ID: 553493
Sample Name: 9Q1fc1TZq4
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:38:33
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

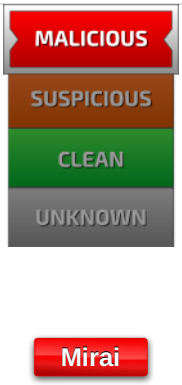
Linux Analysis Report 9Q1fc1TZq4

Overview

General Information

Sample Name:	9Q1fc1TZq4
Analysis ID:	553493
MD5:	b192ed1edacfafe..
SHA1:	0a3451997f43964.
SHA256:	b41bbb2bcc0d31..
Tags:	32 elf mirai sparc
Infos:	

Detection

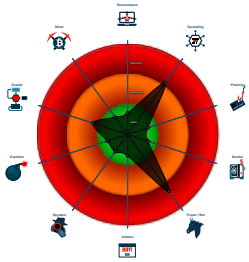


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill multiple processe...
- Sample has stripped symbol table
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553493
Start date:	15.01.2022
Start time:	01:38:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9Q1fc1TZq4
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
Detection:	MAL
Classification:	mal72.spre.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

Copyright Joe Security LLC 2022

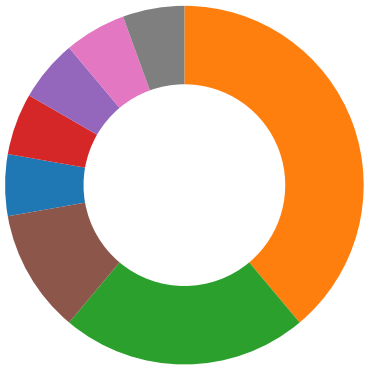
- **system is lnxubuntu20**
- 9Q1fc1TZq4 (PID: 5222, Parent: 5109, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/9Q1fc1TZq4
  - 9Q1fc1TZq4 New Fork (PID: 5224, Parent: 5222)
    - 9Q1fc1TZq4 New Fork (PID: 5241, Parent: 5224)
    - 9Q1fc1TZq4 New Fork (PID: 5243, Parent: 5224)
      - 9Q1fc1TZq4 New Fork (PID: 5245, Parent: 5243)
        - 9Q1fc1TZq4 New Fork (PID: 5251, Parent: 5245)
        - 9Q1fc1TZq4 New Fork (PID: 5253, Parent: 5245)
      - 9Q1fc1TZq4 New Fork (PID: 5248, Parent: 5243)
      - 9Q1fc1TZq4 New Fork (PID: 5249, Parent: 5243)
    - 9Q1fc1TZq4 New Fork (PID: 5225, Parent: 5222)
    - 9Q1fc1TZq4 New Fork (PID: 5226, Parent: 5222)
      - 9Q1fc1TZq4 New Fork (PID: 5229, Parent: 5226)
        - 9Q1fc1TZq4 New Fork (PID: 5259, Parent: 5229)
        - 9Q1fc1TZq4 New Fork (PID: 5261, Parent: 5229)
      - 9Q1fc1TZq4 New Fork (PID: 5232, Parent: 5226)
      - 9Q1fc1TZq4 New Fork (PID: 5235, Parent: 5226)
- **cleanup**

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

System Summary:

Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection:

Copyright Joe Security LLC 2022

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

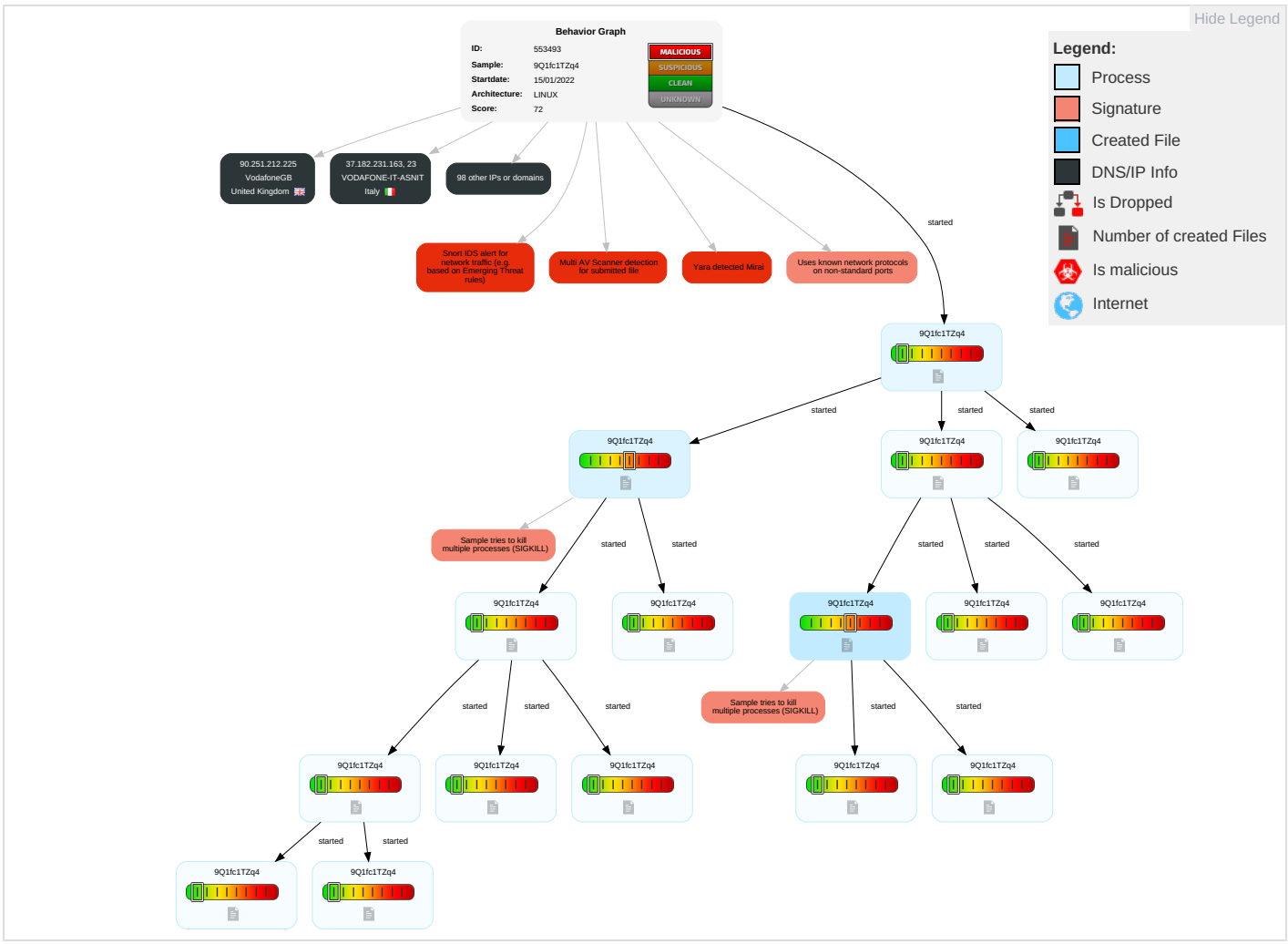
Mitre Att&ck Matrix

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	Direct Volume Access	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
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	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
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	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
9Q1fc1TZq4	52%	Virustotal		Browse
9Q1fc1TZq4	56%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.20.10.19	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
169.59.118.0	unknown	United States		36351	SOFTLAYERUS	false
12.27.146.188	unknown	United States		22024	SPLUNK-WESTUS	false
97.122.201.251	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
92.14.197.234	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
43.200.189.55	unknown	Japan		4249	LILLY-ASUS	false
135.214.247.4	unknown	United States		797	AMERITECH-ASUS	false
181.11.124.63	unknown	Argentina		7303	TelecomArgentinaSAAR	false
148.116.96.162	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
218.247.19.102	unknown	China		17964	DXTNETBeijingDian-Xin-TongNetworkTechnologiesCoLtd	false
92.169.155.202	unknown	France		3215	FranceTelecom-OrangeFR	false
255.11.112.220	unknown	Reserved		unknown	unknown	false
245.3.184.52	unknown	Reserved		unknown	unknown	false
186.218.250.229	unknown	Brazil		28573	CLAROSABR	false
163.1.73.189	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
73.86.243.183	unknown	United States		7922	COMCAST-7922US	false
151.252.218.157	unknown	Germany		34594	OT-ASHR	false
133.70.198.186	unknown	Japan		24268	SAINSNationalUniversityCorporationShizuokaUniversityJ	false
252.36.231.194	unknown	Reserved		unknown	unknown	false
32.185.230.127	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
153.116.140.8	unknown	United States		5501	FRAUNHOFER-CLUSTER-BWResearchInstitutesspreadalloverGe	false
135.41.207.147	unknown	United States		54614	CIKTELECOM-CABLECA	false
196.60.104.159	unknown	unknown		37518	FIBERGRIDSC	false
242.29.155.141	unknown	Reserved		unknown	unknown	false
217.111.58.252	unknown	Germany		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
66.163.200.76	unknown	Canada		15247	RADIANT-VANCOUVERCA	false
242.164.138.231	unknown	Reserved		unknown	unknown	false
145.4.3.32	unknown	Netherlands		702	UUNETUS	false
76.231.211.6	unknown	United States		7018	ATT-INTERNET4US	false
168.43.71.22	unknown	United States		1761	TDIR-CAPNETUS	false
75.229.27.80	unknown	United States		22394	CELLCOUS	false
174.102.62.195	unknown	United States		10796	TWC-10796-MIDWESTUS	false
210.113.80.162	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
217.137.54.23	unknown	United Kingdom		5089	NTLGB	false
152.25.134.106	unknown	United States		81	NCRENUS	false
180.144.209.43	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
121.132.105.18	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
221.182.110.53	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
62.114.184.227	unknown	Egypt		36992	ETISALAT-MISREG	false
173.1.59.247	unknown	United States		26228	SERVEPATHUS	false
20.229.247.195	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
27.117.29.102	unknown	Korea Republic of		17857	NAKDONGDIGITALBUSANNET-AS-KRTBroadKR	false
179.91.90.163	unknown	Brazil		26599	TELEFONICABRASILSABR	false
149.9.8.228	unknown	United States		14987	RETHEMHOSTINGUS	false
9.105.39.192	unknown	United States		3356	LEVEL3US	false
206.208.210.79	unknown	United States		23177	TNB-NETUS	false
164.196.212.57	unknown	United States		2621	DNIC-AS-02621US	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.234.82.181	unknown	Taiwan; Republic of China (ROC)		17710	PIINET-TWPresidentInformationCorpTW	false
167.145.94.0	unknown	United States		25899	LSNETUS	false
218.214.30.213	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	false
173.70.19.21	unknown	United States		701	UUNETUS	false
246.36.186.129	unknown	Reserved		unknown	unknown	false
201.231.42.137	unknown	Argentina		10318	TelecomArgentinaSAAR	false
204.38.223.92	unknown	United States		237	MERIT-AS-14US	false
114.253.184.46	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
53.132.107.174	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
172.73.89.126	unknown	United States		11426	TWC-11426-CAROLINASUS	false
242.199.130.227	unknown	Reserved		unknown	unknown	false
93.207.9.129	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
101.183.140.0	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
187.210.99.34	unknown	Mexico		8151	UninetSAdeCVMX	false
92.239.100.212	unknown	United Kingdom		5089	NTLGB	false
217.4.134.212	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
123.87.18.189	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
111.92.195.214	unknown	Singapore		45814	FARIYA-PKFariyaNetworksPvtLtdPK	false
160.131.191.99	unknown	United States		8103	STATE-OF-FLAUS	false
86.14.109.242	unknown	United Kingdom		5089	NTLGB	false
62.132.145.248	unknown	Germany		286	KPNNL	false
169.236.96.126	unknown	United States		22323	UNIVERSITY-OF-CALIFORNIA-MERCEDUS	false
16.128.90.19	unknown	United States		unknown	unknown	false
48.101.49.65	unknown	United States		2686	ATGS-MMD-ASUS	false
249.210.32.222	unknown	Reserved		unknown	unknown	false
192.208.198.17	unknown	United States		6336	TURN-US-ASNUS	false
24.150.27.121	unknown	Canada		7992	COGECOWAVECA	false
166.8.131.144	unknown	Switzerland		11798	ACEDATACENTERS-AS-1US	false
126.168.175.209	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
176.184.175.32	unknown	France		5410	BOUYGTEL-ISPFR	false
115.32.241.214	unknown	China		4766	KIXS-AS-KRKoreaTelecomKR	false
182.75.16.142	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	false
178.133.76.144	unknown	Ukraine		21497	UMC-ASUA	false
176.99.56.112	unknown	Russian Federation		59476	ASROSINTRARU	false
90.251.212.225	unknown	United Kingdom		5378	VodafoneGB	false
84.240.96.11	unknown	Finland		20904	NETPLAZA-ASFI	false
179.185.47.165	unknown	Brazil		18881	TELEFONICABRASILSABR	false
1.142.198.68	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
18.230.152.161	unknown	United States		16509	AMAZON-02US	false
123.71.229.193	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
164.7.1.167	unknown	France		44013	SANDVIK-ASSE	false
151.95.224.211	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
161.57.94.13	unknown	United States		11206	FSU-AS-1US	false
202.59.56.79	unknown	Australia		9667	HOSTWORKS-AS-AP5GNETWORKOPERATIONSPTYLTDAU	false
90.205.72.173	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
250.66.202.98	unknown	Reserved		unknown	unknown	false
252.72.1.224	unknown	Reserved		unknown	unknown	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.182.231.163	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
192.195.38.207	unknown	United States		63242	AS-CMN-LSUS	false
194.192.108.56	unknown	Denmark		3292	TDCTDCASDK	false
126.212.237.5	unknown	Japan		17676	GIGAINFRASoftbankBBCorp JP	false
109.54.105.56	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
192.243.129.241	unknown	United States		22284	AS22284-DOI-OPSUS	false

Runtime Messages

Command:	/tmp/9Q1fc1TZq4
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.035748270293767
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	9Q1fc1TZq4
File size:	60412
MD5:	b192ed1edacfafee1a66012bfa2c45be

General

SHA1:	0a3451997f43964a25b203672441f3d4b615d224
SHA256:	b41bbb2bcc0d3106fd9767fe53f95329d4178ca48f3fdf700b80619b75207dba
SHA512:	6b4746660989827e03a6cbd51cf925d200e76368f9f792a7dd9dc0f0594410ea735af741d39f26fa48391f666270f39b81292a08f08f6c9e83670ab27137c1f4
SSDEEP:	768:eLobAxU6q9Hfymp0xginSYcCLUB6WsTwR11IQdszoDaS0O+DCDt:eL0AxvSHfymp0xgujcCLs6vTAIau6
File Content Preview:	.ELF.....4...l....4. ...(.....x.....dt.Q.....@..(....@.8R.....#.....b0..`.....!..... ...@....."........`.....$ ... ...@.. ....`....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	60012
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

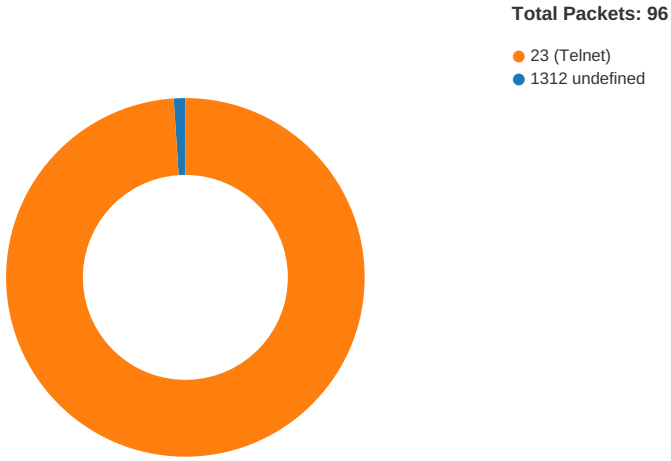
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0xe180	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1e230	0xe230	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e248	0xe248	0x668	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x2e8b4	0xe8b4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2e8bc	0xe8bc	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x2e8c8	0xe8c8	0x164	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x2ea30	0xea2c	0x288	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0xea2c	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	0x10000	0x10000	0xe8b0	0xe8b0	3.3886	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xe8b4	0x2e8b4	0x2e8b4	0x178	0x404	0.3183	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: 9Q1fc1TZq4 PID: 5222 Parent PID: 5109

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	/tmp/9Q1fc1TZq4
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: 9Q1fc1TZq4 PID: 5224 Parent PID: 5222

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Copyright Joe Security LLC 2022

Analysis Process: 9Q1fc1TZq4 PID: 5241 Parent PID: 5224

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5243 Parent PID: 5224

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5245 Parent PID: 5243

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5251 Parent PID: 5245

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5253 Parent PID: 5245

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Copyright Joe Security LLC 2022

Analysis Process: 9Q1fc1TZq4 PID: 5248 Parent PID: 5243

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5249 Parent PID: 5243

General

Start time:	01:39:24
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5225 Parent PID: 5222

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5226 Parent PID: 5222

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5229 Parent PID: 5226

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Copyright Joe Security LLC 2022

File Activities

File Read

Directory Enumerated

Analysis Process: 9Q1fc1TZq4 PID: 5259 Parent PID: 5229

General

Start time:	01:39:30
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5261 Parent PID: 5229

General

Start time:	01:39:30
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5232 Parent PID: 5226

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 9Q1fc1TZq4 PID: 5235 Parent PID: 5226

General

Start time:	01:39:14
Start date:	15/01/2022
Path:	/tmp/9Q1fc1TZq4
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Copyright Joe Security LLC 2022