ID: 553219
Sample Name: TudQawdlbF
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:53:53
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

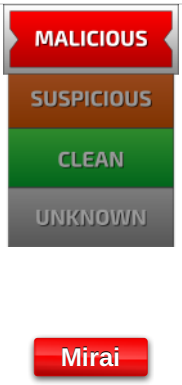
Linux Analysis Report TudQawdlbF

Overview

General Information

Sample Name:	TudQawdlbF
Analysis ID:	553219
MD5:	c334e7bb5fe6853.
SHA1:	8e214ec8b0e9b3..
SHA256:	f4b66f5bfca612a…
Tags:	32 elf mirai renesas
Infos:	

Detection

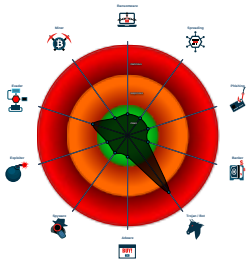


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on no…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Executes the "rm" command used to…
- Sample listens on a socket
- Sample contains strings indicative o…

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:	553219
Start date:	14.01.2022
Start time:	13:53:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TudQawdlbF
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:	Show All

Process Tree

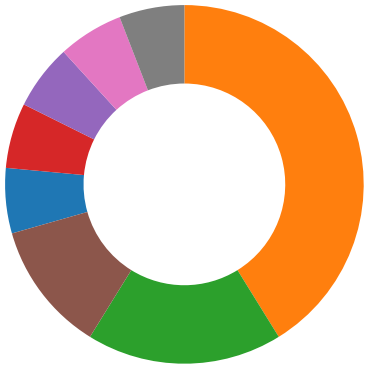
- **system is lnxubuntu20**
- TudQawdlbF (PID: 5209, Parent: 5106, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/TudQawdlbF
  - TudQawdlbF New Fork (PID: 5211, Parent: 5209)
    - TudQawdlbF New Fork (PID: 5213, Parent: 5211)
    - TudQawdlbF New Fork (PID: 5214, Parent: 5211)
    - TudQawdlbF New Fork (PID: 5216, Parent: 5211)
- dash New Fork (PID: 5258, Parent: 4331)
- rm (PID: 5258, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.XirojNzOMl /tmp/tmp.CnxdzwO3rm /tmp/tmp.iXnCqWUK00
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



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

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

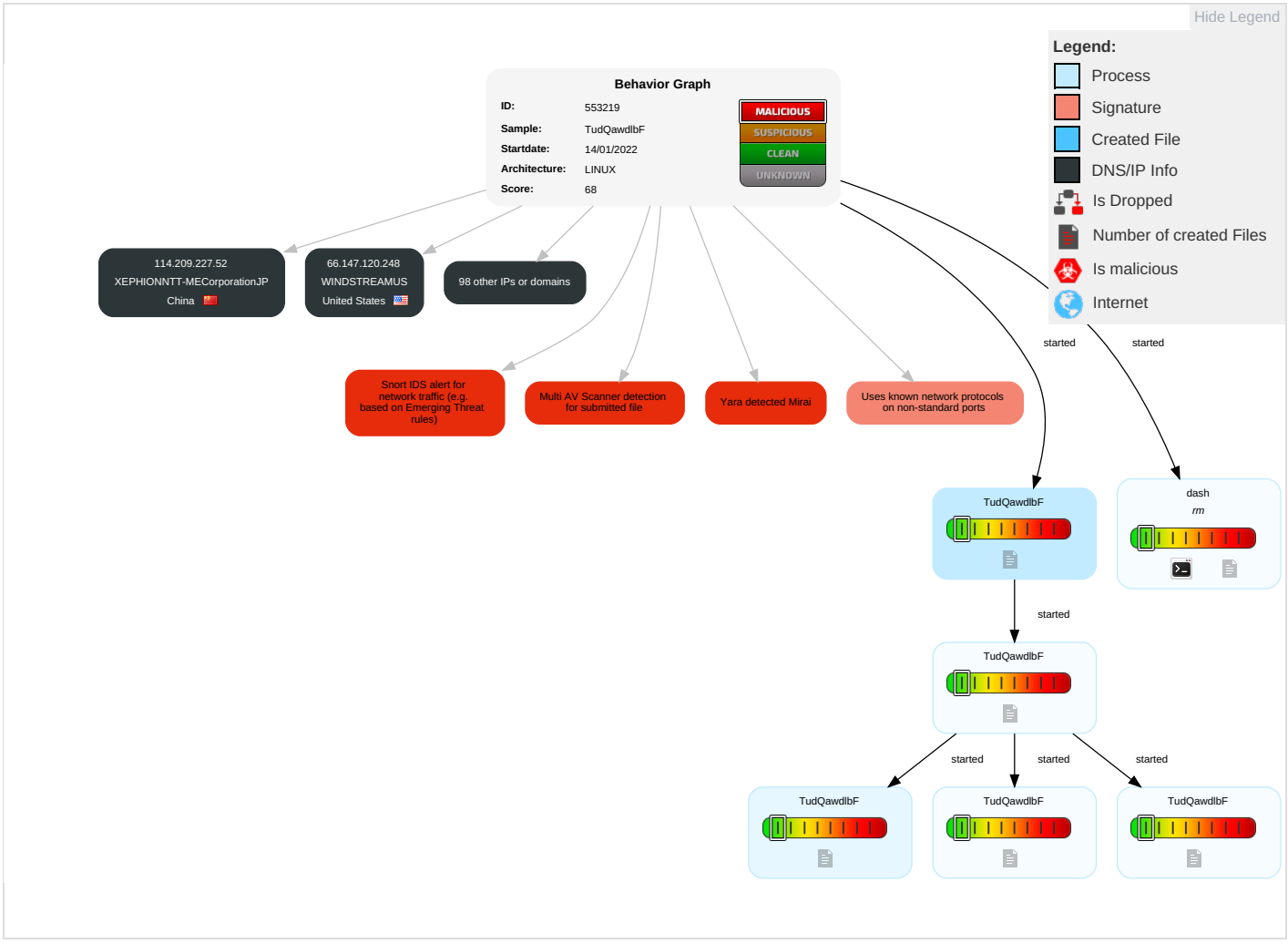
Mitre Att&ck Matrix

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	File Deletion 1	OS Credential Dumping	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 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	Non-Standard Port 1 1	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	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
TudQawdlbF	44%	Virustotal		Browse
TudQawdlbF	40%	Metadefender		Browse
TudQawdlbF	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
144.11.242.71	unknown	United States		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
82.125.79.153	unknown	France		3215	FranceTelecom-OrangeFR	false
98.34.189.138	unknown	United States		7922	COMCAST-7922US	false
182.28.200.252	unknown	Indonesia		4795	INDOSATM2-IDINDOSATM2ASNID	false
191.2.105.207	unknown	Brazil		7738	TelemarNorteLesteSABR	false
165.241.54.131	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
151.211.116.212	unknown	United Kingdom		11003	PANDGUS	false
76.29.27.180	unknown	United States		7922	COMCAST-7922US	false
180.172.248.165	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
39.110.118.152	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
101.234.204.115	unknown	Australia		45577	INTERVOLVE-MELBOURNE-AS-APIntervolvePtyLtdAU	false
64.57.156.131	unknown	United States		18659	FTPS-LLCUS	false
184.223.162.13	unknown	United States		10507	SPCSUS	false
151.157.25.132	unknown	Norway		224	UNINETTUNINETTTheNorwegianUniversityResearchNetwork	false
204.36.210.23	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
124.31.210.124	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
38.112.246.25	unknown	United States		174	COGENT-174US	false
79.37.106.122	unknown	Italy		3269	ASN-IBSNAZIT	false
208.196.44.36	unknown	United States		701	UUNETUS	false
147.252.193.92	unknown	Ireland		1213	HEANETIE	false
91.205.183.104	unknown	Russian Federation		51811	LOKOBANK-ASRU	false
80.117.234.117	unknown	Italy		3269	ASN-IBSNAZIT	false
66.147.120.248	unknown	United States		7029	WINDSTREAMUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.203.245.219	unknown	Czech Republic		25512	CDT-ASTheCzechRepublicCZ	false
132.174.108.236	unknown	United States		4373	OCLC-ASUS	false
156.114.21.35	unknown	Netherlands		13639	ING-AMERICAS-WHOLESALEUS	false
25.19.39.29	unknown	United Kingdom		7922	COMCAST-7922US	false
150.109.138.209	unknown	Singapore		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	false
171.194.174.175	unknown	United States		10794	BANKAMERICAUS	false
142.34.24.20	unknown	Canada		27272	Q9-AS-CAL3CA	false
124.220.114.107	unknown	China		45361	JCN-AS-KRUlsanJung-AngBroadcastingNetworkKR	false
178.121.106.240	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
114.209.227.52	unknown	China		9595	XEPHIONNTT-MECorporationJP	false
12.46.36.249	unknown	United States		2386	INS-ASUS	false
86.17.1.166	unknown	United Kingdom		5089	NTLGB	false
201.77.56.69	unknown	Brazil		28583	RuralWebTelecomunicacoesLtdaBR	false
78.64.30.126	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
146.15.235.165	unknown	United States		1467	DNIC-ASBLK-01467-01468US	false
187.136.222.94	unknown	Mexico		8151	UninetSAdeCVMX	false
191.157.233.183	unknown	Colombia		26611	COMCELSACO	false
159.95.161.30	unknown	France		20617	BNP-PARIBASGB	false
94.66.233.221	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
184.132.54.134	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
99.220.55.165	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
47.22.179.99	unknown	United States		6128	CABLE-NET-1US	false
130.99.153.128	unknown	United States		203	CENTURYLINK-LEGACY-LVLT-203US	false
119.68.28.235	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
213.58.107.86	unknown	Portugal		9186	ONILisbonPortugalPT	false
12.213.2.200	unknown	United States		7018	ATT-INTERNET4US	false
167.185.202.205	unknown	United States		15071	BAX-BGPUS	false
19.214.208.55	unknown	United States		3	MIT-GATEWAYSUS	false
83.92.253.152	unknown	Denmark		3292	TDCTDCASDK	false
136.23.81.170	unknown	United States		394699	GOOGLE-ACCESS-NYCUS	false
188.247.2.168	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
80.170.65.237	unknown	Sweden		1257	TELE2EU	false
103.244.180.104	unknown	New Zealand		132509	DAHL-AS-APDIGIWEBADVANCEDHOSTINGLIMITEDNZ	false
78.157.213.16	unknown	United Kingdom		42831	UKSERVERS-ASUKDedicatedServersHostingandCo-Location	false
59.178.147.154	unknown	India		17813	MTNL-APMahanagarTelephoneNigamLimitedIN	false
8.155.218.254	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
186.253.253.44	unknown	Brazil		26615	TIMSABR	false
182.23.50.158	unknown	Indonesia		4800	LINTASARTA-AS-APNetworkAccessProviderandInternetServic	false
141.250.36.79	unknown	Italy		137	ASGARRConsortiumGARREU	false
164.120.132.110	unknown	United States		14235	STATE-NM-US	false
53.84.31.42	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
24.50.201.17	unknown	United States		14638	LCPRLUS	false
45.231.45.87	unknown	Mexico		265546	HYUNDAIAUTOEVERMEXICOSDERLDECVMX	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.85.20.199	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
82.197.221.42	unknown	Netherlands		25596	CAMBRIUM-ASNL	false
151.71.40.99	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
104.210.176.30	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
220.8.84.129	unknown	Japan		17676	GIGAINFRASoftbankBBCorp JP	false
116.167.148.230	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
93.182.85.162	unknown	Turkey		44558	NETONLINETR	false
197.193.244.10	unknown	Egypt		36992	ETISALAT-MISREG	false
177.250.111.177	unknown	Paraguay		27866	COPACOPY	false
96.9.165.193	unknown	Singapore		134809	VIEWQWEST-AS-APViewQwestSdnBhdMY	false
152.97.244.234	unknown	United States		21766	BEN-LOMAND-TELUS	false
199.33.239.34	unknown	United States		32992	ITECHTOOL-ASN-SFUS	false
171.225.54.141	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
117.115.137.151	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
120.96.248.252	unknown	Taiwan; Republic of China (ROC)		17716	NTU-TWNationalTaiwanUniversity TW	false
75.184.18.44	unknown	United States		11426	TWC-11426-CAROLINASUS	false
96.102.162.17	unknown	United States		7922	COMCAST-7922US	false
80.198.91.106	unknown	Denmark		3292	TDCTDCASDK	false
71.235.175.151	unknown	United States		7922	COMCAST-7922US	false
62.39.174.138	unknown	France		15557	LDCOMNETFR	false
110.102.74.199	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
12.238.112.34	unknown	United States		11085	PDI-HQ-INETUS	false
50.225.232.150	unknown	United States		7922	COMCAST-7922US	false
194.10.160.193	unknown	European Union		2686	ATGS-MMD-ASUS	false
96.63.51.106	unknown	Canada		22995	BARR-XPLR-ASNCA	false
196.111.216.211	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
125.171.111.165	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
72.86.238.183	unknown	United States		701	UUNETUS	false
38.170.192.133	unknown	United States		174	COGENT-174US	false
112.93.165.94	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
130.84.114.72	unknown	France		1303	FR-IDRIS-ORSAYFREU	false
117.184.54.129	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
193.119.122.244	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
17.84.31.213	unknown	United States		714	APPLE-ENGINEERINGUS	false

Runtime Messages

Command:	/tmp/TudQawdlbF
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Yakuza Botnet
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 LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.801600272167886
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	TudQawdlbF
File size:	55112
MD5:	c334e7bb5fe6853b0654ef0207106832
SHA1:	8e214ec8b0e9b3725a5f0dbf0c70a391ca044bb3
SHA256:	f4b66f5bfca612afe7d4d0d430511fedbc247eb91ab65c99c5ae7524a4af4e1b
SHA512:	fa105827e12211609109a9d28e31346f3955cffcea0d1ef40c62f7e2ba572309c3c67c92740fed2c46e4a19f9e22436dae5e615f6645c4805a18285a864ee0f8
SSDEEP:	768:OavUjkefqoege3ePecCiB29tVasevR586k9HCRRvoVimXQkC9o5W1Up:Oav8kWp9+OiumtMlpqFHKAVrQkC9onp
File Content Preview:	.ELF.....*.....@.4.....4. ...(.....@...@.....A...A.....'.....Q.td....././/"O.n.....#.*@.....#.*@,....o&O.n...l....././/.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0

ELF header

Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	54712
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

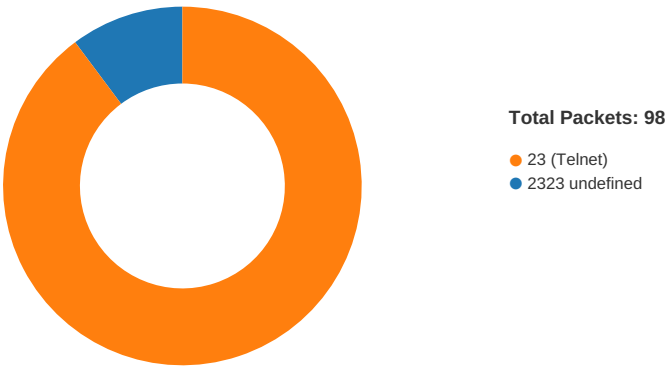
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xc440	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40c520	0xc520	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40c544	0xc544	0xc78	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41d1c0	0xd1c0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41d1c8	0xd1c8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41d1d4	0xd1d4	0x3a4	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41d578	0xd578	0x23d4	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xd578	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	0x400000	0x400000	0xd1bc	0xd1bc	4.4933	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xd1c0	0x41d1c0	0x41d1c0	0x3b8	0x278c	1.5889	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: TudQawdlbF PID: 5209 Parent PID: 5106

General

Start time:	13:54:35
Start date:	14/01/2022
Path:	/tmp/TudQawdlbF
Arguments:	/tmp/TudQawdlbF
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: TudQawdlbF PID: 5211 Parent PID: 5209

General

Start time:	13:54:35
Start date:	14/01/2022
Path:	/tmp/TudQawdlbF
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: TudQawdlbF PID: 5213 Parent PID: 5211

General

Start time:	13:54:35
Start date:	14/01/2022
Path:	/tmp/TudQawdlbF
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: TudQawdlbF PID: 5214 Parent PID: 5211

General

Start time:	13:54:35
Start date:	14/01/2022
Path:	/tmp/TudQawdlbF
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: TudQawdlbF PID: 5216 Parent PID: 5211

General

Start time:	13:54:35
Start date:	14/01/2022

Path:	/tmp/TudQawdlbF
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: dash PID: 5258 Parent PID: 4331

General

Start time:	13:55:59
Start date:	14/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5258 Parent PID: 4331

General

Start time:	13:55:59
Start date:	14/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.XirojNzOMl /tmp/tmp.CnxdzwO3rm /tmp/tmp.iXnCqWUK00
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read