ID: 830702
Sample Name: v8OWS3Ylfj.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:12:59
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Linux Analysis Report v8OWS3Ylfj.elf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Warnings 4
Runtime Messages 4
Process Tree 5
Malware Threat Intel 5
Yara Signatures 5
Initial Sample 5
Memory Dumps 6
Snort Signatures 7
Joe Sandbox Signatures 8
AV Detection 8
Networking 8
System Summary 8
Hooking and other Techniques for Hiding and Protection 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Malware Configuration 9
Behavior Graph 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 10
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 13
General 13
Static ELF Info 13
ELF header 13
Sections 14
Program Segments 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 15
DNS Queries 15
DNS Answers 15
System Behavior 15
Analysis Process: v8OWS3Ylfj.elf PID: 6223, Parent PID: 6125 15
General 15
Analysis Process: v8OWS3Ylfj.elf PID: 6224, Parent PID: 6223 15
General 15
Analysis Process: sh PID: 6224, Parent PID: 6223 15
General 15
File Activities 16
File Read 16
Analysis Process: v8OWS3Ylfj.elf PID: 6225, Parent PID: 6223 16
General 16
Analysis Process: v8OWS3Ylfj.elf PID: 6226, Parent PID: 6225 16
General 16
File Activities 16
File Read 16
Directory Enumerated 16
Analysis Process: v8OWS3Ylfj.elf PID: 6227, Parent PID: 6225 16
General 16

Linux Analysis Report

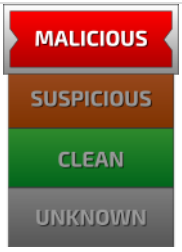
v8OWS3Ylfj.elf

Overview

General Information

Sample Name:	v8OWS3Ylfj.elf
Original Sample Name:	2b318e2fa59dc..
Analysis ID:	830702
MD5:	2b318e2fa59dc..
SHA1:	d5bf527325fbfb..
SHA256:	7bbce804ece6...
Tags:	32 elf intel mirai
Infos:	

Detection



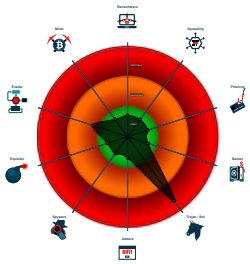
Mirai, Moobot

Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through...
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Yara detected Moobot
- Snort IDS alert for network traffic
- Uses known network protocols on n...
- Machine Learning detection for sam...
- Performs DNS queries to domains w...
- Yara signature match
- Sample has stripped symbol table
- 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:	830702
Start date and time:	2023-03-20 16:12:59 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 1s
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:	v8OWS3Ylfj.elf
Original Sample Name:	2b318e2fa59dccaa45cc59c5fea7e082.elf
Detection:	MAL
Classification:	mal92.troj.linELF@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/v8OWS3Ylfj.elf
PID:	6223
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	done.

Standard Error:	sh: 1: Syntax error: Unterminated quoted string

Process Tree

- **system is lnxubuntu20**
- v8OWS3Ylfj.elf (PID: 6223, Parent: 6125, MD5: 2b318e2fa59dccaa45cc59c5fea7e082) Arguments: /tmp/v8OWS3Ylfj.elf
  - v8OWS3Ylfj.elf New Fork (PID: 6224, Parent: 6223)
  - sh (PID: 6224, Parent: 6223, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv \"/tmp/v8OWS3Ylfj.elf \\xdc\u0420\\xff\\x84\\x88&bin/watchdog; chmod 777 bin/watchdog"
  - v8OWS3Ylfj.elf New Fork (PID: 6225, Parent: 6223)
    - v8OWS3Ylfj.elf New Fork (PID: 6226, Parent: 6225)
    - v8OWS3Ylfj.elf New Fork (PID: 6227, Parent: 6225)
- **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
v8OWS3Ylfj.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
v8OWS3Ylfj.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
v8OWS3Ylfj.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xb9b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xb9cc:$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 • 0xb9e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xb9f4:$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 • 0xba08:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba1c:$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 • 0xba30:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba44:$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 • 0xba58:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba6c:$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 • 0xba80:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba94:$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 • 0xbaa8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbabc:$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 • 0xbad0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbae4:$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 • 0xbaf8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbb0c:$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 • 0xbb20:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbb34:$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 • 0xbb48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
v8OWS3Ylfj.elf	Linux_Trojan_Gafgyt_5bf62ce4	unknown	unknown	• 0x97b1:$a: 89 E5 56 53 31 F6 8D 45 10 83 EC 10 89 45 F4 8B 55 F4 46 8D
v8OWS3Ylfj.elf	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x3d80:$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
6223.1.0000000008048000.0000000008056000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6223.1.0000000008048000.0000000008056000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6223.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xb9b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xb9cc:$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 • 0xb9e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xb9f4:$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 • 0xba08:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba1c:$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 • 0xba30:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba44:$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 • 0xba58:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba6c:$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 • 0xba80:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xba94:$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 • 0xbaa8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbabc:$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 • 0xbad0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbae4:$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 • 0xbaf8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbb0c:$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 • 0xbb20:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbb34:$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 • 0xbb48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6223.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Gafgyt_5bf62ce4	unknown	unknown	• 0x97b1:$a: 89 E5 56 53 31 F6 8D 45 10 83 EC 10 89 45 F4 8B 55 F4 46 8D
6223.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x3d80:$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: 195.133.40.202

Timestamp:	192.168.2.23195.133.40.20236176569992030490 03/20/23-16:13:48.596290
SID:	2030490
Source Port:	36176
Destination Port:	56999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response - Source IP: 195.133.40.202 - Destination IP: 192.168.2.23

Timestamp:	195.133.40.202192.168.2.2356999361762030489 03/20/23-16:13:53.166618
SID:	2030489
Source Port:	56999
Destination Port:	36176
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: 195.164.211.50

Timestamp:	192.168.2.23195.164.211.5057976372152835222 03/20/23-16:13:57.691757
SID:	2835222
Source Port:	57976

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
- Uses known network protocols on non-standard ports
- Performs DNS queries to domains with low reputation

System Summary

- Malicious sample detected (through community Yara rule)

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

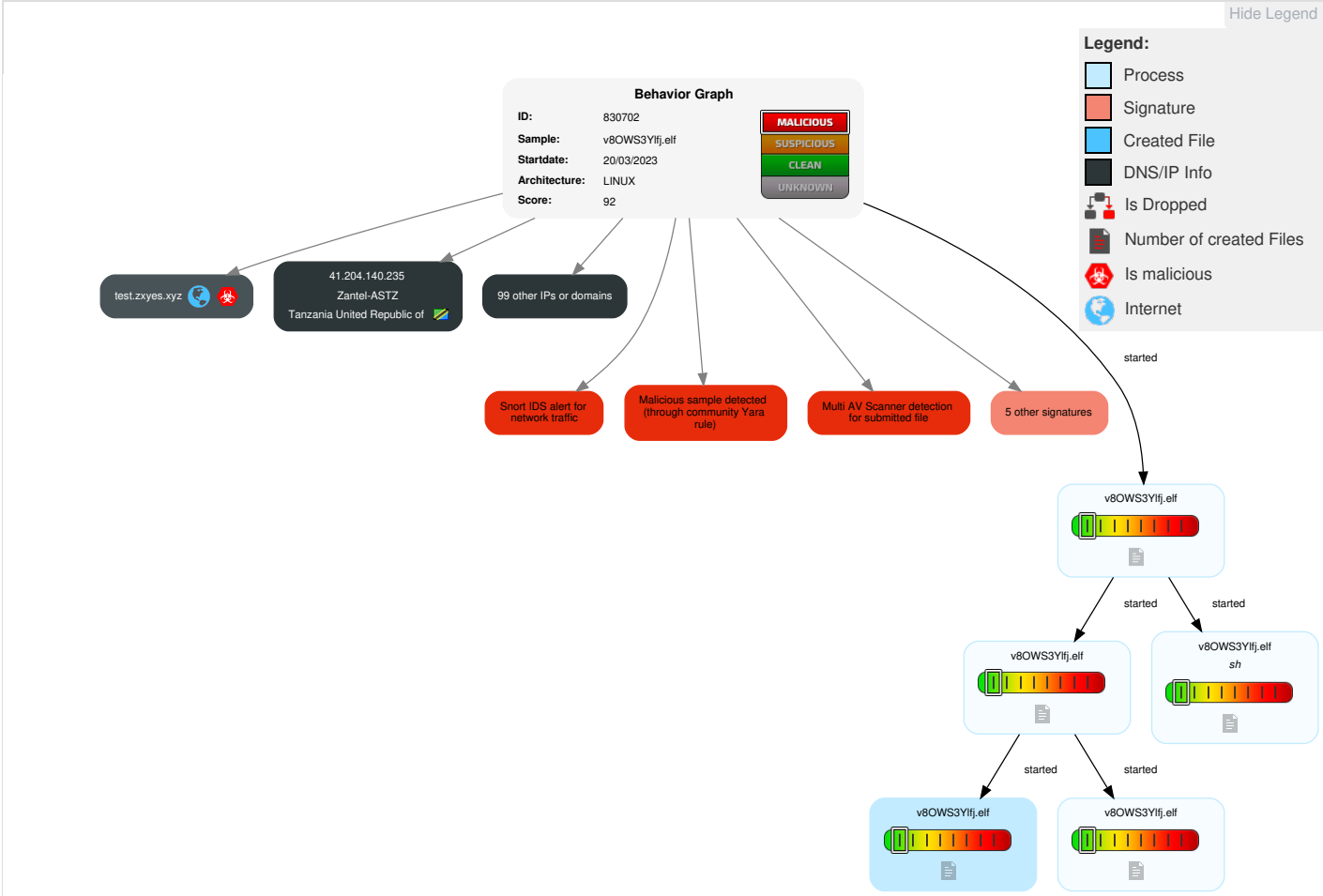
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	Path Interception	1 Scripting	1 OS Credential Dumping	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	Rootkit	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)	Obfuscated Files or Information	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
v8OWS3Ylfj.elf	57%	Virustotal		Browse
v8OWS3Ylfj.elf	59%	ReversingLabs	Linux.Trojan.LnxMirai	
v8OWS3Ylfj.elf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
test.zxyes.xyz	2%	Virustotal		Browse

URLs

No Antivirus matches

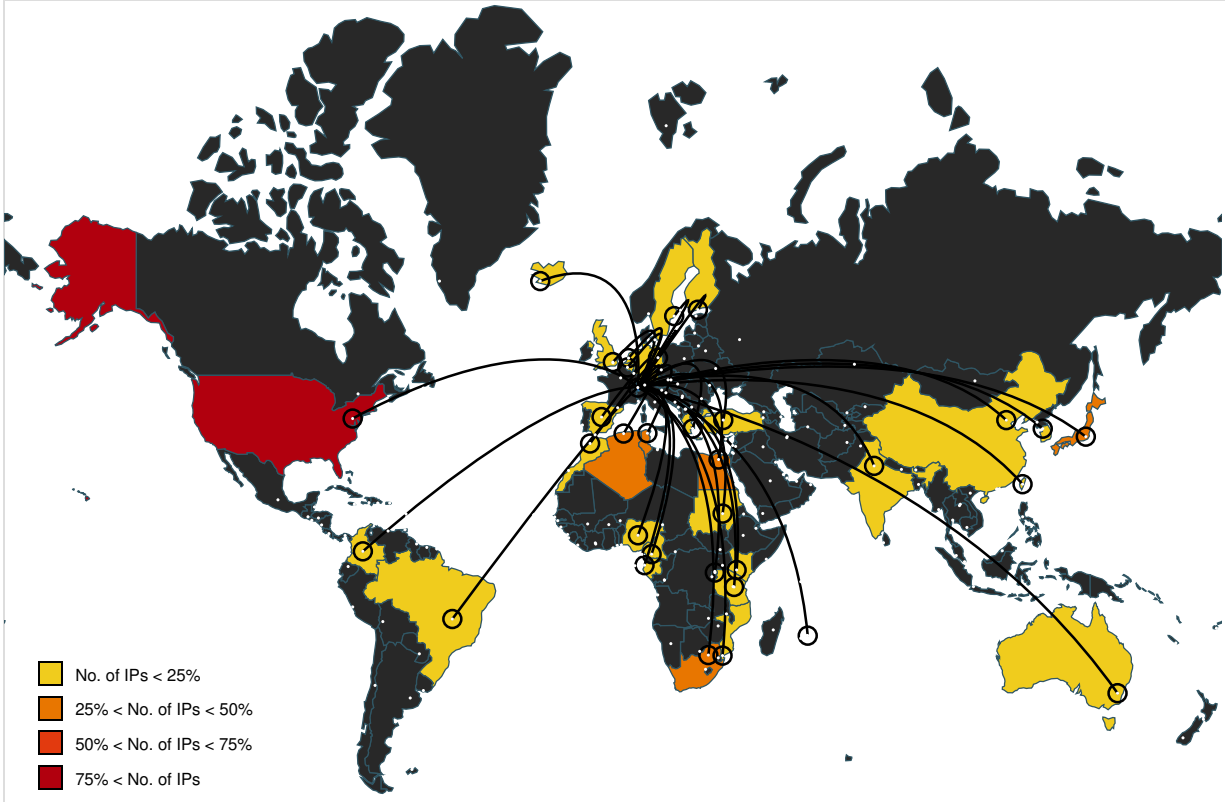
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
test.zxyes.xyz	195.133.40.202	true	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.116.97.50	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.122.250.100	unknown	South Africa		16637	MTNNS-ASZA	false
41.158.229.80	unknown	Gabon		16058	Gabon-TelecomGA	false
157.202.176.43	unknown	United States		1759	TSF-IP-CORETeliaFinlandOyjEU	false
162.153.29.187	unknown	United States		10796	TWC-10796-MIDWESTUS	false
41.78.111.29	unknown	Sudan		37211	MAX-NET-FOR-INTERNET-SERVICESSD	false
157.57.242.60	unknown	United States		3598	MICROSOFT-CORP-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.86.112.180	unknown	Brazil		21612	FUNDACAOINSTITUTOOSWALDOCRUZBR	false
157.71.207.91	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
197.206.187.63	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.203.147.109	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.112.136.32	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
154.241.231.35	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.254.120.33	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
157.202.176.45	unknown	United States		1759	TSF-IP-CORETeliaFinlandOyjEU	false
157.240.97.103	unknown	United States		32934	FACEBOOKUS	false
191.71.196.136	unknown	Colombia		26611	COMCELSACO	false
41.240.27.36	unknown	Sudan		36998	SDN-MOBITELSD	false
90.158.197.168	unknown	Turkey		9021	ISNETTR	false
159.65.206.40	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
1.41.26.120	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
157.229.129.223	unknown	United States		122	UPMC-AS122US	false
157.80.125.244	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
41.214.230.4	unknown	Morocco		36925	ASMediMA	false
157.62.20.95	unknown	United States		22192	SSHENETUS	false
157.74.162.171	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
146.233.213.243	unknown	United States		53527	COUNTY-OF-LOS-ANGELES-SHERIFFS-DEPARTMENTUS	false
197.30.214.19	unknown	Tunisia		37492	ORANGE-TN	false
41.240.108.63	unknown	Sudan		36998	SDN-MOBITELSD	false
102.105.183.19	unknown	Tunisia		37693	TUNISIANATN	false
197.221.108.123	unknown	South Africa		37236	Reflex-SolutionsZA	false
41.102.124.94	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.186.110.64	unknown	Rwanda		36890	MTNRW-ASNRW	false
41.158.143.123	unknown	Gabon		16058	Gabon-TelecomGA	false
41.108.235.41	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.91.221.202	unknown	United States		1767	ILIGHT-NETUS	false
197.23.201.49	unknown	Tunisia		37693	TUNISIANATN	false
108.13.86.247	unknown	United States		5650	FRONTIER-FRTRUS	false
77.226.252.166	unknown	Spain		12430	VODAFONE_ESES	false
146.124.59.136	unknown	Greece		3260	INTRACOMGR	false
41.232.55.184	unknown	Egypt		8452	TE-ASTE-ASEG	false
219.202.15.245	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
157.148.116.78	unknown	China		136958	UNICOM-GUANGZHOU-IDCChinaUnicomGuangdongIPnetworkCN	false
157.24.67.210	unknown	Finland		1741	FUNETASFI	false
41.244.252.243	unknown	Cameroon		37620	VIETTEL-CM-ASCM	false
41.23.191.240	unknown	South Africa		29975	VODACOM-ZA	false
41.47.7.55	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.180.119.67	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
157.157.39.79	unknown	Iceland		6677	ICENET-AS1IS	false
157.252.160.112	unknown	United States		3592	TRINCOLL-ASUS	false
197.58.116.239	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.158.15.113	unknown	Mozambique		30619	TDM-ASMZ	false
197.53.119.213	unknown	Egypt		8452	TE-ASTE-ASEG	false
211.175.167.21	unknown	Korea Republic of		9457	DREAMX-ASDREAMLINECOKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.199.145.238	unknown	Germany		25560	RHTEC-ASrh-tecIPBackboneDE	false
157.227.16.98	unknown	Australia		4704	SANNETRakutenMobileIncJP	false
1.170.61.234	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
197.46.254.215	unknown	Egypt		8452	TE-ASTE-ASEG	false
121.94.172.86	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
132.147.143.250	unknown	United States		11776	ATLANTICBB-JOHNSTOWNUS	false
197.42.235.247	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.204.140.235	unknown	Tanzania United Republic of		36930	Zantel-ASTZ	false
213.89.240.214	unknown	Sweden		39651	COMHEM-SWEDENSE	false
191.41.153.32	unknown	Brazil		7738	TelemarNorteLesteSABR	false
197.25.176.170	unknown	Tunisia		37671	GLOBALNET-ASTN	false
197.225.3.139	unknown	Mauritius		23889	MauritiusTelecomMU	false
110.251.172.54	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
197.53.119.223	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.164.123.130	unknown	Belgium		49964	VERIXI-BACKUPNETWORKBE	false
197.89.135.46	unknown	South Africa		10474	OPTINETZA	false
217.8.241.179	unknown	United Kingdom		20738	GD-EMEA-DC-LD5GB	false
41.221.123.188	unknown	unknown		36974	AFNET-ASCI	false
157.74.88.27	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
41.216.185.187	unknown	South Africa		40065	CNSERVERSUS	false
41.91.9.71	unknown	Egypt		33771	SAFARICOM-LIMITEDKE	false
197.211.78.67	unknown	South Africa		29918	IMPOL-ASNZA	false
157.45.145.241	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
197.174.209.103	unknown	South Africa		37168	CELL-CZA	false
197.204.101.21	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.98.89.102	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.31.140.147	unknown	Tunisia		37492	ORANGE-TN	false
208.229.94.48	unknown	United States		4208	THE-ISERV-COMPANYUS	false
197.130.198.23	unknown	Morocco		6713	IAM-ASMA	false
41.228.168.97	unknown	Tunisia		37492	ORANGE-TN	false
197.139.229.118	unknown	Kenya		36914	KENET-ASKE	false
157.180.240.213	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
41.11.91.70	unknown	South Africa		29975	VODACOM-ZA	false
157.149.244.2	unknown	United States		3464	ASC-NETUS	false
4.173.232.107	unknown	United States		3356	LEVEL3US	false
41.217.30.150	unknown	Nigeria		37340	SpectranetNG	false
157.240.98.11	unknown	United States		32934	FACEBOOKUS	false
135.239.89.179	unknown	United States		10455	LUCENT-CIOUS	false
157.54.149.249	unknown	United States		3598	MICROSOFT-CORP-ASUS	false
197.88.158.211	unknown	South Africa		10474	OPTINETZA	false
152.217.237.100	unknown	United States		30313	IRSUS	false
197.125.162.90	unknown	Egypt		36992	ETISALAT-MISREG	false
157.56.241.225	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
197.62.75.231	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.241.76.144	unknown	United States		32934	FACEBOOKUS	false
145.149.26.3	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	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):	6.548832915017976
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	v8OWS3Ylfj.elf
File size:	55632
MD5:	2b318e2fa59dccaa45cc59c5fea7e082
SHA1:	d5bf527325fbfbda5d26272bb88874bc504dd260
SHA256:	7bbce804ece6b26f0fcf2937fd5217518848f044c95cc6d033f5a08f04598a06
SHA512:	cb9c55ee85b5d0a8d881201cd99b4b998353e58239350d597db1bb5a2ce09bde7a7e72a941a9c6b18fba8cf43a86e837297ca33dfcd8913e86c7715ca4972f66
SSDEEP:	1536:JeESt/basV2rcZhG6ySN7na65lSR9zWOIaEjrqMds:JeESt/basVTgS7na65QRVtXESS
TLSH:	A9436BC4F643D8F5EC8705702077FB379B72E1E922A8D647D3B4D932AC52651EA06A8C
File Content Preview:	.ELF.....d...4.....4. ...(.....e...e.....H(.....Q.td.....U..S.....w....h..... []...$.....U.....=.g...t..5....$e.....$e.....u.....t....h.T.....

Static ELF Info

ELF header

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

ELF header	
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	0xb436	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80534e6	0xb4e6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8053500	0xb500	0x1ffc	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8056500	0xd500	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8056508	0xd508	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8056520	0xd520	0x260	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8056780	0xd780	0x25c8	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xd780	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	0xd4fc	0xd4fc	6.5875	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xd500	0x8056500	0x8056500	0x280	0x2848	3.4669	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

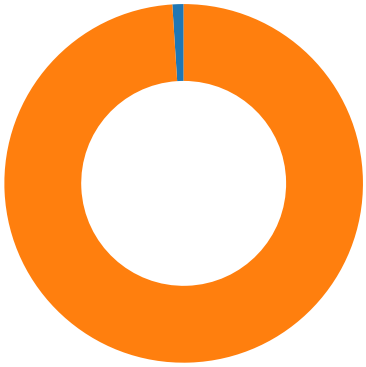
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23195.133.40.202361765699920304900 03/20/23-16:13:48.596290	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	36176	56999	192.168.2.23	195.133.40.202
195.133.40.202192.168.2.235699936176203048900 03/20/23-16:13:53.166618	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	36176	195.133.40.202	192.168.2.23
192.168.2.23195.164.211.50579763721528352220 03/20/23-16:13:57.691757	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	57976	37215	192.168.2.23	195.164.211.50

Network Port Distribution

Total Packets: 99

- 37215 undefined
- 443 (HTTPS)



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:13:48.544802904 CET	192.168.2.23	8.8.8.8	0x5faf	Standard query (0)	test.zxyes.xyz	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 16:13:48.568625927 CET	8.8.8.8	192.168.2.23	0x5faf	No error (0)	test.zxyes.xyz		195.133.40.202	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: v8OWS3Ylfj.elf PID: 6223, Parent PID: 6125

General

Start time:	16:13:47
Start date:	20/03/2023
Path:	/tmp/v8OWS3Ylfj.elf
Arguments:	/tmp/v8OWS3Ylfj.elf
File size:	55632 bytes
MD5 hash:	2b318e2fa59dccaa45cc59c5fea7e082

Analysis Process: v8OWS3Ylfj.elf PID: 6224, Parent PID: 6223

General

Start time:	16:13:47
Start date:	20/03/2023
Path:	/tmp/v8OWS3Ylfj.elf
Arguments:	n/a
File size:	55632 bytes
MD5 hash:	2b318e2fa59dccaa45cc59c5fea7e082

Analysis Process: sh PID: 6224, Parent PID: 6223

General

Start time:	16:13:47
Start date:	20/03/2023

Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv \"/tmp/v8OWS3Ylfj.elf \\xdc\u0420\\xff\\x84\\x88&bin/watchdog; chmod 777 bin/watchdog"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: v8OWS3Ylfj.elf PID: **6225**, Parent PID: **6223**

General

Start time:	16:13:48
Start date:	20/03/2023
Path:	/tmp/v8OWS3Ylfj.elf
Arguments:	n/a
File size:	55632 bytes
MD5 hash:	2b318e2fa59dccaa45cc59c5fea7e082

Analysis Process: v8OWS3Ylfj.elf PID: **6226**, Parent PID: **6225**

General

Start time:	16:13:48
Start date:	20/03/2023
Path:	/tmp/v8OWS3Ylfj.elf
Arguments:	n/a
File size:	55632 bytes
MD5 hash:	2b318e2fa59dccaa45cc59c5fea7e082

File Activities

File Read

Directory Enumerated

Analysis Process: v8OWS3Ylfj.elf PID: **6227**, Parent PID: **6225**

General

Start time:	16:13:48
Start date:	20/03/2023
Path:	/tmp/v8OWS3Ylfj.elf
Arguments:	n/a
File size:	55632 bytes
MD5 hash:	2b318e2fa59dccaa45cc59c5fea7e082