ID: 557410
Sample Name: V15hQSZlC3
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:07:16
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

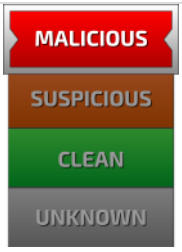
V15hQSZlC3

Overview

General Information

Sample Name:	V15hQSZlC3
Analysis ID:	557410
MD5:	75797bc071034c..
SHA1:	0a31fec94f3e33c..
SHA256:	eb1e72903ad912.
Tags:	32 elf mirai powerpc
Infos:	

Detection



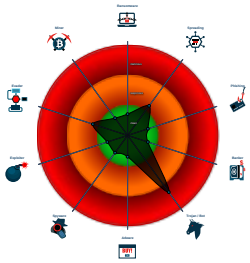
Mirai

Score:	68
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 n…
- 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…
- Executes the "rm" command used t…
- Sample listens on a socket

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:	557410
Start date:	21.01.2022
Start time:	04:07:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V15hQSZlC3
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:	mal68.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/V15hQSZlC3
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	DaddyL33T Infected Your Shit
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- V15hQSZlC3 (PID: 5214, Parent: 5111, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/V15hQSZlC3
  - V15hQSZlC3 New Fork (PID: 5216, Parent: 5214)
    - V15hQSZlC3 New Fork (PID: 5333, Parent: 5216)
    - V15hQSZlC3 New Fork (PID: 5334, Parent: 5216)
      - V15hQSZlC3 New Fork (PID: 5337, Parent: 5334)
        - V15hQSZlC3 New Fork (PID: 5347, Parent: 5337)
        - V15hQSZlC3 New Fork (PID: 5348, Parent: 5337)
      - V15hQSZlC3 New Fork (PID: 5339, Parent: 5334)
      - V15hQSZlC3 New Fork (PID: 5342, Parent: 5334)
    - V15hQSZlC3 New Fork (PID: 5217, Parent: 5214)
    - V15hQSZlC3 New Fork (PID: 5218, Parent: 5214)
      - V15hQSZlC3 New Fork (PID: 5222, Parent: 5218)
        - V15hQSZlC3 New Fork (PID: 5329, Parent: 5222)
        - V15hQSZlC3 New Fork (PID: 5330, Parent: 5222)
      - V15hQSZlC3 New Fork (PID: 5223, Parent: 5218)
      - V15hQSZlC3 New Fork (PID: 5224, Parent: 5218)
- dash New Fork (PID: 5266, Parent: 4331)
  - rm (PID: 5266, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.mGBdYrIAjO /tmp/tmp.nilNg8yhqU /tmp/tmp.xo9oKnmcRG
- **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

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

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

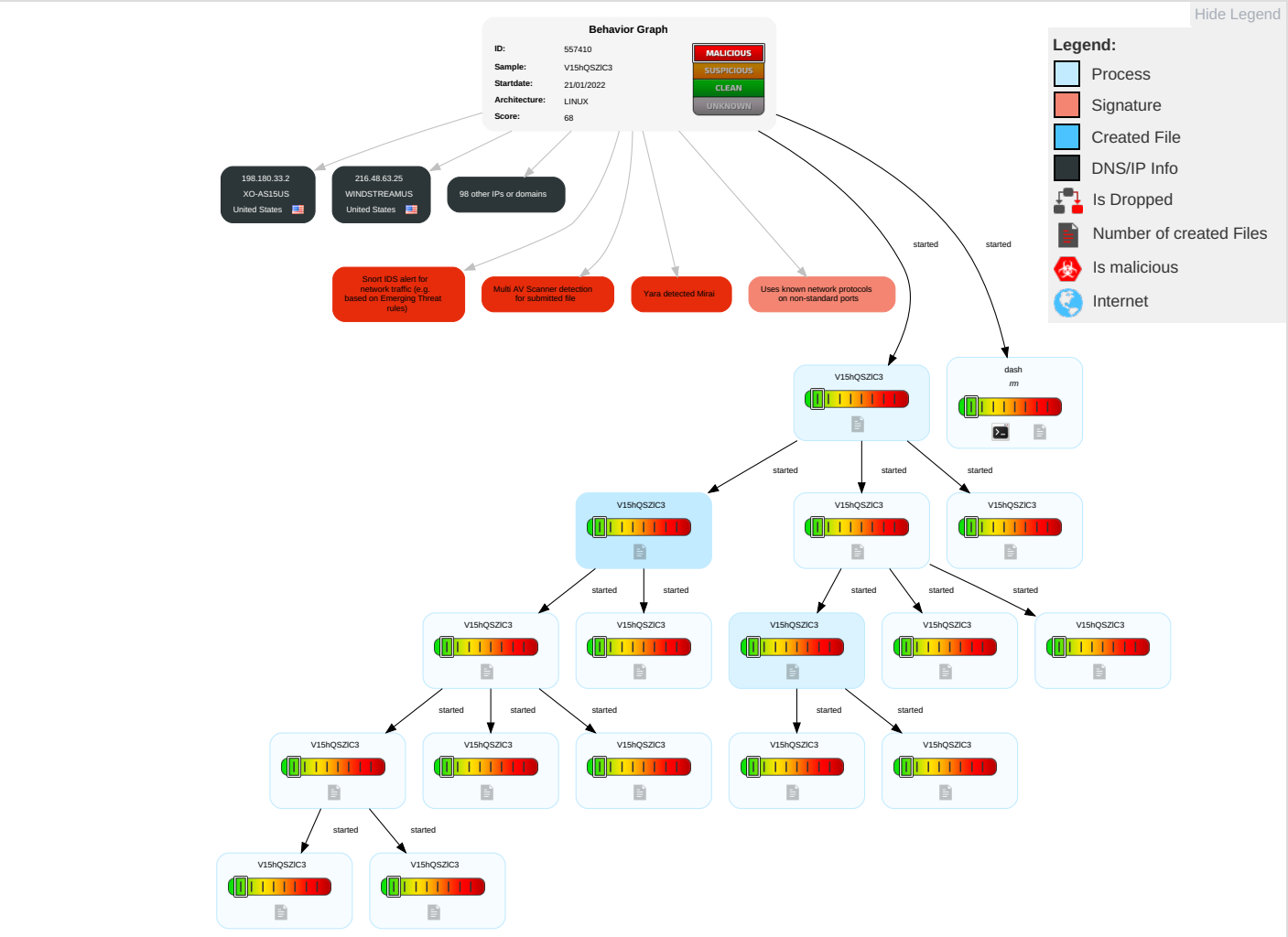
Mitre Att&ck Matrix

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 File Deletion	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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	1 Application Layer Protocol	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
V15hQSZIC3	46%	Virustotal		Browse
V15hQSZIC3	56%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

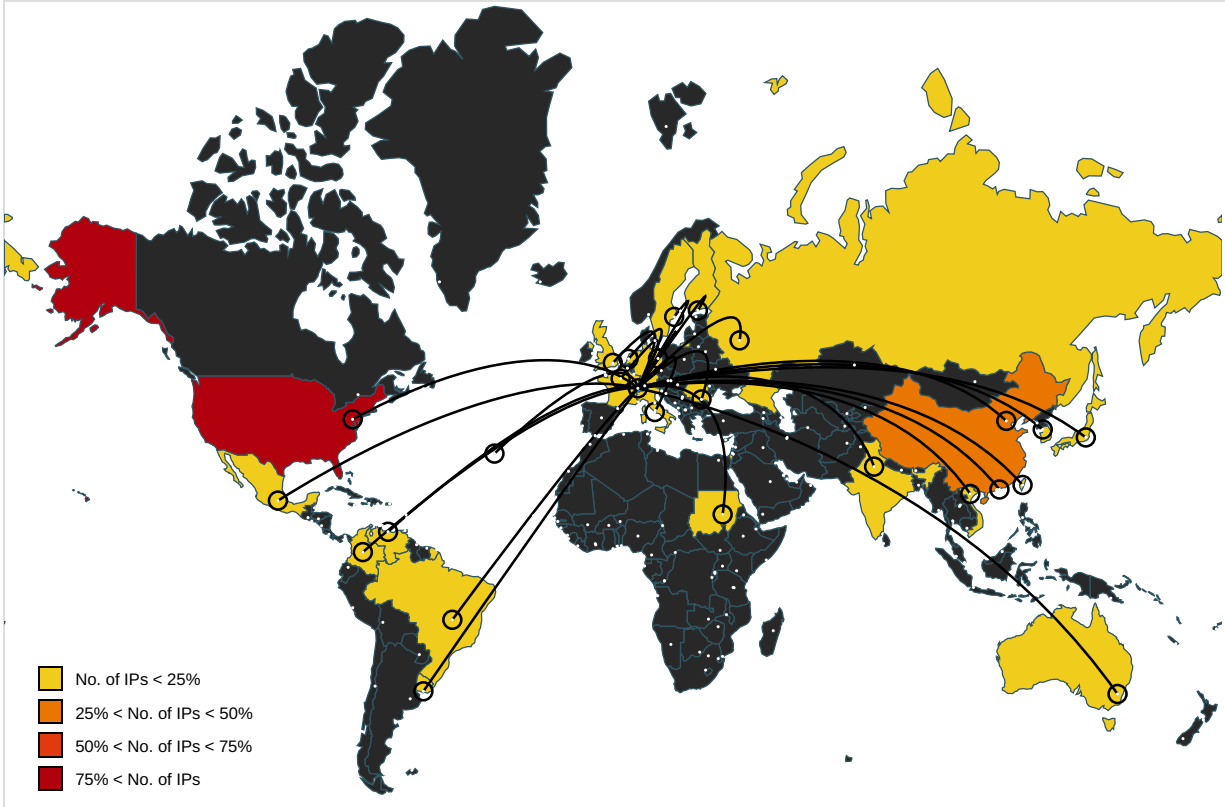
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
219.43.156.34	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
4.83.244.200	unknown	United States		3356	LEVEL3US	false
154.3.74.146	unknown	United States		174	COGENT-174US	false
240.230.248.86	unknown	Reserved		unknown	unknown	false
88.167.1.133	unknown	France		12322	PROXADFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
177.73.222.160	unknown	unknown		262573	GILMARDOSSANTOSCIALTDABR	false
110.152.176.194	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
86.148.62.142	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
93.172.23.62	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
168.237.2.178	unknown	United States		3136	STATE-OF-WISCONSIN-AS1US	false
175.94.198.188	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
179.79.229.167	unknown	Brazil		26615	TIMSABR	false
42.73.166.23	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
211.148.32.11	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
32.92.242.241	unknown	United States		2686	ATGS-MMD-ASUS	false
125.88.90.212	unknown	China		4813	BACKBONE-GUANGDONG-APChinaTelecomGroupCN	false
193.33.248.121	unknown	United Kingdom		25180	EXPONENTIAL-E-ASGB	false
145.145.137.23	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
168.51.160.215	unknown	United States		1761	TDIR-CAPNETUS	false
65.32.66.139	unknown	United States		33363	BHN-33363US	false
130.175.68.167	unknown	United States		12173	UAUS	false
67.118.202.168	unknown	United States		11191	F2W-ASUS	false
133.118.92.177	unknown	Japan		2522	PPP-EXPJapanNetworkInformationCenterJP	false
64.9.242.239	unknown	United States		36492	GOOGLEWIFIUS	false
89.30.228.114	unknown	Netherlands		25525	REASONNET-ASAmsterdamtheNetherlandsNL	false
111.151.13.250	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
154.97.229.193	unknown	Sudan		36998	SDN-MOBITELSD	false
186.165.99.66	unknown	Venezuela		21575	ENTELPERUSAPE	false
38.169.105.64	unknown	United States		174	COGENT-174US	false
66.79.7.42	unknown	United States		22561	CENTURYLINK-LEGACY-LIGHTCOREUS	false
252.130.173.94	unknown	Reserved		unknown	unknown	false
130.255.35.230	unknown	Russian Federation		39812	KAMENSKTEL-ASPobedyStr37bKamensk-UralskyRU	false
145.209.118.214	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
151.214.52.31	unknown	United States		11003	PANDGUS	false
80.14.1.195	unknown	France		3215	FranceTelecom-OrangeFR	false
191.242.141.211	unknown	Brazil		262730	BytewebComunicacaoMultimidiaLtdaBR	false
190.128.73.12	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	false
169.184.22.144	unknown	United States		37611	AfrihostZA	false
75.160.134.191	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
1.79.211.224	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
111.54.138.238	unknown	China		56042	CMNET-SHANXI-APChinaMobilecommunicationscorporationCN	false
255.228.188.17	unknown	Reserved		unknown	unknown	false
99.183.173.13	unknown	United States		7018	ATT-INTERNET4US	false
19.235.79.195	unknown	United States		3	MIT-GATEWAYSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
99.126.165.27	unknown	United States		7018	ATT-INTERNET4US	false
97.181.172.187	unknown	United States		6167	CELLCO-PARTUS	false
117.90.184.11	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
145.235.189.29	unknown	Sweden		1257	TELE2EU	false
146.118.183.18	unknown	Australia		134111	CSIRO-PAWSEY-AS-APCommonwealthScientificandIndustrialRe	false
114.78.112.184	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
161.31.175.176	unknown	United States		40581	AREON-ASUS	false
198.180.33.2	unknown	United States		2828	XO-AS15US	false
192.47.33.191	unknown	Japan		5501	FRAUNHOFER-CLUSTER-BWResearchInstitutesspreadalloverGe	false
19.55.221.17	unknown	United States		3	MIT-GATEWAYSUS	false
123.203.7.132	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	false
130.232.1.148	unknown	Finland		1741	FUNETASFI	false
201.35.0.95	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
89.49.3.124	unknown	Germany		5430	FREENETDEfreenetDatenkommunikationsGmbHDE	false
246.250.119.203	unknown	Reserved		unknown	unknown	false
216.48.63.25	unknown	United States		7029	WINDSTREAMUS	false
103.42.251.212	unknown	India		133726	BLUEWEB-ASBLUEWEBNETWORKSOLUTIONSPVTLTDIN	false
121.85.39.119	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
149.95.27.187	unknown	United States		174	COGENT-174US	false
179.25.214.74	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
204.97.148.165	unknown	United States		3931	LOGICALUS	false
168.66.47.187	unknown	United States		265240	ULTRANETSERVICOSEMINTERNETLTDABR	false
47.139.36.108	unknown	United States		5650	FRONTIER-FRTRUS	false
36.20.185.19	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
246.2.169.240	unknown	Reserved		unknown	unknown	false
13.181.255.136	unknown	United States		7018	ATT-INTERNET4US	false
189.141.64.115	unknown	Mexico		8151	UninetSAdeCVMX	false
67.75.143.181	unknown	United States		3549	LVLT-3549US	false
211.180.177.153	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
12.215.91.11	unknown	United States		7018	ATT-INTERNET4US	false
252.176.137.165	unknown	Reserved		unknown	unknown	false
101.119.53.233	unknown	Australia		133612	VODAFONE-AS-APVodafoneAustraliaPtyLtdAU	false
163.78.97.113	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
111.154.178.244	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
216.139.133.157	unknown	United States		22136	NYCTUS	false
220.170.81.177	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
63.37.215.231	unknown	United States		3356	LEVEL3US	false
126.39.23.141	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
161.10.197.59	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
27.77.42.218	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.115.98.121	unknown	United States		20001	TWC-20001-PACWESTUS	false
149.249.13.220	unknown	Germany		15404	COLTTechnologyServicesGroupSE	false
20.156.174.140	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
75.120.33.119	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
210.240.23.2	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
249.37.45.136	unknown	Reserved		unknown	unknown	false
59.208.115.119	unknown	China		2516	KDDIKDDICORPORATIONJP	false
153.131.187.101	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
81.18.70.58	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
163.168.3.222	unknown	Switzerland		786	JANETJiscServicesLimitedGB	false
173.227.122.35	unknown	United States		3549	LVLT-3549US	false
191.11.247.34	unknown	Brazil		26599	TELEFONICABRASILSABR	false
2.226.67.222	unknown	Italy		12874	FASTWEBIT	false
248.155.127.231	unknown	Reserved		unknown	unknown	false
241.2.117.29	unknown	Reserved		unknown	unknown	false
174.127.145.108	unknown	United States		11404	AS-WAVE-1US	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.242471120921623
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	V15hQSZlC3
File size:	51396
MD5:	75797bc071034cc54c68ae81e403096e
SHA1:	0a31fec94f3e33c040a27717d3e5bcfb43c97acb
SHA256:	eb1e72903ad912f0b7a2d20587fa4a2714f8adfc67b716c79dbdc781128dfa5b
SHA512:	9203c30e9addd7d1e81a5a9fa989ad11b70f56f8323342980288407 68b8aef2203920bb8d503a0bd10c543f5c213274c3513e2febc2bfd591d2a36fdc7bd8512
SSDEEP:	768:Sx2Mfcy7pgpC1uwECS5VUhRiogRxA3fgLTW9lvf3KYHJ2VVFsYuWX2IeTrw:K2zy7qpC1uwJ2OErdgA3KYp21j3XLmw
File Content Preview:	.ELF.....4.....4. ...(..... ... .$...$...$...t.....dt.Q.....!..\|.....$H...H..%...$8!. |...N.. .!..|.....?...../...@..\?.....<.+../...A..$8...}).....<N..

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x100001f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	50916
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

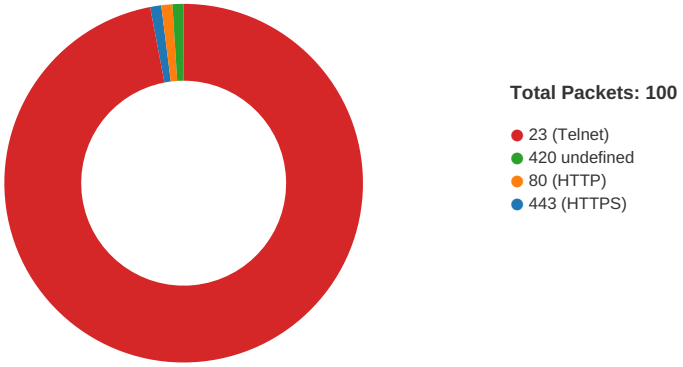
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0xbe7c	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1000bf34	0xbf34	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1000bf54	0xbf54	0x5cc	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1001c524	0xc524	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1001c52c	0xc52c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1001c538	0xc538	0x140	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1001c678	0xc678	0x20	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x1001c698	0xc698	0x74	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1001c70c	0xc698	0x20c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xc698	0x4b	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x10000000	0x10000000	0xc520	0xc520	4.0177	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xc524	0x1001c524	0x1001c524	0x174	0x3f4	0.4228	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: V15hQSZlC3 PID: 5214, Parent PID: 5111

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	/tmp/V15hQSZlC3
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: V15hQSZlC3 PID: 5216, Parent PID: 5214

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: V15hQSZlC3 PID: 5333, Parent PID: 5216

General

Start time:	04:10:53
Start date:	21/01/2022

Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5334**, Parent PID: **5216**

General

Start time:	04:10:53
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5337**, Parent PID: **5334**

General

Start time:	04:10:53
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5347**, Parent PID: **5337**

General

Start time:	04:10:58
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5348**, Parent PID: **5337**

General

Start time:	04:10:58
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5339**, Parent PID: **5334**

General

Start time:	04:10:53
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5342**, Parent PID: **5334**

General

Start time:	04:10:53
Start date:	21/01/2022

Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5217**, Parent PID: **5214**

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5218**, Parent PID: **5214**

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5222**, Parent PID: **5218**

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: V15hQSZlC3 PID: **5329**, Parent PID: **5222**

General

Start time:	04:10:53
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5330**, Parent PID: **5222**

General

Start time:	04:10:53
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5223**, Parent PID: **5218**

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: V15hQSZlC3 PID: **5224**, Parent PID: **5218**

General

Start time:	04:08:00
Start date:	21/01/2022
Path:	/tmp/V15hQSZlC3
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: dash PID: **5266**, Parent PID: **4331**

General

Start time:	04:09:22
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5266**, Parent PID: **4331**

General

Start time:	04:09:22
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.mGBdYrIAjO /tmp/tmp.nilNg8yhqU /tmp/tmp.xo9oKnmcRG
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read