283522203/20/23-16:22:02.177570	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42520	37215	192.168.2.23	86.71.8.242
192.168.2.23156.224.24.2494779656999203049003/20/23-16:20:45.109110	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	47796	56999	192.168.2.23	156.224.24.249
192.168.2.23192.107.143.1594789637215283522203/20/23-16:22:19.853858	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47896	37215	192.168.2.23	192.107.143.159
192.168.2.238.8.8.846438532023883 03/20/23-16:21:34.369876	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	46438	53	192.168.2.23	8.8.8.8

Network Port Distribution



Total Packets: 98

- 37215 undefined
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:20:44.511899948 CET	192.168.2.23	8.8.8.8	0xbd46	Standard query (0)	j.xnyidc.top	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:21:34.369875908 CET	192.168.2.23	8.8.8.8	0x9d8a	Standard query (0)	j.xnyidc.top	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 16:20:44.889858007 CET	8.8.8.8	192.168.2.23	0xbd46	No error (0)	j.xnyidc.top		156.224.24.249	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:21:34.751024961 CET	8.8.8.8	192.168.2.23	0x9d8a	No error (0)	j.xnyidc.top		156.224.24.249	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: 8lsvVMbYw7.elf PID: **6211**, Parent PID: **6129**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/tmp/8lsvVMbYw7.elf
Arguments:	/tmp/8lsvVMbYw7.elf
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: 8lsvVMbYw7.elf PID: **6213**, Parent PID: **6211**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/tmp/8lsvVMbYw7.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: **6213**, Parent PID: **6211**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv /tmp/8lsvVMbYw7.elf bin/watchdog; chmod 777 bin/watchdog"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6215**, Parent PID: **6213**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6215**, Parent PID: **6213**

General	
Start time:	16:20:43
Start date:	20/03/2023
Path:	/usr/bin/rm
Arguments:	rm -rf bin/watchdog
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: sh PID: **6216**, Parent PID: **6213**

General	
Start time:	16:20:43
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **6216**, Parent PID: **6213**

General	
Start time:	16:20:43
Start date:	20/03/2023
Path:	/usr/bin/mkdir
Arguments:	mkdir bin
File size:	88408 bytes
MD5 hash:	088c9d1df5a28ed16c726eca15964cb7

File Activities

File Read

Directory Created

Analysis Process: sh PID: **6217**, Parent PID: **6213**

General	
Start time:	16:20:43
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: **6217**, Parent PID: **6213**

General	
Start time:	16:20:43
Start date:	20/03/2023
Path:	/usr/bin/mv
Arguments:	mv /tmp/8lsvVMbYw7.elf bin/watchdog
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: **6218**, Parent PID: **6213**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **6218**, Parent PID: **6213**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/usr/bin/chmod
Arguments:	chmod 777 bin/watchdog
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Permission Modified

Analysis Process: 8lsvVMbYw7.elf PID: **6219**, Parent PID: **6211**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/tmp/8lsvVMbYw7.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 8lsvVMbYw7.elf PID: **6221**, Parent PID: **6219**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/tmp/8lsvVMbYw7.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: 8lsvVMbYw7.elf PID: **6222**, Parent PID: **6219**

General

Start time:	16:20:43
Start date:	20/03/2023
Path:	/tmp/8lsvVMbYw7.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c