ID: 830724
Sample Name: XHZFo8hExw.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:35:09
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

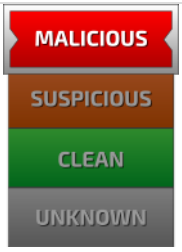
XHZFo8hExw.elf

Overview

General Information

Sample Name:	XHZFo8hExw.elf
Original Sample Name:	f90025024613f…
Analysis ID:	830724
MD5:	f90025024613f…
SHA1:	b44c167b326ff…
SHA256:	d502542baec7…
Tags:	32 elf intel mirai
Infos:	

Detection



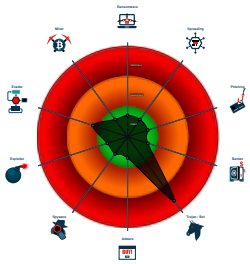
Mirai, Moobot

Score:	96
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…
- Machine Learning detection for sam…
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…

Classification



Analysis Advice

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:	830724
Start date and time:	2023-03-20 16:35:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
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:	XHZFo8hExw.elf
Original Sample Name:	f90025024613f3a9d54373f3cc68eefd.elf
Detection:	MAL
Classification:	mal96.troj.linELF@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/XHZFo8hExw.elf
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	done.

Standard Error:	sh: 1: cannot open : No such file

Process Tree

- **system is lnxubuntu20**
- XHZFo8hExw.elf (PID: 6226, Parent: 6119, MD5: f90025024613f3a9d54373f3cc68eefd) Arguments: /tmp/XHZFo8hExw.elf
  - XHZFo8hExw.elf New Fork (PID: 6227, Parent: 6226)
  - sh (PID: 6227, Parent: 6226, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv */tmp/XHZFo8hExw.elf <\\xc0\\xbc\\xff\\x84\\x83\\x86\tbin/watchdog; chmod 777 bin/watchdog"
    - sh New Fork (PID: 6228, Parent: 6227)
    - rm (PID: 6228, Parent: 6227, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/watchdog
    - sh New Fork (PID: 6229, Parent: 6227)
    - mkdir (PID: 6229, Parent: 6227, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6230, Parent: 6227)
    - chmod (PID: 6230, Parent: 6227, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/watchdog
  - XHZFo8hExw.elf New Fork (PID: 6231, Parent: 6226)
    - XHZFo8hExw.elf New Fork (PID: 6232, Parent: 6231)
    - XHZFo8hExw.elf New Fork (PID: 6233, Parent: 6231)
- **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
XHZFo8hExw.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
XHZFo8hExw.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
XHZFo8hExw.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xc218:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc22c:$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 • 0xc240:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc254:$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 • 0xc268:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc27c:$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 • 0xc290:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc2a4:$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 • 0xc2b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc2cc:$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 • 0xc2e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc2f4:$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 • 0xc308:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc31c:$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 • 0xc330:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc344:$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 • 0xc358:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc36c:$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 • 0xc380:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc394:$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 • 0xc3a8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
XHZFo8hExw.elf	Linux_Trojan_Gafgyt_5bf62ce4	unknown	unknown	• 0xa011:$a: 89 E5 56 53 31 F6 8D 45 10 83 EC 10 89 45 F4 8B 55 F4 46 8D
XHZFo8hExw.elf	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x45e0:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3
Click to see the 5 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
6226.1.0000000008048000.0000000008056000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6226.1.0000000008048000.0000000008056000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6226.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xc218:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc22c:$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 • 0xc240:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc254:$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 • 0xc268:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc27c:$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 • 0xc290:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc2a4:$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 • 0xc2b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc2cc:$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 • 0xc2e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc2f4:$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 • 0xc308:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc31c:$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 • 0xc330:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc344:$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 • 0xc358:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc36c:$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 • 0xc380:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc394:$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 • 0xc3a8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6226.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Gafgyt_5bf62ce4	unknown	unknown	• 0xa011:$a: 89 E5 56 53 31 F6 8D 45 10 83 EC 10 89 45 F4 8B 55 F4 46 8D
6226.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x45e0:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3

Click to see the 6 entries

Snort Signatures

ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1) - Source IP: 192.168.2.23 - Destination IP: 103.161.181.97

Timestamp:	192.168.2.23103.161.181.9751628569992030490 03/20/23-16:35:53.346108
SID:	2030490
Source Port:	51628
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: 156.224.11.114

Timestamp:	192.168.2.23156.224.11.11456256372152835222 03/20/23-16:36:47.049175
SID:	2835222
Source Port:	56256
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: 41.237.5.201

Timestamp:	192.168.2.2341.237.5.201409863721528352222 03/20/23-16:36:24.420831
SID:	2835222
Source Port:	40986

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: 157.122.72.69

Timestamp:	192.168.2.23157.122.72.6939570372152835222 03/20/23-16:36:24.331963
SID:	2835222
Source Port:	39570
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: 41.36.233.70

Timestamp:	192.168.2.2341.36.233.70395903721528352222 03/20/23-16:37:00.531602
SID:	2835222
Source Port:	39590
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: 147.46.79.137

Timestamp:	192.168.2.23147.46.79.137329763721528352222 03/20/23-16:37:21.136876
SID:	2835222
Source Port:	32976
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response - Source IP: 103.161.181.97 - Destination IP: 192.168.2.23

Timestamp:	103.161.181.97192.168.2.2356999516282030489 03/20/23-16:37:52.298836
SID:	2030489
Source Port:	56999
Destination Port:	51628
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: 197.39.68.98

Timestamp:	192.168.2.23197.39.68.98395743721528352222 03/20/23-16:36:06.532616
SID:	2835222
Source Port:	39574
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: 41.237.5.201

Timestamp:	192.168.2.2341.237.5.201409883721528352222 03/20/23-16:36:24.422131
SID:	2835222
Source Port:	40988
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: 154.38.241.212

Timestamp:	192.168.2.23154.38.241.21259410372152835222 03/20/23-16:36:58.418193
SID:	2835222
Source Port:	59410
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: 197.39.56.45	
Timestamp:	192.168.2.23197.39.56.4557594372152835222 03/20/23-16:37:32.803566
SID:	2835222
Source Port:	57594
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: 27.0.158.180	
Timestamp:	192.168.2.2327.0.158.18046574372152835222 03/20/23-16:36:00.398384
SID:	2835222
Source Port:	46574
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: 41.239.113.31	
Timestamp:	192.168.2.2341.239.113.3144976372152835222 03/20/23-16:36:12.950349
SID:	2835222
Source Port:	44976
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: 163.15.165.22	
Timestamp:	192.168.2.23163.15.165.2239134372152835222 03/20/23-16:37:53.743391
SID:	2835222
Source Port:	39134
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

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

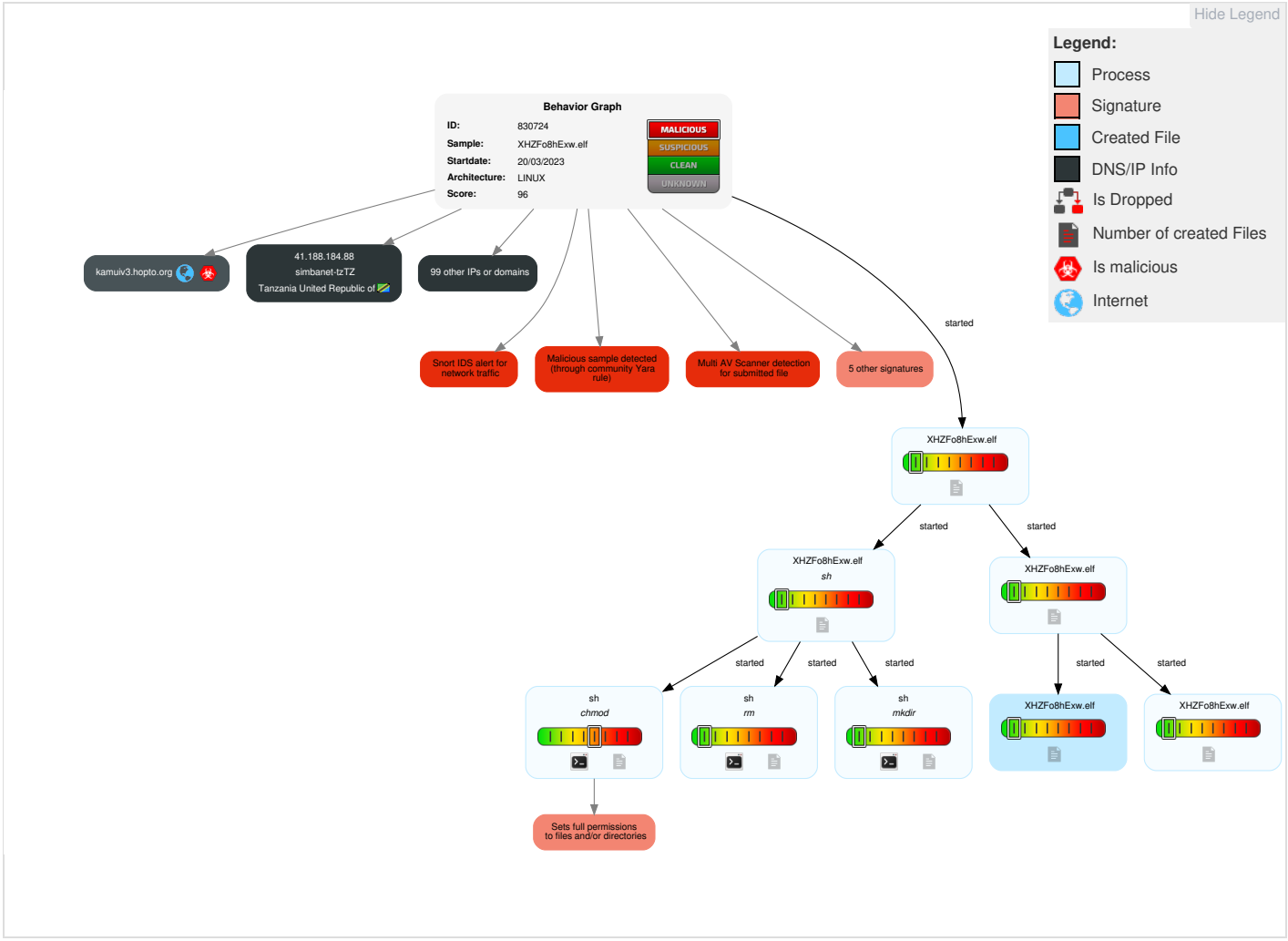
Mitre Att&ck Matrix

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	System Service 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
XHZFo8hExw.elf	59%	ReversingLabs	Linux.Trojan.Mirai	
XHZFo8hExw.elf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

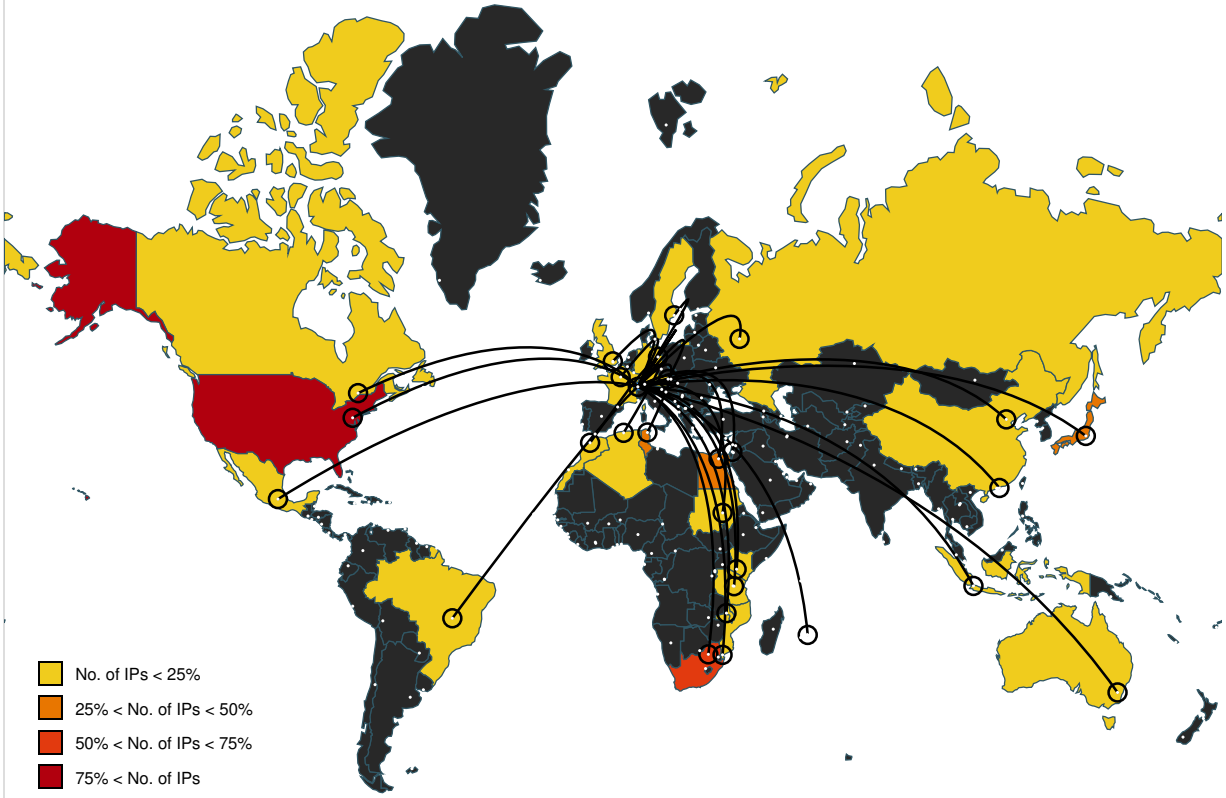
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kamuiv3.hopto.org	103.161.181.97	true	true		unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.222.253.14	unknown	United States		4704	SANNETRakutenMobileIncJP	false
123.2.106.131	unknown	Australia		38285	VOCUS-RETAIL-AUVocusRetailAU	false
197.252.128.188	unknown	Sudan		15706	SudatelSD	false
157.248.240.207	unknown	United States		32934	FACEBOOKUS	false
69.13.83.61	unknown	United States		54489	CORESPACE-DALUS	false
197.21.53.58	unknown	Tunisia		37693	TUNISIANATN	false
41.239.14.56	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.29.92.236	unknown	South Africa		29975	VODACOM-ZA	false
197.22.223.233	unknown	Tunisia		37693	TUNISIANATN	false
197.211.30.86	unknown	Kenya		15399	WANANCHI-KE	false
157.64.218.80	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
136.136.78.96	unknown	United States		60311	ONEFMCH	false
103.79.96.223	unknown	Indonesia		64308	IDNIC-DATAON-AS-IDPTIndoDevNiagaInternetID	false
45.92.107.116	unknown	United Kingdom		208485	EKSENBILISIMTR	false
157.85.134.11	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
157.219.235.195	unknown	United States		4704	SANNETRakutenMobileIncJP	false
197.166.154.65	unknown	Egypt		24863	LINKdotNET-ASEG	false
178.130.158.179	unknown	Palestinian Territory Occupied		51407	MADA-ASPS	false
157.20.68.147	unknown	unknown		24297	FCNUniversityPublicCorporationOsakaJP	false
157.222.253.161	unknown	United States		4704	SANNETRakutenMobileIncJP	false
177.213.86.27	unknown	Brazil		26599	TELEFONICABRASILSAB R	false
197.21.90.14	unknown	Tunisia		37693	TUNISIANATN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
175.176.224.75	unknown	Hong Kong		9229	SPEEDCAST-APSPEEDCASTLimitedHK	false
197.78.176.195	unknown	South Africa		16637	MTNNS-ASZA	false
157.67.71.116	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
157.247.205.7	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
197.169.172.171	unknown	South Africa		37168	CELL-CZA	false
20.215.158.192	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
197.89.123.84	unknown	South Africa		10474	OPTINETZA	false
157.175.218.249	unknown	United States		16509	AMAZON-02US	false
62.224.13.74	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
157.242.3.106	unknown	United States		25789	LMUUS	false
41.60.37.66	unknown	Mauritius		30969	ZOL-ASGB	false
157.125.18.12	unknown	Sweden		31655	ASN-GAMMATELECOMGB	false
157.135.242.106	unknown	United States		600	OARNET-ASUS	false
197.211.114.49	unknown	Malawi		37187	SKYBANDMW	false
197.64.175.149	unknown	South Africa		16637	MTNNS-ASZA	false
197.226.252.37	unknown	Mauritius		23889	MauritiusTelecomMU	false
41.19.78.128	unknown	South Africa		29975	VODACOM-ZA	false
197.37.162.226	unknown	Egypt		8452	TE-ASTE-ASEG	false
205.36.77.137	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
102.224.168.208	unknown	unknown		36926	CKL1-ASNKE	false
157.14.236.67	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	false
19.16.45.213	unknown	United States		3	MIT-GATEWAYSUS	false
41.44.233.222	unknown	Egypt		8452	TE-ASTE-ASEG	false
126.240.235.65	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
41.38.222.243	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.98.43.171	unknown	United States		3527	NIH-NETUS	false
41.141.72.150	unknown	Morocco		36903	MT-MPLSMA	false
41.230.50.120	unknown	Tunisia		37705	TOPNETTN	false
41.122.225.65	unknown	South Africa		16637	MTNNS-ASZA	false
197.18.83.242	unknown	Tunisia		37693	TUNISIANATN	false
197.165.20.92	unknown	Egypt		24863	LINKdotNET-ASEG	false
157.187.69.254	unknown	United States		668	DNIC-AS-00668US	false
41.43.219.135	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.188.184.88	unknown	Tanzania United Republic of		37084	simbanet-tzTZ	false
41.195.197.32	unknown	South Africa		16637	MTNNS-ASZA	false
197.4.200.59	unknown	Tunisia		5438	ATI-TN	false
157.14.224.90	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	false
197.251.50.141	unknown	Sudan		37197	SUDRENSD	false
177.244.235.199	unknown	Mexico		13999	MegaCableSAdeCVMX	false
157.74.40.98	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
17.199.135.173	unknown	United States		714	APPLE-ENGINEERINGUS	false
208.115.146.123	unknown	United States		17385	ORBITELUS	false
52.195.214.237	unknown	United States		16509	AMAZON-02US	false
157.107.251.195	unknown	Japan		4685	ASAHI-NETAsahiNetJP	false
157.87.159.74	unknown	United States		21612	FUNDACAOINSTITUTOOSWALDOCRUZBR	false
41.225.230.125	unknown	Tunisia		37671	GLOBALNET-ASTN	false
53.212.253.138	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
197.89.196.43	unknown	South Africa		10474	OPTINETZA	false
122.137.112.239	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
100.172.140.117	unknown	United States		21928	T-MOBILE-AS21928US	false
197.206.228.129	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.163.181.143	unknown	Germany		22192	SSHENETUS	false
41.55.86.135	unknown	South Africa		37168	CELL-CZA	false
41.145.167.174	unknown	South Africa		5713	SAIX-NETZA	false
125.215.76.137	unknown	Japan		7522	STCNSTNetIncorporatedJP	false
197.235.69.37	unknown	Mozambique		37223	VODACOM-MZ	false
197.77.89.52	unknown	South Africa		16637	MTNNS-ASZA	false
157.75.1.57	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
157.245.211.186	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
142.237.203.2	unknown	Canada		32347	PRAN-ASNCA	false
135.89.221.28	unknown	United States		10455	LUCENT-CIOUS	false
157.76.253.214	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
197.49.160.167	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.30.202.42	unknown	Tunisia		37492	ORANGE-TN	false
89.2.156.164	unknown	France		21502	ASN-NUMERICABLEFR	false
197.36.184.199	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.32.129.131	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.77.13.122	unknown	Japan		4678	FINECanonITSolutionsIncJP	false
62.182.140.55	unknown	Russian Federation		29497	KUBANGSMRU	false
64.242.55.75	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
157.215.239.34	unknown	United States		4704	SANNETRakutenMobileIncJP	false
201.123.86.80	unknown	Mexico		8151	UninetSAdeCVMX	false
197.179.217.80	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
41.204.140.219	unknown	Tanzania United Republic of		36930	Zantel-ASTZ	false
41.239.63.43	unknown	Egypt		8452	TE-ASTE-ASEG	false
97.251.204.235	unknown	United States		6167	CELLCO-PARTUS	false
197.206.175.64	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.193.123.107	unknown	South Africa		11845	Vox-TelecomZA	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 LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.508652600152545
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	XHZFo8hExw.elf
File size:	58448
MD5:	f90025024613f3a9d54373f3cc68eefd
SHA1:	b44c167b326ff981979a38c1086cebe9d27feb66
SHA256:	d502542baec72142eef5bbe366c81681acaca46c920c37c724d2cd0b8a93a223
SHA512:	84c3505f1361c7907bd3533254ab0a8054365e7e7313205e97b7ae9ff5e209fd217dfb02e0876c91ed7de9beb116c89c4121eb5ee1fc3301459a38a13e6028e5
SSDEEP:	1536:ka4CVvtTO8yJT/0fSGUPk+nU61TH6V/Ps06r6M3:d4CxtTO8yd/0KGUs+n31Ta9k0JA
TLSH:	43434BC4F647E8F5DC5706741036EB778B32F5FA2218D743D3A99A32AC92601E617A8C
File Content Preview:	.ELF.....d...4.....4. ...(.....\...\.....`..`.....H(.....Q.td.....U..S.....w....h....s... []...$.....U.....=.b...t..5....$`.....$`.....u.....t....h\].....

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	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xbc96	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8053d46	0xbd46	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8053d60	0xbd60	0x1ffc	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8056000	0xe000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8056008	0xe008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8056020	0xe020	0x260	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8056280	0xe280	0x25c8	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xe280	0x3e	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	0x8048000	0x8048000	0xdd5c	0xdd5c	6.5895	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xe000	0x8056000	0x8056000	0x280	0x2848	3.4568	0x6	RW	0x1000		.ctors .dtors .data .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
192.168.2.23103.161.181.975162856999203049003/20/23-16:35:53.346108	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	51628	56999	192.168.2.23	103.161.181.97
192.168.2.23156.224.11.1145625637215283522203/20/23-16:36:47.049175	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56256	37215	192.168.2.23	156.224.11.114
192.168.2.2341.237.5.2014098637215283522203/20/23-16:36:24.420831	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40986	37215	192.168.2.23	41.237.5.201
192.168.2.23157.122.72.6939570372152835222203/20/23-16:36:24.331963	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39570	37215	192.168.2.23	157.122.72.69
192.168.2.2341.36.233.7039590372152835222203/20/23-16:37:00.531602	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39590	37215	192.168.2.23	41.36.233.70
192.168.2.23147.46.79.13732976372152835222203/20/23-16:37:21.136876	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	32976	37215	192.168.2.23	147.46.79.137
103.161.181.97192.168.2.2356999516282030489203/20/23-16:37:52.298836	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	51628	103.161.181.97	192.168.2.23
192.168.2.23197.39.68.983957437215283522203/20/23-16:36:06.532616	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39574	37215	192.168.2.23	197.39.68.98
192.168.2.2341.237.5.2014098837215283522203/20/23-16:36:24.422131	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40988	37215	192.168.2.23	41.237.5.201
192.168.2.23154.38.241.2125941037215283522203/20/23-16:36:58.418193	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59410	37215	192.168.2.23	154.38.241.212
192.168.2.23197.39.56.4557594372152835222203/20/23-16:37:32.803566	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57594	37215	192.168.2.23	197.39.56.45
192.168.2.2327.0.158.18046574372152835222203/20/23-16:36:00.398384	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46574	37215	192.168.2.23	27.0.158.180
192.168.2.2341.239.113.3144976372152835222203/20/23-16:36:12.950349	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44976	37215	192.168.2.23	41.239.113.31
192.168.2.23163.15.165.2239134372152835222203/20/23-16:37:53.743391	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	39134	37215	192.168.2.23	163.15.165.22

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:35:53.149841070 CET	192.168.2.23	8.8.8.8	0xb6e9	Standard query (0)	kamuiv3.hopto.org	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 16:35:53.170298100 CET	8.8.8.8	192.168.2.23	0xb6e9	No error (0)	kamuiv3.hopto.org		103.161.181.97	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: XHZFo8hExw.elf PID: 6226, Parent PID: 6119

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/tmp/XHZFo8hExw.elf
Arguments:	/tmp/XHZFo8hExw.elf
File size:	58448 bytes
MD5 hash:	f90025024613f3a9d54373f3cc68eefd

Analysis Process: XHZFo8hExw.elf PID: 6227, Parent PID: 6226

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/tmp/XHZFo8hExw.elf
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	f90025024613f3a9d54373f3cc68eefd

Analysis Process: sh PID: 6227, Parent PID: 6226

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv */tmp/XHZFo8hExw.elf <\\xc0\\xbc\\xff\\x84\\x83\\x86\tbin/watchdog; chmod 777 bin/watchdog"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6228, Parent PID: 6227

General

Start time:	16:35:52
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: **6227**

General

Start time:	16:35:52
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: **6227**

General

Start time:	16:35:52
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: **6227**

General

Start time:	16:35:52
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: **6227**

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **6230**, Parent PID: **6227**

General

Start time:	16:35:52
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: XHZFo8hExw.elf PID: **6231**, Parent PID: **6226**

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/tmp/XHZFo8hExw.elf
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	f90025024613f3a9d54373f3cc68eefd

Analysis Process: XHZFo8hExw.elf PID: **6232**, Parent PID: **6231**

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/tmp/XHZFo8hExw.elf
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	f90025024613f3a9d54373f3cc68eefd

File Activities

File Read

Directory Enumerated

Analysis Process: XHZFo8hExw.elf PID: **6233**, Parent PID: **6231**

General

Start time:	16:35:52
Start date:	20/03/2023
Path:	/tmp/XHZFo8hExw.elf
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	f90025024613f3a9d54373f3cc68eefd