ID: 830684
Sample Name: ID25Z9LfKe.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 15:58:57
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

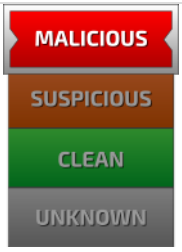
lD25Z9LfKe.elf

Overview

General Information

Sample Name:	lD25Z9LfKe.elf
Original Sample Name:	c929d58b6bb8…
Analysis ID:	830684
MD5:	c929d58b6bb8…
SHA1:	711976261f2f1…
SHA256:	e1366976365d…
Tags:	32 elf mirai powerpc
Infos:	

Detection



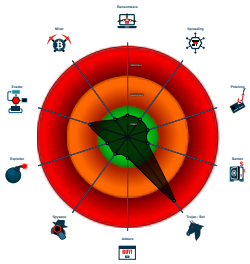
Mirai, Moobot

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.

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830684
Start date and time:	2023-03-20 15:58:57 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
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:	lD25Z9LfKe.elf
Original Sample Name:	c929d58b6bb8f66edc985003ba50c3c1.elf
Detection:	MAL
Classification:	mal92.troj.linELF@0/0@2/0

Warnings

Runtime Messages

Command:	/tmp/lD25Z9LfKe.elf
PID:	6224
Exit Code:	0
Exit Code Info:	
Killed:	False

Standard Output:	done.
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- ID25Z9LfKe.elf (PID: 6224, Parent: 6126, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/ID25Z9LfKe.elf
  - ID25Z9LfKe.elf New Fork (PID: 6226, Parent: 6224)
  - sh (PID: 6226, Parent: 6224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv /tmp/ID25Z9LfKe.elf bin/watchdog; chmod 777 bin/watchdog"
    - sh New Fork (PID: 6228, Parent: 6226)
    - rm (PID: 6228, Parent: 6226, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/watchdog
    - sh New Fork (PID: 6229, Parent: 6226)
    - mkdir (PID: 6229, Parent: 6226, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6230, Parent: 6226)
    - mv (PID: 6230, Parent: 6226, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/ID25Z9LfKe.elf bin/watchdog
    - sh New Fork (PID: 6231, Parent: 6226)
    - chmod (PID: 6231, Parent: 6226, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/watchdog
  - ID25Z9LfKe.elf New Fork (PID: 6232, Parent: 6224)
    - ID25Z9LfKe.elf New Fork (PID: 6234, Parent: 6232)
    - ID25Z9LfKe.elf New Fork (PID: 6236, Parent: 6232)
- **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
ID25Z9LfKe.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
ID25Z9LfKe.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
lD25Z9LfKe.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xd33c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd350:$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 • 0xd364:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd378:$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 • 0xd38c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3a0:$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 • 0xd3b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3c8:$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 • 0xd3dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3f0:$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 • 0xd404:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd418:$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 • 0xd42c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd440:$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 • 0xd454:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd468:$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 • 0xd47c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd490:$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 • 0xd4a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd4b8:$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 • 0xd4cc:$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
6224.1.00007effc4001000.00007effc4011000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6224.1.00007effc4001000.00007effc4011000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6224.1.00007effc4001000.00007effc4011000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xd33c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd350:$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 • 0xd364:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd378:$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 • 0xd38c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3a0:$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 • 0xd3b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3c8:$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 • 0xd3dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3f0:$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 • 0xd404:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd418:$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 • 0xd42c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd440:$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 • 0xd454:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd468:$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 • 0xd47c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd490:$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 • 0xd4a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd4b8:$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 • 0xd4cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Process Memory Space: lD25Z9LfKe.elf PID: 6224	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
Process Memory Space: lD25Z9LfKe.elf PID: 6224	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x3754:$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 • 0x3768:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x377c:$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 • 0x3790:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x37a4:$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 • 0x37b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x37cc:$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 • 0x37e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x37f4:$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 • 0x3808:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x381c:$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 • 0x3830:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x3844:$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 • 0x3858:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x386c:$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 • 0x3880:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x3894:$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 • 0x38a8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x38bc:$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 • 0x38d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x38e4:$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

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

Timestamp:	192.168.2.238.8.8.833891532023883 03/20/23-15:59:46.829796
SID:	2023883
Source Port:	33891
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.37.68.246

Timestamp:	192.168.2.2341.37.68.246423023721528352222 03/20/23-16:00:54.853824
SID:	2835222
Source Port:	42302
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: 192.119.137.74

Timestamp:	192.168.2.23192.119.137.7457754372152835222 03/20/23-16:01:50.220586
SID:	2835222
Source Port:	57754
Destination Port:	37215
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:	156.224.24.249192.168.2.2356999478282030489 03/20/23-16:01:45.327043
SID:	2030489
Source Port:	56999
Destination Port:	47828
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: 197.39.222.152

Timestamp:	192.168.2.23197.39.222.15245430372152835222 03/20/23-16:01:18.217927
SID:	2835222
Source Port:	45430
Destination Port:	37215
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:	156.224.24.249192.168.2.2356999477962030489 03/20/23-16:00:44.195958
SID:	2030489
Source Port:	56999
Destination Port:	47796
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: 197.214.98.38

Timestamp:	192.168.2.23197.214.98.3835290372152835222 03/20/23-16:00:31.085625
SID:	2835222
Source Port:	35290
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: 141.117.56.180	
Timestamp:	192.168.2.23141.117.56.18059180372152835222 03/20/23-16:01:09.639143
SID:	2835222
Source Port:	59180
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:	192.168.2.23156.224.24.24947828569992030490 03/20/23-16:00:49.583605
SID:	2030490
Source Port:	47828
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: 34.117.1.253	
Timestamp:	192.168.2.2334.117.1.25340848372152835222 03/20/23-16:00:17.642577
SID:	2835222
Source Port:	40848
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: 103.167.148.132	
Timestamp:	192.168.2.23103.167.148.13246324372152835222 03/20/23-16:00:41.668931
SID:	2835222
Source Port:	46324
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: 41.237.49.241	
Timestamp:	192.168.2.2341.237.49.24132970372152835222 03/20/23-16:00:38.463363
SID:	2835222
Source Port:	32970
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: 41.234.87.51	
Timestamp:	192.168.2.2341.234.87.5138528372152835222 03/20/23-16:01:07.497528
SID:	2835222
Source Port:	38528
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: 41.236.241.240	
Timestamp:	192.168.2.2341.236.241.24052042372152835222 03/20/23-16:01:35.636258
SID:	2835222
Source Port:	52042
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: 197.234.59.68	
Timestamp:	192.168.2.23197.234.59.6833038372152835222 03/20/23-16:00:22.715968
SID:	2835222
Source Port:	33038

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: 41.34.164.79

Timestamp:	192.168.2.2341.34.164.7957718372152835222 03/20/23-15:59:50.971789
SID:	2835222
Source Port:	57718
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:	192.168.2.238.8.8.859786532023883 03/20/23-16:00:49.089429
SID:	2023883
Source Port:	59786
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 20.28.196.139

Timestamp:	192.168.2.2320.28.196.13955414372152835222 03/20/23-16:01:13.960170
SID:	2835222
Source Port:	55414
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 03/20/23-15:59:47.422349
SID:	2030490
Source Port:	47796
Destination Port:	56999
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

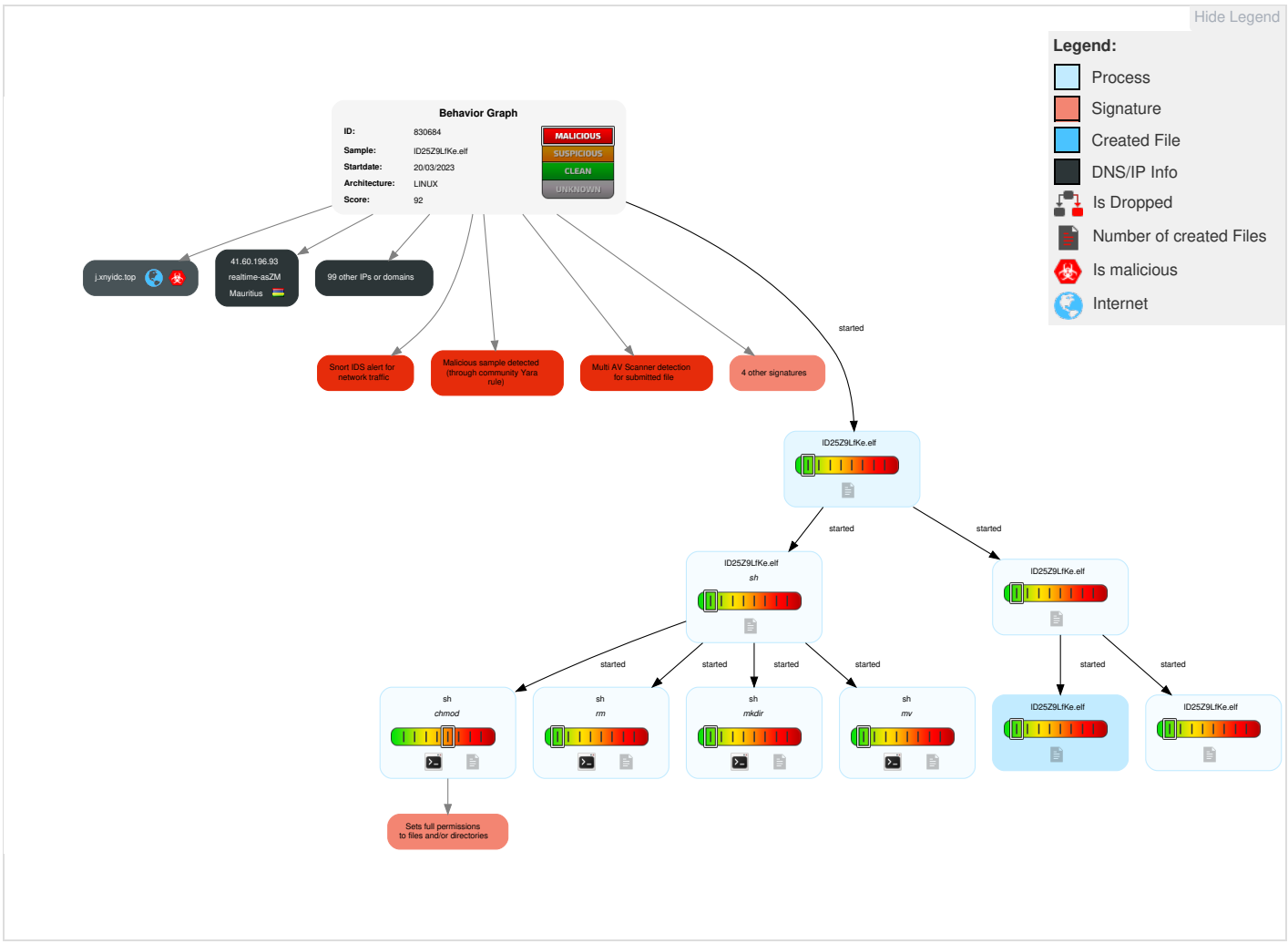
Mitre Att&ck Matrix

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
ID25Z9LfKe.elf	61%	Virustotal		Browse
ID25Z9LfKe.elf	62%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

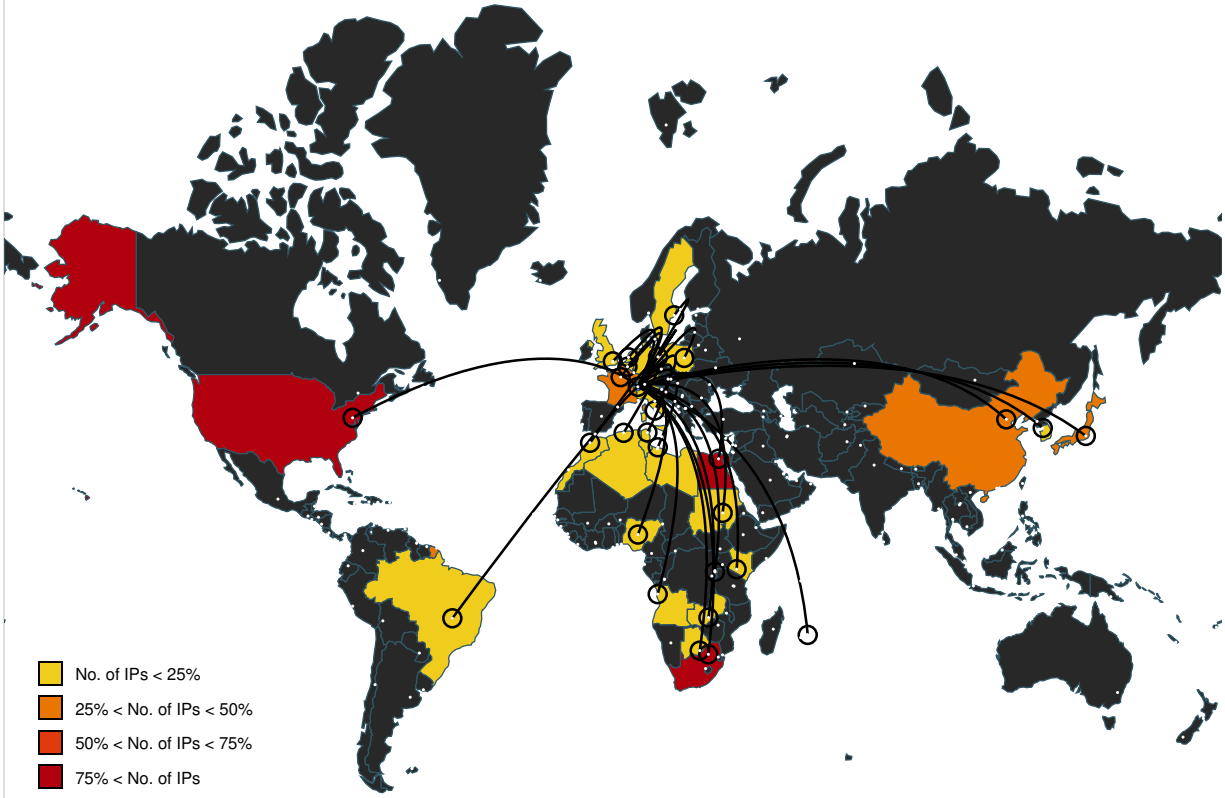
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
j.xnyidc.top	156.224.24.249	true	true		unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.140.45.249	unknown	Morocco		36903	MT-MPLSMA	false
197.32.82.226	unknown	Egypt		8452	TE-ASTE-ASEG	false
163.158.117.225	unknown	Netherlands		15435	KABELFOONDELTAFiberNederlandNL	false
197.222.170.148	unknown	Egypt		37069	MOBINILEG	false
156.68.4.30	unknown	United States		297	AS297US	false
157.170.134.145	unknown	United States		22192	SSHENETUS	false
191.251.70.242	unknown	Brazil		18881	TELEFONICABRASILSAB R	false
157.25.93.74	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
197.166.178.20	unknown	Egypt		24863	LINKdotNET-ASEG	false
41.37.167.64	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.157.17.94	unknown	South Africa		37168	CELL-CZA	false
197.13.10.211	unknown	Tunisia		37504	MeninxTN	false
166.7.140.80	unknown	United States		4152	USDA-1US	false
42.244.163.220	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
197.96.136.79	unknown	South Africa		3741	ISZA	false
41.28.116.156	unknown	South Africa		29975	VODACOM-ZA	false
41.225.142.122	unknown	Tunisia		37671	GLOBALNET-ASTN	false
157.187.164.211	unknown	United States		668	DNIC-AS-00668US	false
197.67.5.199	unknown	South Africa		16637	MTNNS-ASZA	false
157.201.93.207	unknown	United States		33281	BRIGHAM-YOUNG-UNIVERSITY-IDAHOUS	false
41.197.85.111	unknown	Rwanda		36934	Broadband-Systems-CorporationRW	false
157.91.133.253	unknown	United States		1767	ILIGHT-NETUS	false
116.40.18.77	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
25.39.89.88	unknown	United Kingdom		7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.38.199.133	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.215.94.18	unknown	United States		4704	SANNETRakutenMobileIncJP	false
41.140.45.231	unknown	Morocco		36903	MT-MPLSMA	false
157.78.121.27	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
41.87.162.76	unknown	Botswana		14988	BTC-GATE1BW	false
157.229.129.36	unknown	United States		122	UPMC-AS122US	false
197.53.131.60	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.208.8.24	unknown	Sudan		36998	SDN-MOBITELSD	false
146.113.78.52	unknown	United States		19653	CTSTELECOMUS	false
41.169.49.23	unknown	South Africa		36937	Neotel-ASZA	false
115.32.176.38	unknown	China		4766	KIXS-AS-KRKoreaTelecomKR	false
93.42.245.167	unknown	Italy		12874	FASTWEBIT	false
217.174.200.116	unknown	France		16128	AGARIK-NETWORKAGARIKprovideWEBServersHostingandddedic	false
116.227.65.226	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
197.205.16.187	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.234.167.162	unknown	South Africa		37315	CipherWaveZA	false
105.120.48.139	unknown	Nigeria		36873	VNL1-ASNG	false
41.133.87.44	unknown	South Africa		10474	OPTINETZA	false
197.43.173.201	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.213.176.58	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
41.215.72.106	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
177.143.135.107	unknown	Brazil		28573	CLAROSABR	false
41.29.197.7	unknown	South Africa		29975	VODACOM-ZA	false
157.68.50.108	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
51.166.246.213	unknown	United States		2686	ATGS-MMD-ASUS	false
218.9.165.51	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
157.172.225.249	unknown	France		22192	SSHENETUS	false
72.211.79.5	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
197.150.214.14	unknown	Egypt		37069	MOBINILEG	false
65.165.199.98	unknown	United States		397461	DURA-DHQ01US	false
41.108.235.23	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.192.154.253	unknown	Egypt		36992	ETISALAT-MISREG	false
144.159.93.230	unknown	United States		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
197.82.0.71	unknown	South Africa		10474	OPTINETZA	false
62.112.56.5	unknown	Germany		13157	GOPAS-ASSchellerdamm16DE	false
41.254.111.167	unknown	Libyan Arab Jamahiriya		21003	GPTC-ASLY	false
148.136.130.185	unknown	Sweden		3246	TDCSONGTele2BusinessTDCSwedenSE	false
41.54.81.5	unknown	South Africa		37168	CELL-CZA	false
197.254.68.2	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
41.38.222.219	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.53.118.43	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.240.217.45	unknown	unknown		37705	TOPNETTN	false
157.217.179.234	unknown	United States		4704	SANNETRakutenMobileIncJP	false
41.85.100.79	unknown	South Africa		328418	Olena-Trading-ASZA	false
197.0.31.226	unknown	Tunisia		37705	TOPNETTN	false
81.201.187.28	unknown	France		41157	OXYMIUMFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.209.232.177	unknown	France		12322	PROXADFR	false
41.60.103.187	unknown	Mauritius		30969	ZOL-ASGB	false
41.30.242.98	unknown	South Africa		29975	VODACOM-ZA	false
197.223.25.39	unknown	Egypt		37069	MOBINILEG	false
41.213.11.5	unknown	South Africa		33762	rainZA	false
41.60.196.93	unknown	Mauritius		37146	realtime-asZM	false
197.34.133.169	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.110.164.253	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.167.121.188	unknown	Egypt		24863	LINKdotNET-ASEG	false
41.78.159.18	unknown	Nigeria		37249	CWHOUSENG	false
132.166.229.117	unknown	France		777	CEA-SaclayEU	false
197.104.43.201	unknown	South Africa		37168	CELL-CZA	false
157.104.170.195	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
157.111.84.0	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
64.209.21.87	unknown	United States		3549	LVLT-3549US	false
41.237.81.183	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.170.134.112	unknown	United States		22192	SSHENETUS	false
41.112.220.172	unknown	South Africa		16637	MTNNS-ASZA	false
197.123.173.64	unknown	Egypt		36992	ETISALAT-MISREG	false
216.90.206.88	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
41.167.92.137	unknown	South Africa		36937	Neotel-ASZA	false
197.133.107.209	unknown	Egypt		24835	RAYA-ASEG	false
123.234.32.254	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
197.194.23.197	unknown	Egypt		36992	ETISALAT-MISREG	false
157.114.174.50	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
20.68.251.26	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
197.89.224.214	unknown	South Africa		10474	OPTINETZA	false
197.217.201.64	unknown	Angola		11259	ANGOLATELECOMAO	false
43.177.91.167	unknown	Japan		4249	LILLY-ASUS	false
188.188.192.207	unknown	Belgium		44944	BASE-ASTelenetGroupNVSABE	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, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.271370241540659
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	ID25Z9LfKe.elf
File size:	62988
MD5:	c929d58b6bb8f66edc985003ba50c3c1
SHA1:	711976261f2f197a341dca8afdb7679f04aa3f99
SHA256:	e1366976365db1f2bffdc37d4e64e12f883f9a20e02b12d52b6a1b346b8f0692
SHA512:	3982301f57bf1e26ee56855de69eb9dce72e2ff1b3437ab9608433955c09f8c2f2e44d120daaaa7edc12e755884555dc5cfa0578f03d18233e256de9c9feb4bb
SSDEEP:	768:qkaZjEoakZNRGHRnDmX7Xm+t/UGV8+BCpEMCi/J9KCrMvuBxANUr6FV+tMiwWfIC:MvolWm+phBgd/KCAWBxANee++bWfvF
TLSH:	C0534B02B31C0A07D1A31AB0253F5BD197BBEAD022F4F684751F979A96B5E361182FCD
File Content Preview:	.ELF.....4....,....4. ...(.....p...p.....t...t...t...l..%t.....dt.Q.....!..|.....$H...H..-...$8!. |...N.. .!..|.....?.....T..../...@..\?.....+../...A..$8...}).....N..

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
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	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0xd184	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1000d23c	0xd23c	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1000d260	0xd260	0x1e10	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x1001f074	0xf074	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1001f07c	0xf07c	0x8	0x0	0x3	WA	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.data	PROGBITS	0x1001f088	0xf088	0x314	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1001f39c	0xf39c	0x44	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x1001f3e0	0xf3e0	0x74	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1001f454	0xf3e0	0x2194	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf3e0	0x4b	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	0x10000000	0x10000000	0xf070	0xf070	6.3212	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xf074	0x1001f074	0x1001f074	0x36c	0x2574	2.8425	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

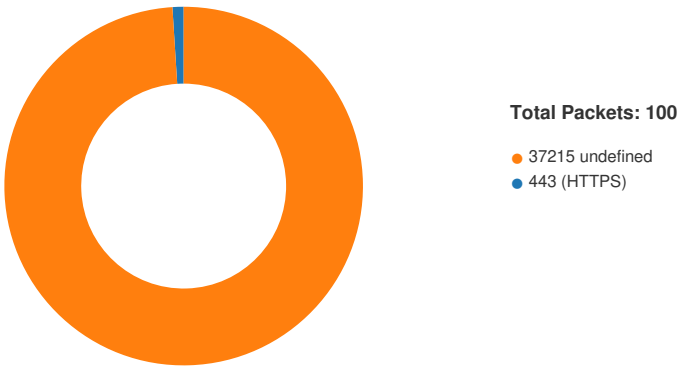
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.238.8.8.833891532023883 03/20/23-15:59:46.829796	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	33891	53	192.168.2.23	8.8.8.8
192.168.2.2341.37.68.24642302372152835222 03/20/23-16:00:54.853824	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42302	37215	192.168.2.23	41.37.68.246
192.168.2.23192.119.137.745775437215283522203/20/23-16:01:50.220586	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57754	37215	192.168.2.23	192.119.137.74
156.224.24.249192.168.2.2356999478282030489 03/20/23-16:01:45.327043	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	47828	156.224.24.249	192.168.2.23
192.168.2.23197.39.222.152454303721528352220 03/20/23-16:01:18.217927	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45430	37215	192.168.2.23	197.39.222.152
156.224.24.249192.168.2.2356999477962030489 03/20/23-16:00:44.195958	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	47796	156.224.24.249	192.168.2.23
192.168.2.23197.214.98.383529037215283522203/20/23-16:00:31.085625	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35290	37215	192.168.2.23	197.214.98.38
192.168.2.23141.117.56.1805918037215283522203/20/23-16:01:09.639143	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59180	37215	192.168.2.23	141.117.56.180
192.168.2.23156.224.24.2494978285699920304900 03/20/23-16:00:49.583605	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	47828	56999	192.168.2.23	156.224.24.249
192.168.2.2334.117.1.25340848372152835222 03/20/23-16:00:17.642577	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40848	37215	192.168.2.23	34.117.1.253
192.168.2.23103.167.148.13246324372152835222 03/20/23-16:00:41.668931	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46324	37215	192.168.2.23	103.167.148.132
192.168.2.2341.237.49.24132970372152835222 03/20/23-16:00:38.463363	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32970	37215	192.168.2.23	41.237.49.241

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2341.234.87.51 38528372152835222 03/20/23-16:01:07.497528	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38528	37215	192.168.2.23	41.234.87.51
192.168.2.2341.236.241.240520423721528352222 03/20/23-16:01:35.636258	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52042	37215	192.168.2.23	41.236.241.240
192.168.2.23197.234.59.683303837215283522203/20/23-16:00:22.715968	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33038	37215	192.168.2.23	197.234.59.68
192.168.2.2341.34.164.795771837215283522203/20/23-15:59:50.971789	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57718	37215	192.168.2.23	41.34.164.79
192.168.2.238.8.8.859786532023883 03/20/23-16:00:49.089429	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	59786	53	192.168.2.23	8.8.8.8
192.168.2.2320.28.196.13955541437215283522203/20/23-16:01:13.960170	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55414	37215	192.168.2.23	20.28.196.139
192.168.2.23156.224.24.2494779656999203049003/20/23-15:59:47.422349	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

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 15:59:46.829796076 CET	192.168.2.23	8.8.8.8	0xa123	Standard query (0)	j.xnyidc.top	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:00:49.089428902 CET	192.168.2.23	8.8.8.8	0xb38e	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 15:59:47.205801010 CET	8.8.8.8	192.168.2.23	0xa123	No error (0)	j.xnyidc.top		156.224.24.249	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:00:49.369513035 CET	8.8.8.8	192.168.2.23	0xb38e	No error (0)	j.xnyidc.top		156.224.24.249	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: lD25Z9LfKe.elf PID: **6224**, Parent PID: **6126**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/tmp/lD25Z9LfKe.elf
Arguments:	/tmp/lD25Z9LfKe.elf
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: lD25Z9LfKe.elf PID: **6226**, Parent PID: **6224**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/tmp/lD25Z9LfKe.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: sh PID: **6226**, Parent PID: **6224**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv /tmp/lD25Z9LfKe.elf bin/watchdog; chmod 777 bin/watchdog"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6228**, Parent PID: **6226**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6228**, Parent PID: **6226**

General

Start time:	15:59:45
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: 6229, Parent PID: 6226

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: 6229, Parent PID: 6226

General

Start time:	15:59:45
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: 6230, Parent PID: 6226

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: 6230, Parent PID: 6226

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/usr/bin/mv
Arguments:	mv /tmp/ID25Z9LfKe.elf bin/watchdog
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: 6231, Parent PID: 6226

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **6231**, Parent PID: **6226**

General

Start time:	15:59:45
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: lD25Z9LfKe.elf PID: **6232**, Parent PID: **6224**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/tmp/lD25Z9LfKe.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: lD25Z9LfKe.elf PID: **6234**, Parent PID: **6232**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/tmp/lD25Z9LfKe.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: lD25Z9LfKe.elf PID: **6236**, Parent PID: **6232**

General

Start time:	15:59:45
Start date:	20/03/2023
Path:	/tmp/lD25Z9LfKe.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6