ID: 553483
Sample Name: fVA3Q44QAK
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:01:50
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

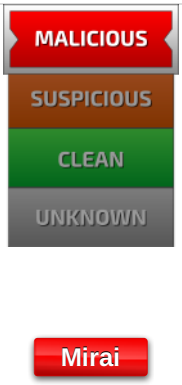
Linux Analysis Report fVA3Q44QAK

Overview

General Information

Sample Name:	fVA3Q44QAK
Analysis ID:	553483
MD5:	cd652152128984..
SHA1:	ecb03ba794a579..
SHA256:	00a6f460395d2f5..
Tags:	32 elf intel mirai
Infos:	

Detection

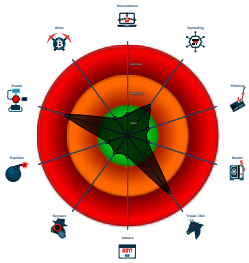


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample contains only a LOAD segm...
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...
- Executes the "rm" command used to...
- 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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553483
Start date:	15.01.2022
Start time:	01:01:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fVA3Q44QAK
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.troj.evad.lin@0/0@0/0
Warnings:	Show All

Process Tree

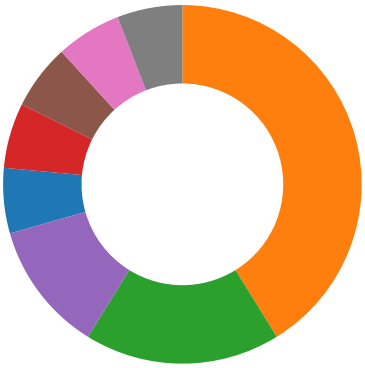
- **system is lnxubuntu20**
- fVA3Q44QAK (PID: 5218, Parent: 5108, MD5: cd6521521289846e8001d5f05cf0e10d) Arguments: /tmp/fVA3Q44QAK
  - fVA3Q44QAK New Fork (PID: 5219, Parent: 5218)
    - fVA3Q44QAK New Fork (PID: 5326, Parent: 5219)
    - fVA3Q44QAK New Fork (PID: 5328, Parent: 5219)
      - fVA3Q44QAK New Fork (PID: 5329, Parent: 5328)
        - fVA3Q44QAK New Fork (PID: 5335, Parent: 5329)
        - fVA3Q44QAK New Fork (PID: 5336, Parent: 5329)
      - fVA3Q44QAK New Fork (PID: 5330, Parent: 5328)
      - fVA3Q44QAK New Fork (PID: 5331, Parent: 5328)
  - fVA3Q44QAK New Fork (PID: 5220, Parent: 5218)
  - fVA3Q44QAK New Fork (PID: 5221, Parent: 5218)
    - fVA3Q44QAK New Fork (PID: 5222, Parent: 5221)
      - fVA3Q44QAK New Fork (PID: 5325, Parent: 5222)
      - fVA3Q44QAK New Fork (PID: 5327, Parent: 5222)
    - fVA3Q44QAK New Fork (PID: 5223, Parent: 5221)
    - fVA3Q44QAK New Fork (PID: 5224, Parent: 5221)
- dash New Fork (PID: 5264, Parent: 4331)
- rm (PID: 5264, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.FZJy5QRkED /tmp/tmp.Cx4p8ienxO /tmp/tmp.ayYQw5P6KC
- **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
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Stealing of Sensitive Information
- Remote Access Functionality

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

Data Obfuscation:

Sample is packed with UPX

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

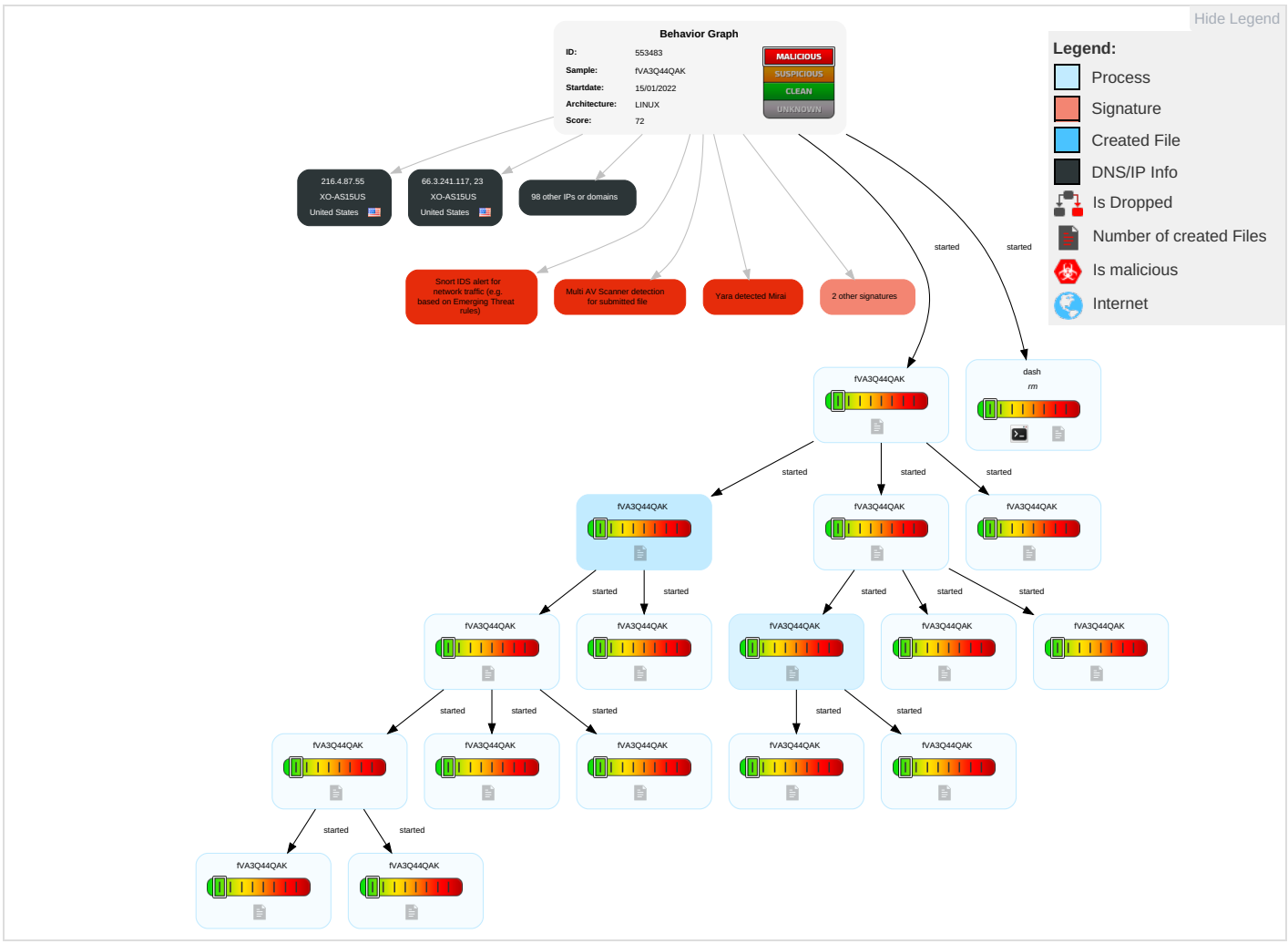
Mitre Att&ck Matrix

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	Obfuscated Files or Information 1	OS Credential Dumping 1	System Service Discovery	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	File Deletion 1	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
fVA3Q44QAK	37%	Virustotal		Browse
fVA3Q44QAK	51%	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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
118.211.239.132	unknown	Australia		4739	INTERNODE-ASInternodePtyLtdAU	false
210.106.38.203	unknown	Korea Republic of		17839	DREAMPLUS-AS-KRLGHelloVisionCorpKR	false
242.236.222.254	unknown	Reserved		unknown	unknown	false
119.222.246.123	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
118.251.164.218	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
61.125.29.174	unknown	Japan		9595	XEPHIONNTT-MECorporationJP	false
197.89.97.58	unknown	South Africa		10474	OPTINETZA	false
145.151.15.79	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
213.46.86.255	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
147.125.210.77	unknown	Austria		2488	IIASA-NETInternationalInstituteforAppliedSystemsAnalys	false
32.249.33.88	unknown	United States		2686	ATGS-MMD-ASUS	false
74.136.69.5	unknown	United States		10796	TWC-10796-MIDWESTUS	false
248.169.175.87	unknown	Reserved		unknown	unknown	false
27.197.55.18	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
213.52.109.228	unknown	Norway		2116	ASN-CATCHCOMNO	false
156.34.23.163	unknown	Canada		855	CANET-ASN-4CA	false
122.4.122.86	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
66.3.241.117	unknown	United States		2828	XO-AS15US	false
112.252.196.33	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
156.49.160.15	unknown	Sweden		29975	VODACOM-ZA	false
89.113.117.183	unknown	Russian Federation		44699	STROITELNAYA_INNOVACIARU	false
87.196.249.120	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
192.84.228.183	unknown	Hungary		1741	FUNETASFI	false
32.220.131.221	unknown	United States		46690	SNET-FCCUS	false
1.255.173.186	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
4.164.140.27	unknown	United States		3356	LEVEL3US	false
36.17.156.115	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
153.15.14.52	unknown	Norway		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
151.208.73.143	unknown	United States		11003	PANDGUS	false
61.191.66.240	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
42.66.128.89	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
206.32.17.122	unknown	United States		3356	LEVEL3US	false
113.82.60.114	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
48.5.47.35	unknown	United States		2686	ATGS-MMD-ASUS	false
122.131.61.127	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
196.142.51.78	unknown	Egypt		36935	Vodafone-EG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
118.143.163.141	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
45.167.218.35	unknown	Brazil		268009	BELINFONETSERVICOSDECOMUNICACAOEMULTIMIDIAEBR	false
85.208.2.15	unknown	Finland		209378	INIOS-ASFI	false
150.210.115.42	unknown	United States		31822	CITY-UNIVERSITY-OF-NEW-YORKUS	false
80.107.7.150	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
253.91.52.203	unknown	Reserved		unknown	unknown	false
168.151.75.250	unknown	United States		204472	ROYALEASNDE	false
142.22.118.16	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
5.24.72.65	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
88.16.182.184	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
194.12.251.222	unknown	Bulgaria		8262	EVOLINK-ASBG	false
99.13.97.229	unknown	United States		7018	ATT-INTERNET4US	false
246.175.96.4	unknown	Reserved		unknown	unknown	false
147.75.13.99	unknown	Switzerland		35914	ARMOR-DEFENSEUS	false
191.30.36.92	unknown	Brazil		18881	TELEFONICABRASILSABR	false
65.144.152.0	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
155.200.239.157	unknown	United States		8698	NationwideBuildingSocietyGB	false
247.249.240.163	unknown	Reserved		unknown	unknown	false
167.181.16.213	unknown	United States		62481	SUNTRUST-BANKUS	false
14.116.97.246	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
14.255.164.60	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
153.85.227.119	unknown	United States		14962	NCR-252US	false
241.197.46.115	unknown	Reserved		unknown	unknown	false
253.193.91.235	unknown	Reserved		unknown	unknown	false
208.27.147.39	unknown	United States		36837	ASN-TELETRACUS	false
81.137.109.241	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
37.195.118.225	unknown	Russian Federation		31200	NTKIPv6customersRU	false
181.24.7.243	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
181.21.8.118	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
108.132.57.207	unknown	United States		16509	AMAZON-02US	false
149.131.43.106	unknown	United States		33022	WELLESLEY-COLLEGEUS	false
67.29.230.68	unknown	United States		202818	LEVEL3COMMUNICATIONSFR	false
96.178.243.163	unknown	United States		7922	COMCAST-7922US	false
250.124.165.154	unknown	Reserved		unknown	unknown	false
107.204.213.78	unknown	United States		7018	ATT-INTERNET4US	false
158.178.211.100	unknown	United Kingdom		15830	EQUINIX-CONNECT-EMEAGB	false
216.4.87.55	unknown	United States		2828	XO-AS15US	false
18.243.215.229	unknown	United States		16509	AMAZON-02US	false
12.239.5.98	unknown	United States		7018	ATT-INTERNET4US	false
194.216.31.188	unknown	United Kingdom		702	UUNETUS	false
116.96.79.11	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
74.192.181.152	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
2.149.14.35	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
105.120.247.64	unknown	Nigeria		36873	VNL1-ASNG	false
194.64.149.47	unknown	Germany		4589	EASYNETEasynetGlobalServicesEU	false
146.88.159.180	unknown	Malaysia		133847	ICT-AS-APAnppleTechEnterpriseMY	false
4.143.53.39	unknown	United States		3356	LEVEL3US	false
167.212.83.51	unknown	United States		33166	BFS-49-33166US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.78.192.218	unknown	United States		11763	IBX-CHICAGOUS	false
85.219.218.240	unknown	Poland		205738	MARMITEPL	false
177.56.151.219	unknown	Brazil		22085	ClaroSABR	false
102.228.74.21	unknown	unknown		36926	CKL1-ASNKE	false
81.102.118.139	unknown	United Kingdom		5089	NTLGB	false
197.252.128.132	unknown	Sudan		15706	SudatelSD	false
60.186.225.153	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
184.7.217.32	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
169.132.160.131	unknown	United States		7270	NET2PHONEUS	false
42.164.86.69	unknown	China		4249	LILLY-ASUS	false
63.57.227.252	unknown	United States		701	UUNETUS	false
196.240.143.25	unknown	Seychelles		37518	FIBERGRIDSC	false
124.66.201.250	unknown	Japan		18281	TAC-NETTokonameNew-TVCorporationJP	false
205.221.42.4	unknown	United States		6122	ICN-ASUS	false
126.54.223.48	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
57.166.240.145	unknown	Belgium		2686	ATGS-MMD-ASUS	false

Runtime Messages

Command:	/tmp/fVA3Q44QAK
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 LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.87055577615585
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	fVA3Q44QAK
File size:	24728
MD5:	cd6521521289846e8001d5f05cf0e10d
SHA1:	ecb03ba794a579a02ad8e0ef94b29ebed527a155
SHA256:	00a6f460395d2f545eba81ead528fcf2883582412affb7b052e7fef3478361c0
SHA512:	f454f474a2de88b0923adf988d07d94c0e352b444bfb94fbadc0a0cf842faef5daa1e9c651274c24c979e12f369ce138e6cb48d38eb133093704f06f79b3b320
SSDEEP:	768:i/QOC0Yhn6RODyF94cwNEFCnNBml1YHtfzbcN:i/nihnuFHwTNBuktcN
File Content Preview:	.ELF.....g..4.....4. ...(....._..._.....W...W.....Q.td.....tUPX!.....Z.....?d..ELF.....d.....4.,..4. (.....k.-.#.`.....?..P.....d..l

Static ELF Info

ELF header

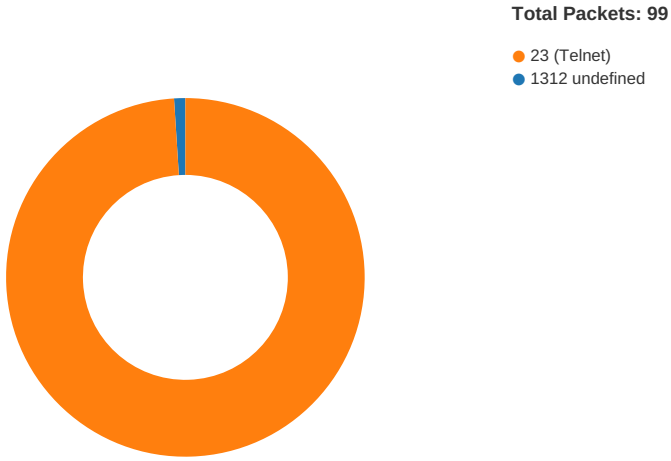
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xc067a0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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	0x5f9b	0x5f9b	4.5585	0x5	R E	0x1000		
LOAD	0x700	0x8055700	0x8055700	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: fVA3Q44QAK PID: 5218 Parent PID: 5108

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	/tmp/fVA3Q44QAK
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5219 Parent PID: 5218

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

File Activities

File Read

Directory Enumerated

Analysis Process: fVA3Q44QAK PID: 5326 Parent PID: 5219

General

Start time:	01:05:21

Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5328 Parent PID: 5219

General

Start time:	01:05:21
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5329 Parent PID: 5328

General

Start time:	01:05:21
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5335 Parent PID: 5329

General

Start time:	01:05:26
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5336 Parent PID: 5329

General

Start time:	01:05:26
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5330 Parent PID: 5328

General

Start time:	01:05:21
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5331 Parent PID: 5328

General

Start time:	01:05:21
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5220 Parent PID: 5218

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5221 Parent PID: 5218

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5222 Parent PID: 5221

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

File Activities

File Read

Directory Enumerated

Analysis Process: fVA3Q44QAK PID: 5325 Parent PID: 5222

General

Start time:	01:05:21
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5327 Parent PID: 5222

General

Start time:	01:05:21
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5223 Parent PID: 5221

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: fVA3Q44QAK PID: 5224 Parent PID: 5221

General

Start time:	01:02:31
Start date:	15/01/2022
Path:	/tmp/fVA3Q44QAK
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	cd6521521289846e8001d5f05cf0e10d

Analysis Process: dash PID: 5264 Parent PID: 4331

General

Start time:	01:03:56
Start date:	15/01/2022
Path:	/usr/bin/dash

Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5264 Parent PID: 4331

General

Start time:	01:03:56
Start date:	15/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.FZJy5QRkED /tmp/tmp.Cx4p8ienxO /tmp/tmp.ayYQw5P6KC
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read