ID: 831106
Sample Name: 3f8dH3KxbO.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:29:20
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

Linux Analysis Report

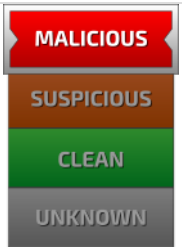
3f8dH3KxbO.elf

Overview

General Information

Sample Name:	3f8dH3KxbO.elf
Original Sample Name:	b2c7b530dda1…
Analysis ID:	831106
MD5:	b2c7b530dda1…
SHA1:	5a4fa656800a0..
SHA256:	792754c6e660…
Tags:	32 elf intel mirai
Infos:	

Detection



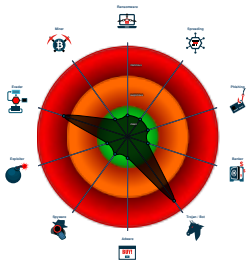
Mirai

Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Sample deletes itself
- Sample is packed with UPX
- Uses known network protocols on n…
- Connects to many ports of the same…
- Sample contains only a LOAD segm…
- Yara signature match
- HTTP GET or POST without a user …

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:	831106
Start date and time:	2023-03-21 03:29:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s
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:	3f8dH3KxbO.elf
Original Sample Name:	b2c7b530dda1e86285699cc34666bcf7.elf
Detection:	MAL
Classification:	mal96.troj.evad.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/3f8dH3KxbO.elf
PID:	6229
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	nkuvgpkpi/vwp2

Copyright Joe Security LLC 2023

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 3f8dH3KxbO.elf (PID: 6229, Parent: 6131, MD5: b2c7b530dda1e86285699cc34666bcf7) Arguments: /tmp/3f8dH3KxbO.elf
  - 3f8dH3KxbO.elf New Fork (PID: 6230, Parent: 6229)
  - 3f8dH3KxbO.elf New Fork (PID: 6232, Parent: 6229)
    - 3f8dH3KxbO.elf New Fork (PID: 6233, 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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth (Nextron Systems)	• 0xd13e:$x2: /dev/misc/watchdog • 0xd130:$x3: /dev/watchdog • 0xd275:$s1: LCOGQGPTGP
6229.1.0000000008048000.0000000008056000.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
6229.1.0000000008048000.0000000008056000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x78e0:$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
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_88de437f	unknown	unknown	• 0x9da2:$a: 24 08 8B 4C 24 04 85 D2 74 0D 31 C0 89 F6 C6 04 08 00 40 39 D0

Click to see the 3 entries

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.35.80.175

Timestamp:	192.168.2.2341.35.80.175373503721528352222 03/21/23-03:30:32.951807
SID:	2835222
Source Port:	37350
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: 156.247.27.187

Copyright Joe Security LLC 2023

Timestamp:	192.168.2.23156.247.27.1873388437215283522 2 03/21/23-03:30:43.507431
SID:	2835222
Source Port:	33884
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: 154.38.230.95

Timestamp:	192.168.2.23154.38.230.9548244372152835222 03/21/23-03:30:28.214197
SID:	2835222
Source Port:	48244
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: 197.246.192.49

Timestamp:	192.168.2.23197.246.192.4940868372152835222 03/21/23-03:30:30.427381
SID:	2835222
Source Port:	40868
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: 156.226.11.103

Timestamp:	192.168.2.23156.226.11.10359142372152835222 03/21/23-03:30:48.796217
SID:	2835222
Source Port:	59142
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: 156.254.44.245

Timestamp:	192.168.2.23156.254.44.24551292372152835222 03/21/23-03:30:30.585388
SID:	2835222
Source Port:	51292
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: 154.213.189.79

Timestamp:	192.168.2.23154.213.189.7935618372152835222 03/21/23-03:30:38.901778
SID:	2835222
Source Port:	35618
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: 154.211.47.114

Timestamp:	192.168.2.23154.211.47.11446036372152835222 03/21/23-03:30:28.311917
SID:	2835222
Source Port:	46036
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: 156.254.89.39

Timestamp:	192.168.2.23156.254.89.3942060372152835222 03/21/23-03:30:35.326766
SID:	2835222
Source Port:	42060
Destination Port:	37215

Copyright Joe Security LLC 2023

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: 156.227.245.46	
Timestamp:	192.168.2.23156.227.245.4649918372152835222 03/21/23-03:30:36.616130
SID:	2835222
Source Port:	49918
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: 41.236.89.9	
Timestamp:	192.168.2.2341.236.89.945968372152835222 03/21/23-03:30:35.158451
SID:	2835222
Source Port:	45968
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: 154.201.25.124	
Timestamp:	192.168.2.23154.201.25.12433512372152835222 03/21/23-03:30:39.166861
SID:	2835222
Source Port:	33512
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: 154.208.147.249	
Timestamp:	192.168.2.23154.208.147.24947468372152835222 03/21/23-03:30:26.768093
SID:	2835222
Source Port:	47468
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: 41.43.16.185	
Timestamp:	192.168.2.2341.43.16.185512763721528352222 03/21/23-03:30:38.721581
SID:	2835222
Source Port:	51276
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: 156.254.66.63	
Timestamp:	192.168.2.23156.254.66.6360202372152835222 03/21/23-03:30:39.166793
SID:	2835222
Source Port:	60202
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: 154.216.21.93	
Timestamp:	192.168.2.23154.216.21.9338882372152835222 03/21/23-03:30:42.237111
SID:	2835222
Source Port:	38882
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: 156.254.58.127

Timestamp:	192.168.2.23156.254.58.12744726372152835222 03/21/23-03:30:39.695821
SID:	2835222
Source Port:	44726
Destination Port:	37215
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

Uses known network protocols on non-standard ports

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

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Sample deletes itself

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

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	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated Files or Information	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 File Deletion	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

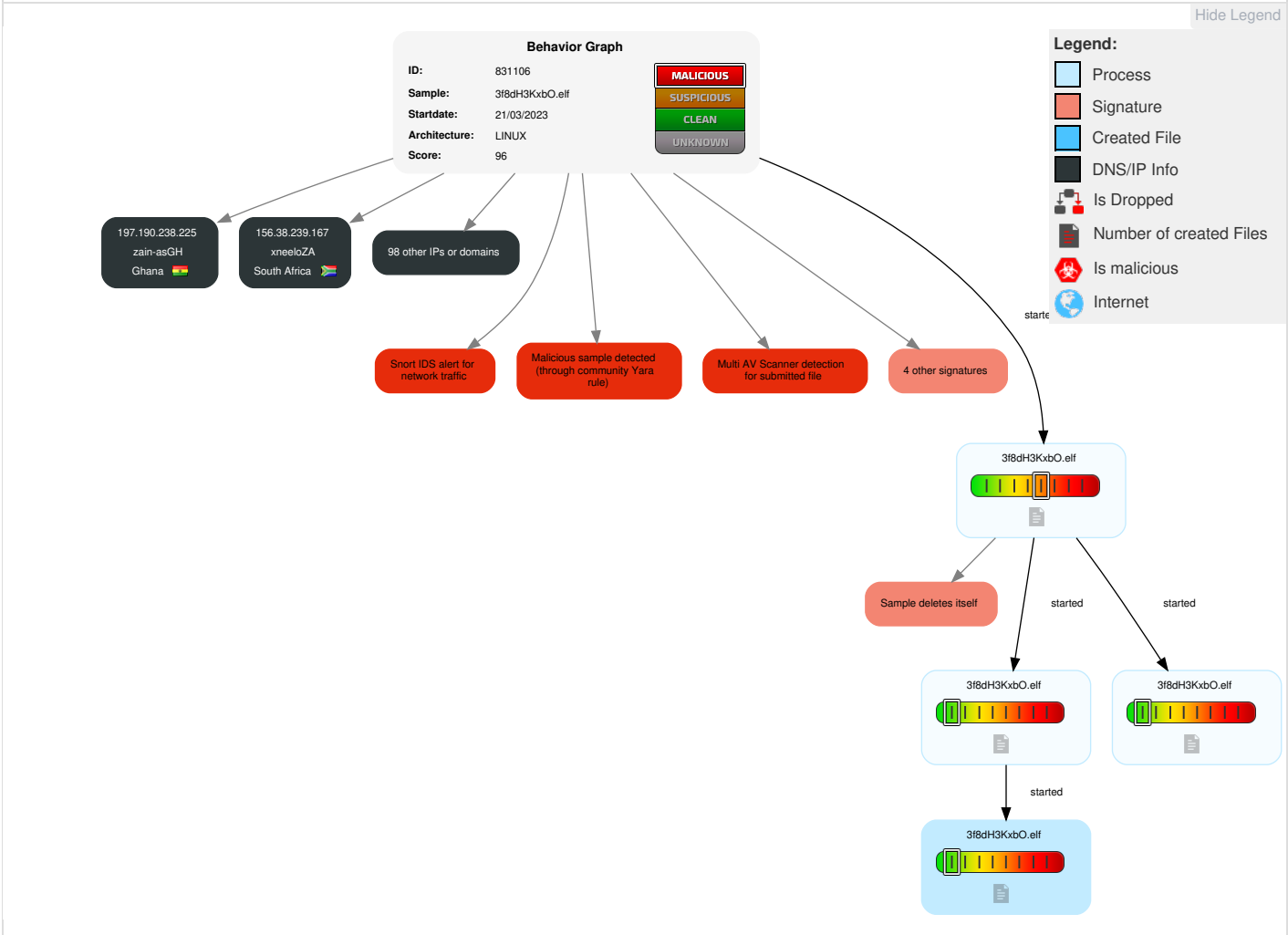
Copyright Joe Security LLC 2023

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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	2 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
3f8dH3KxbO.elf	46%	ReversingLabs	Linux.Trojan.Mirai	

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link
3f8dH3KxbO.elf	42%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

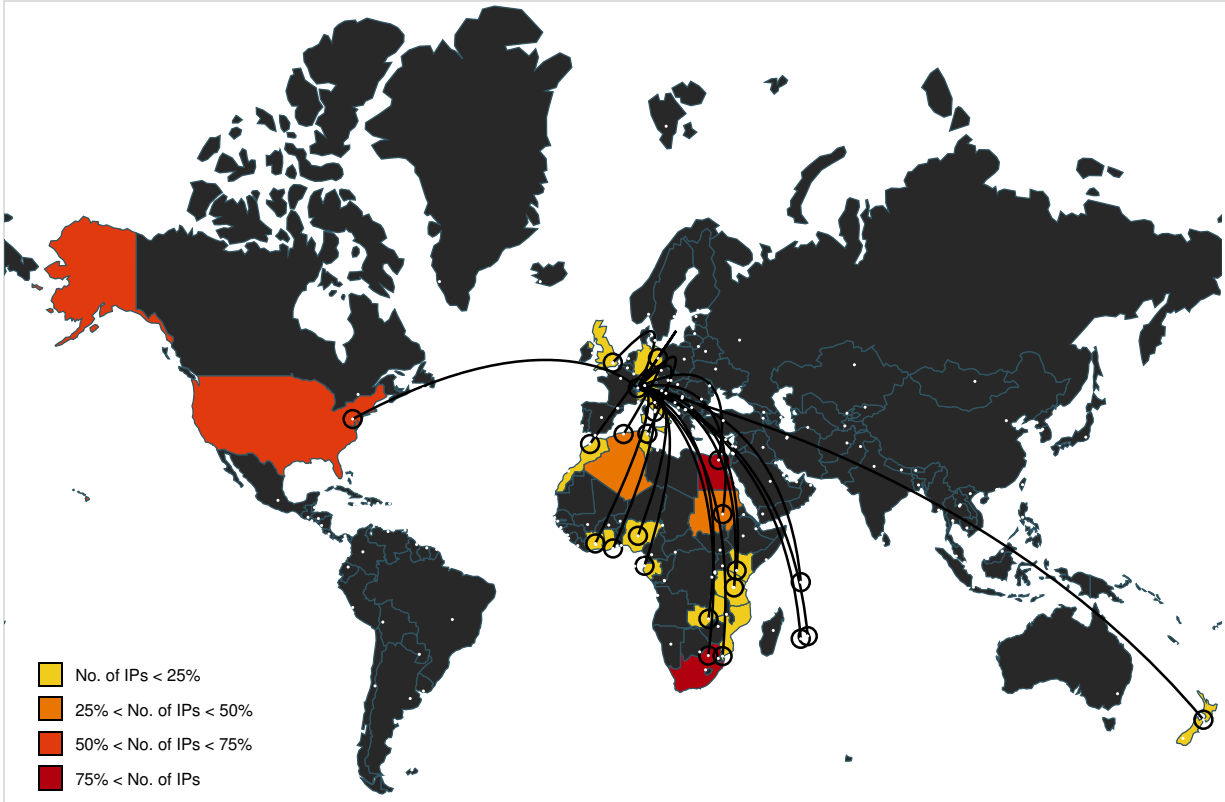
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.131.5.125	unknown	Morocco		6713	IAM-ASMA	false
156.67.84.15	unknown	Germany		47273	KSI-KR-ASPL	false
102.151.100.161	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
41.240.39.15	unknown	Sudan		36998	SDN-MOBITELSD	false
197.231.214.201	unknown	unknown		36974	AFNET-ASCI	false
102.35.244.95	unknown	Reunion		37002	ReunicableRE	false
41.113.110.238	unknown	South Africa		16637	MTNNS-ASZA	false

Copyright Joe Security LLC 2023

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.7.73.38	unknown	United States		29975	VODACOM-ZA	false
154.31.65.173	unknown	United States		174	COGENT-174US	false
154.219.20.176	unknown	Seychelles		26484	IKGUL-26484US	false
154.233.4.156	unknown	Cote D'ivoire		36974	AFNET-ASCI	false
154.64.230.200	unknown	United States		174	COGENT-174US	false
102.191.160.210	unknown	Egypt		24835	RAYA-ASEG	false
197.96.173.28	unknown	South Africa		3741	ISZA	false
102.74.121.109	unknown	Morocco		6713	IAM-ASMA	false
197.179.205.74	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
41.119.144.198	unknown	South Africa		16637	MTNNS-ASZA	false
41.101.212.198	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.95.142.127	unknown	Sudan		36998	SDN-MOBITELSD	false
41.60.37.73	unknown	Mauritius		30969	ZOL-ASGB	false
154.189.85.215	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.21.203.55	unknown	South Africa		36994	Vodacom-VBZA	false
154.248.34.181	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.21.245.107	unknown	United States		17113	AS-TIERP-17113US	false
154.3.74.152	unknown	United States		174	COGENT-174US	false
41.158.217.95	unknown	Gabon		16058	Gabon-TelecomGA	false
156.92.190.242	unknown	United States		10695	WAL-MARTUS	false
102.112.147.76	unknown	Mauritius		23889	MauritiusTelecomMU	false
102.118.234.60	unknown	Mauritius		23889	MauritiusTelecomMU	false
41.193.111.25	unknown	South Africa		11845	Vox-TelecomZA	false
154.104.45.65	unknown	Tunisia		37693	TUNISIANATN	false
156.192.53.245	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.64.208.79	unknown	Egypt		36992	ETISALAT-MISREG	false
156.38.239.167	unknown	South Africa		37153	xneeloZA	false
156.208.228.196	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.157.29.91	unknown	South Africa		37168	CELL-CZA	false
154.75.225.26	unknown	Tanzania United Republic of		37035	MIC-ASTZ	false
197.255.83.89	unknown	Ghana		37074	UG-ASGH	false
197.190.238.225	unknown	Ghana		37140	zain-asGH	false
102.94.133.183	unknown	Nigeria		37075	ZAINUGASUG	false
102.124.182.193	unknown	Sudan		36972	MTNSD	false
154.101.208.19	unknown	Sudan		36998	SDN-MOBITELSD	false
156.78.238.80	unknown	United States		18862	NCS-HEALTHCAREUS	false
156.69.42.178	unknown	New Zealand		297	AS297US	false
41.183.48.215	unknown	South Africa		37028	FNBCONNECTZA	false
102.123.192.245	unknown	Sudan		36972	MTNSD	false
41.201.246.154	unknown	Algeria		36947	ALGTEL-ASDZ	false
154.187.179.105	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.122.135.251	unknown	Egypt		36992	ETISALAT-MISREG	false
154.48.159.84	unknown	United States		203499	WI-NET-SOLIS-ASES	false
41.73.250.186	unknown	Nigeria		16284	UNSPECIFIEDNG	false
197.240.45.188	unknown	unknown		37705	TOPNETTN	false
102.227.2.93	unknown	unknown		36926	CKL1-ASNKE	false
154.7.198.41	unknown	United States		174	COGENT-174US	false
197.240.178.134	unknown	unknown		37705	TOPNETTN	false
102.215.238.72	unknown	unknown		36926	CKL1-ASNKE	false
41.77.133.223	unknown	Mozambique		37110	moztel-asMZ	false
156.149.192.241	unknown	New Zealand		137	ASGARRConsortiumGARREU	false
102.56.184.23	unknown	Egypt		36992	ETISALAT-MISREG	false
197.226.239.39	unknown	Mauritius		23889	MauritiusTelecomMU	false
154.172.76.132	unknown	Ghana		30986	SCANCOMGH	false
41.157.30.26	unknown	South Africa		37168	CELL-CZA	false
156.197.159.190	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.138.47.129	unknown	United States		29975	VODACOM-ZA	false
156.14.244.252	unknown	Italy		137	ASGARRConsortiumGARREU	false

Copyright Joe Security LLC 2023

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.251.50.153	unknown	Sudan		37197	SUDRENSD	false
41.195.148.72	unknown	South Africa		16637	MTNNS-ASZA	false
41.27.126.231	unknown	South Africa		29975	VODACOM-ZA	false
154.248.156.19	unknown	Algeria		36947	ALGTEL-ASDZ	false
102.158.159.135	unknown	Tunisia		37705	TOPNETTN	false
197.12.117.100	unknown	Tunisia		37703	ATLAXTN	false
197.255.13.183	unknown	Nigeria		35074	COBRANET-ASLB	false
102.56.135.23	unknown	Egypt		36992	ETISALAT-MISREG	false
41.131.254.160	unknown	Egypt		24863	LINKdotNET-ASEG	false
154.134.179.153	unknown	Egypt		37069	MOBINILEG	false
102.76.172.183	unknown	Morocco		6713	IAM-ASMA	false
156.48.59.176	unknown	United Kingdom		29975	VODACOM-ZA	false
41.179.39.151	unknown	Egypt		24863	LINKdotNET-ASEG	false
102.40.143.241	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.149.186.147	unknown	South Africa		5713	SAIX-NETZA	false
102.72.163.70	unknown	Morocco		6713	IAM-ASMA	false
156.85.165.199	unknown	United States		10695	WAL-MARTUS	false
41.30.144.251	unknown	South Africa		29975	VODACOM-ZA	false
154.155.93.132	unknown	Kenya		36926	CKL1-ASNKE	false
156.80.19.43	unknown	United States		393649	BOOZ-AS2US	false
41.51.169.87	unknown	South Africa		37168	CELL-CZA	false
197.151.20.192	unknown	Egypt		37069	MOBINILEG	false
102.216.30.80	unknown	unknown		36926	CKL1-ASNKE	false
41.80.99.71	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
154.74.68.104	unknown	Tanzania United Republic of		37035	MIC-ASTZ	false
41.239.14.29	unknown	Egypt		8452	TE-ASTE-ASEG	false
154.245.126.240	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.160.163.9	unknown	Egypt		36992	ETISALAT-MISREG	false
154.131.114.70	unknown	Egypt		37069	MOBINILEG	false
156.55.40.30	unknown	United States		22146	LANDAMUS	false
156.48.59.169	unknown	United Kingdom		29975	VODACOM-ZA	false
197.207.57.210	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.230.19.149	unknown	Seychelles		135357	SKHT-ASShenzhenKatherineHengTechnologyInformationCo	false
197.228.192.238	unknown	South Africa		37251	TELKOMMOBILEZA	false
41.133.122.213	unknown	South Africa		10474	OPTINETZA	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 (GNU/Linux), statically linked, no section header
Entropy (8bit):	7.923069223559225
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	3f8dH3KxbO.elf
File size:	24880
MD5:	b2c7b530dda1e86285699cc34666bcf7
SHA1:	5a4fa656800a06fbd556084b2c878469fbe1ce47
SHA256:	792754c6e660335fe22a3099a2953c7d51b9b5c9eb6bed989790393ba1ef8ce9
SHA512:	631e26ad79486e33e7165e956615e806ef844ed5aa8b8c7c55b4466c8919b12e2d787a240e631d252978f8ba4747e9046d297432ce30d0a3f8d267363940f59a
SSDEEP:	768:eM6CVAD/s90GDQIRzaRtcSo73WnbcuyD7URQRjT:YCVA41DQIGRu3Wnouy8Ry3
TLSH:	9BB2E17960A93A15D5EA617A086EBFDF2195C70F520996F3C9F4B6135087FB02C2C0DA
File Content Preview:	.ELF.....@^..4.....4. ...(.....4`..4`.....g...g.....Q.td.....-].UPX!.....0...0.....T.....?..k.I/.j....\.d*nlz.e..../:..5.KT7S..RmC..G.....O.H..!..g.....C..

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:	

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0xc01000	0xc01000	0x6034	0x6034	7.9264	0x5	R E	0x1000		
LOAD	0x7e0	0x80567e0	0x80567e0	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Copyright Joe Security LLC 2023

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2341.35.80.175 37350372152835222 03/21/23-03:30:32.951807	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	37350	37215	192.168.2.23	41.35.80.175
192.168.2.23156.247.27.1 873388372152835222 03/21/23-03:30:43.507431	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33884	37215	192.168.2.23	156.247.27.187
192.168.2.23154.38.230.95 48244372152835222 03/21/23-03:30:28.214197	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	48244	37215	192.168.2.23	154.38.230.95
192.168.2.23197.246.192.49 4086372152835222 03/21/23-03:30:30.427381	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	40868	37215	192.168.2.23	197.246.192.49
192.168.2.23156.226.11.1 035914237152835222 03/21/23-03:30:48.796217	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	59142	37215	192.168.2.23	156.226.11.103
192.168.2.23156.254.44.2 455129237152835222 03/21/23-03:30:30.585388	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51292	37215	192.168.2.23	156.254.44.245
192.168.2.23154.213.189.79 3561837152835222 03/21/23-03:30:38.901778	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	35618	37215	192.168.2.23	154.213.189.79
192.168.2.23154.211.47.1 1446036372152835222 03/21/23-03:30:28.311917	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46036	37215	192.168.2.23	154.211.47.114
192.168.2.23156.254.89.3 942060372152835222 03/21/23-03:30:35.326766	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	42060	37215	192.168.2.23	156.254.89.39
192.168.2.23156.227.245.4 649918372152835222 03/21/23-03:30:36.616130	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	49918	37215	192.168.2.23	156.227.245.46
192.168.2.2341.236.89.94 5968372152835222 03/21/23-03:30:35.158451	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45968	37215	192.168.2.23	41.236.89.9
192.168.2.23154.201.25.1 2433512372152835222 03/21/23-03:30:39.166861	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33512	37215	192.168.2.23	154.201.25.124
192.168.2.23154.208.147.24 9474468372152835222 03/21/23-03:30:26.768093	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	47468	37215	192.168.2.23	154.208.147.249
192.168.2.2341.43.16.185 51276372152835222 03/21/23-03:30:38.721581	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	51276	37215	192.168.2.23	41.43.16.185
192.168.2.23156.254.66.6 360202372152835222 03/21/23-03:30:39.166793	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60202	37215	192.168.2.23	156.254.66.63
192.168.2.23154.216.21.9 338882372152835222 03/21/23-03:30:42.237111	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	38882	37215	192.168.2.23	154.216.21.93
192.168.2.23156.254.58.1 2744726372152835222 03/21/23-03:30:39.695821	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44726	37215	192.168.2.23	156.254.58.127

TCP Packets

System Behavior

Analysis Process: 3f8dH3KxbO.elf PID: **6229**, Parent PID: **6131**

General

Start time:	03:30:08
Start date:	21/03/2023
Path:	/tmp/3f8dH3KxbO.elf
Arguments:	/tmp/3f8dH3KxbO.elf
File size:	24880 bytes
MD5 hash:	b2c7b530dda1e86285699cc34666bcf7

File Activities

File Deleted

Analysis Process: 3f8dH3KxbO.elf PID: **6230**, Parent PID: **6229**

General

Start time:	03:30:08
Start date:	21/03/2023
Path:	/tmp/3f8dH3KxbO.elf
Arguments:	n/a
File size:	24880 bytes
MD5 hash:	b2c7b530dda1e86285699cc34666bcf7

Analysis Process: 3f8dH3KxbO.elf PID: **6232**, Parent PID: **6229**

General

Start time:	03:30:08
Start date:	21/03/2023
Path:	/tmp/3f8dH3KxbO.elf
Arguments:	n/a
File size:	24880 bytes
MD5 hash:	b2c7b530dda1e86285699cc34666bcf7

Analysis Process: 3f8dH3KxbO.elf PID: **6233**, Parent PID: **6232**

General

Start time:	03:30:08
Start date:	21/03/2023
Path:	/tmp/3f8dH3KxbO.elf
Arguments:	n/a
File size:	24880 bytes
MD5 hash:	b2c7b530dda1e86285699cc34666bcf7

File Activities

File Read

Directory Enumerated

Copyright Joe Security LLC 2023