ID: 557419
Sample Name: QuSDT8cmP0
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:22:24
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

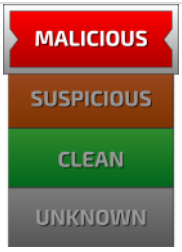
QuSDT8cmP0

Overview

General Information

Sample Name:	QuSDT8cmP0
Analysis ID:	557419
MD5:	d60f2b0aded8eb..
SHA1:	8afb2e9490ca96..
SHA256:	478df6827563de..
Tags:	32 elf mirai sparc
Infos:	

Detection



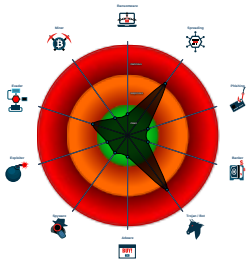
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample tries to kill multiple process…
- 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:	557419
Start date:	21.01.2022
Start time:	04:22:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QuSDT8cmP0
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.spre.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/QuSDT8cmP0
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	DaddyL33T Infected Your Shit
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- QuSDT8cmP0 (PID: 5223, Parent: 5111, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/QuSDT8cmP0
  - QuSDT8cmP0 New Fork (PID: 5225, Parent: 5223)
    - QuSDT8cmP0 New Fork (PID: 5243, Parent: 5225)
    - QuSDT8cmP0 New Fork (PID: 5244, Parent: 5225)
      - QuSDT8cmP0 New Fork (PID: 5247, Parent: 5244)
        - QuSDT8cmP0 New Fork (PID: 5250, Parent: 5247)
        - QuSDT8cmP0 New Fork (PID: 5253, Parent: 5247)
      - QuSDT8cmP0 New Fork (PID: 5248, Parent: 5244)
      - QuSDT8cmP0 New Fork (PID: 5251, Parent: 5244)
    - QuSDT8cmP0 New Fork (PID: 5226, Parent: 5223)
    - QuSDT8cmP0 New Fork (PID: 5227, Parent: 5223)
      - QuSDT8cmP0 New Fork (PID: 5231, Parent: 5227)
        - QuSDT8cmP0 New Fork (PID: 5261, Parent: 5231)
        - QuSDT8cmP0 New Fork (PID: 5263, Parent: 5231)
      - QuSDT8cmP0 New Fork (PID: 5232, Parent: 5227)
      - QuSDT8cmP0 New Fork (PID: 5234, Parent: 5227)
- **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)

System Summary

Sample tries to kill multiple processes (SIGKILL)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

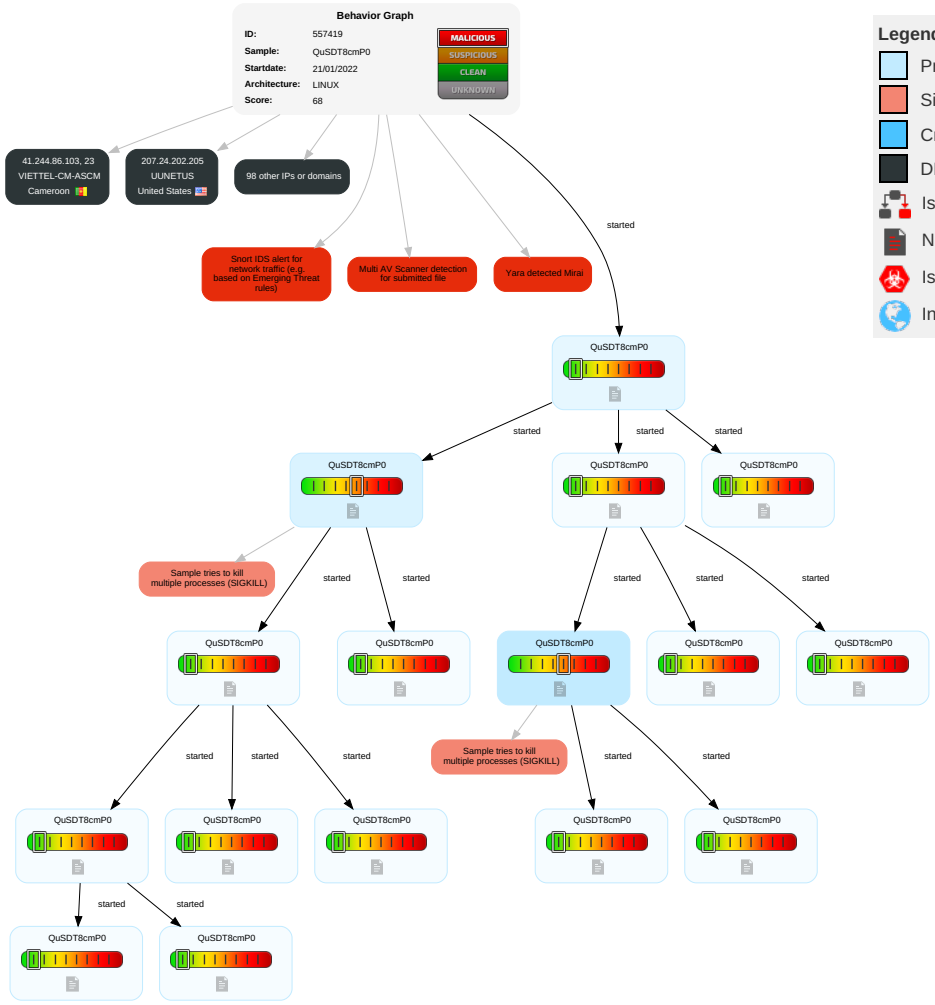
Mitre Att&ck Matrix

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	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 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
QuSDT8cmP0	48%	Virustotal		Browse
QuSDT8cmP0	51%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

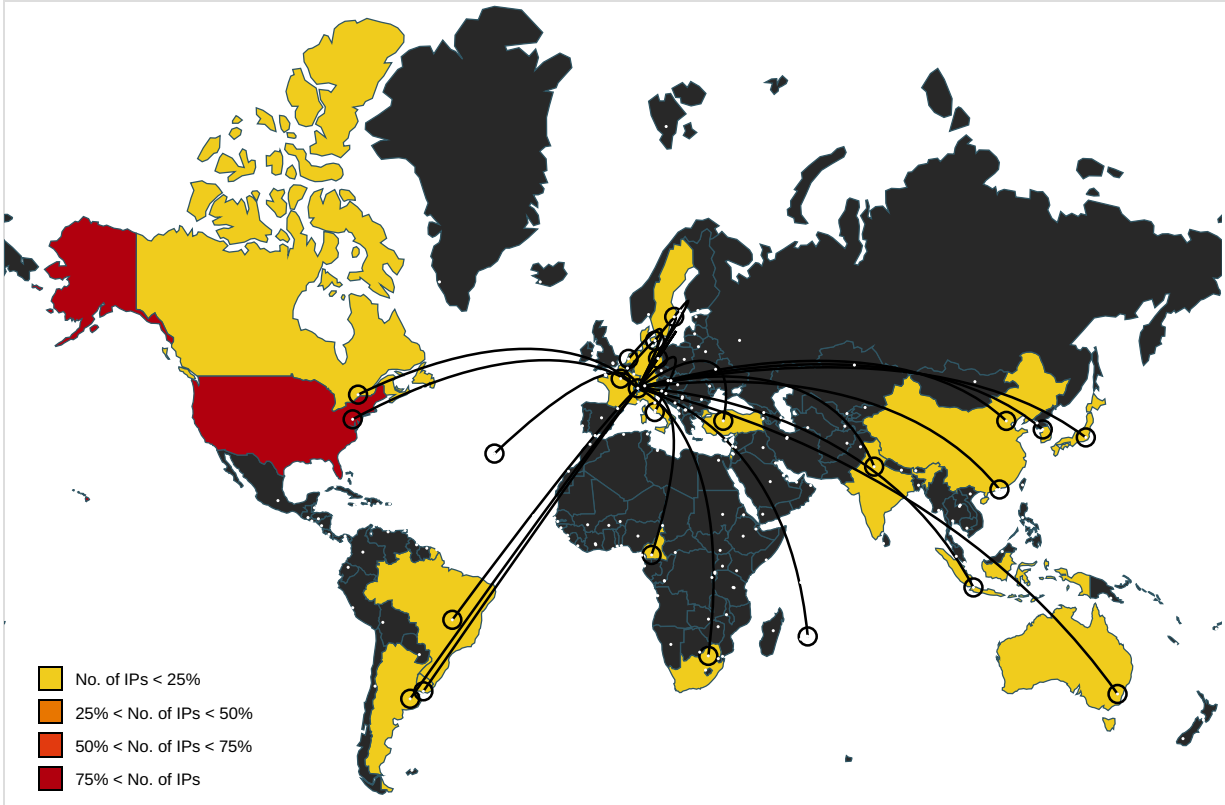
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
168.199.202.201	unknown	United States		264757	GALLOVICENTEAR	false
150.44.183.19	unknown	Japan		9991	SHUDO-UHiroshimaShudoUniversityJP	false
18.13.159.86	unknown	United States		3	MIT-GATEWAYSUS	false
77.173.178.44	unknown	Netherlands		1136	KPNKPNNationalEU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
126.24.142.249	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
72.54.152.63	unknown	United States		17184	ATL-CBEYONDUS	false
4.78.135.156	unknown	United States		3356	LEVEL3US	false
253.204.211.94	unknown	Reserved		unknown	unknown	false
53.110.115.41	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
79.181.131.77	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
142.31.146.148	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
167.159.138.239	unknown	United States		16988	IPAPERUS	false
222.120.81.51	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
245.152.136.82	unknown	Reserved		unknown	unknown	false
242.80.56.190	unknown	Reserved		unknown	unknown	false
223.126.250.170	unknown	China		58453	CMI-INT-HKLevel30Tower1HK	false
166.230.146.159	unknown	United States		29946	UNION-CELLUS	false
120.197.138.66	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
207.62.134.92	unknown	United States		2152	CSUNET-NWUS	false
47.38.202.110	unknown	United States		20115	CHARTER-20115US	false
123.75.94.21	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
190.178.224.253	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
36.211.134.114	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
44.245.91.182	unknown	United States		16509	AMAZON-02US	false
73.122.251.194	unknown	United States		7922	COMCAST-7922US	false
20.92.53.11	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
198.223.111.113	unknown	United States		6167	CELLCO-PARTUS	false
43.36.199.156	unknown	Japan		4249	LILLY-ASUS	false
112.155.118.62	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
171.188.4.158	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
172.126.83.5	unknown	United States		7018	ATT-INTERNET4US	false
114.203.165.12	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
195.180.36.66	unknown	Germany		4589	EASYNETEasynetGlobalServicesEU	false
135.123.1.243	unknown	United States		18676	AVAYAUS	false
179.82.200.112	unknown	Brazil		26599	TELEFONICABRASILSABR	false
119.147.192.68	unknown	China		4816	CHINANET-IDC-GDChinaTelecomGroupCN	false
204.107.47.96	unknown	United States		36092	CENTENEUS	false
212.159.237.202	unknown	European Union		29063	ATOS-NL-ASEindhovenNL	false
69.158.136.31	unknown	Canada		577	BACOMCA	false
167.107.163.97	unknown	United States		14799	EXP-EC2000US	false
155.111.161.22	unknown	United States		61153	PROCTERGAMBLENCSCDE	false
39.134.230.0	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
145.24.212.10	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
160.180.17.139	unknown	Italy		36903	MT-MPLSMA	false
54.135.223.195	unknown	United States		14618	AMAZON-AESUS	false
198.197.59.205	unknown	United States		292	ESNET-WESTUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
174.230.185.67	unknown	United States		22394	CELLCOUS	false
168.206.172.110	unknown	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	false
19.174.112.247	unknown	United States		3	MIT-GATEWAYSUS	false
76.228.30.240	unknown	United States		7018	ATT-INTERNET4US	false
167.58.180.37	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
133.29.224.39	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
88.238.39.231	unknown	Turkey		9121	TTNETTR	false
79.244.123.100	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
108.130.186.163	unknown	United States		16509	AMAZON-02US	false
91.33.106.70	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
250.107.140.6	unknown	Reserved		unknown	unknown	false
194.245.81.249	unknown	Germany		5517	CSLDE	false
177.59.108.172	unknown	Brazil		22085	ClaroSABR	false
147.19.211.229	unknown	United States		10796	TWC-10796-MIDWESTUS	false
18.234.211.50	unknown	United States		14618	AMAZON-AESUS	false
165.77.133.140	unknown	United States		4725	ODNSoftBankMobileCorpJP	false
165.38.170.201	unknown	United States		37053	RSAWEB-ASZA	false
136.241.186.233	unknown	United States		22174	NET-SUC-TECH-ALFUS	false
83.252.133.11	unknown	Sweden		39651	COMHEM-SWEDENSE	false
2.106.70.230	unknown	Denmark		3292	TDCTDCASDK	false
254.10.165.210	unknown	Reserved		unknown	unknown	false
207.24.202.205	unknown	United States		701	UUNETUS	false
168.215.97.191	unknown	United States		10753	LVLT-10753US	false
27.206.90.28	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
103.91.192.164	unknown	Australia		136521	TAFENSW-AS1-APTAFENSWAU	false
39.203.152.169	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
77.136.223.94	unknown	France		15557	LDCOMNETFR	false
97.69.69.6	unknown	United States		33363	BHN-33363US	false
210.38.58.248	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
16.135.247.4	unknown	United States		33383	HPESUS	false
102.119.201.157	unknown	Mauritius		23889	MauritiusTelecomMU	false
242.184.238.84	unknown	Reserved		unknown	unknown	false
13.151.161.248	unknown	United States		7018	ATT-INTERNET4US	false
36.9.94.93	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
221.230.6.111	unknown	China		23650	CHINANET-JS-AS-APASNumberforCHINANETjiangsuprovinceba	false
45.161.107.22	unknown	Brazil		268451	MINASTELECOMUNICACOESEPORTAISDEPROVEDORESLTDBR	false
104.178.245.211	unknown	United States		7018	ATT-INTERNET4US	false
248.139.233.80	unknown	Reserved		unknown	unknown	false
133.213.96.112	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
112.70.64.95	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
4.211.149.36	unknown	United States		3356	LEVEL3US	false
197.169.124.226	unknown	South Africa		37168	CELL-CZA	false
159.198.170.204	unknown	United States		21595	BAXTERUS	false
19.215.98.23	unknown	United States		3	MIT-GATEWAYSUS	false
133.178.151.58	unknown	Japan		385	AFCONC-BLOCK1-ASUS	false
176.28.40.73	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
158.57.112.25	unknown	United States		1932	CONEDUS	false
59.153.53.52	unknown	Hong Kong		38478	SUNNYVISION-AS-APSunnyVisionLimitedHK	false
76.20.122.181	unknown	United States		7922	COMCAST-7922US	false
74.110.216.199	unknown	United States		701	UUNETUS	false
66.194.62.13	unknown	United States		40455	MAPCOEXPRESSUS	false
171.57.98.135	unknown	India		9874	STARHUB-MOBILEStarHubLtdSG	false
250.213.10.215	unknown	Reserved		unknown	unknown	false
41.244.86.103	unknown	Cameroon		37620	VIETTEL-CM-ASCM	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, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.034603716214055
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	QuSDT8cmP0
File size:	60196
MD5:	d60f2b0aded8eb8614c30b43b6944fd9
SHA1:	8afb2e9490ca96238e6be2abd660da2350a220a5
SHA256:	478df6827563def2d75e26b35c3444f10474ebbe970766127f941f66a2e391da
SHA512:	d69875bbf39af8288d17710bf71b72a2225e4842353662a9535721807d1bfff472554d5bcebada949db61275da4ee7f63af93fe4dc18f893f5a9daccf0ef09c3
SSDEEP:	768:02oW+YBq9esj3ld89S6h/KpADsB06WslGiChXd//qxTxcO+hI7Q:02B+YBSesj3ld8wm/KeDsB06vlwKm7
File Content Preview:	.ELF.....4.....4. ...(.....x.....dt.Q.....@..(....@.86.....#.....aX..`....!....#...@.....".....`.....$#...#...@.. .....`....

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:	59796
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	0xe110	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1e1c0	0xe1c0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e1d8	0xe1d8	0x600	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x2e7dc	0xe7dc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2e7e4	0xe7e4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x2e7f0	0xe7f0	0x164	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x2e958	0xe954	0x288	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0xe954	0x3e	0x0	0x0		0	0	1

Program Segments

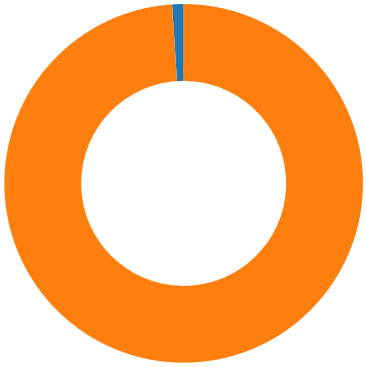
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x10000	0x10000	0xe7d8	0xe7d8	3.3762	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xe7dc	0x2e7dc	0x2e7dc	0x178	0x404	0.3411	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 97

- 23 (Telnet)
- 420 undefined



TCP Packets

System Behavior

Analysis Process: QuSDT8cmP0 PID: 5223, Parent PID: 5111

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	/tmp/QuSDT8cmP0
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: QuSDT8cmP0 PID: 5225, Parent PID: 5223

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: QuSDT8cmP0 PID: 5243, Parent PID: 5225

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5244**, Parent PID: **5225**

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5247**, Parent PID: **5244**

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5250**, Parent PID: **5247**

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5253**, Parent PID: **5247**

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5248**, Parent PID: **5244**

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5251**, Parent PID: **5244**

General

Start time:	04:23:16
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5226**, Parent PID: **5223**

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5227**, Parent PID: **5223**

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5231**, Parent PID: **5227**

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: QuSDT8cmP0 PID: **5261**, Parent PID: **5231**

General

Start time:	04:23:21
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5263**, Parent PID: **5231**

General

Start time:	04:23:21
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5232**, Parent PID: **5227**

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0

Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QuSDT8cmP0 PID: **5234**, Parent PID: **5227**

General

Start time:	04:23:07
Start date:	21/01/2022
Path:	/tmp/QuSDT8cmP0
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e