ID: 626473
Sample Name: csqe8VS0YI
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:14:29
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

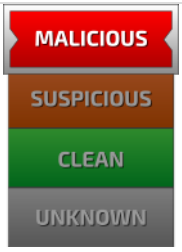
csqe8VS0YI

Overview

General Information

Sample Name:	csqe8VS0YI
Analysis ID:	626473
MD5:	beae05ed2e1e21.
SHA1:	ad4d5696752104.
SHA256:	a5cb465d21d917..
Tags:	32 elf mirai motorola
Infos:	

Detection



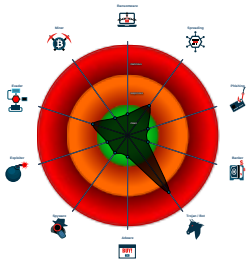
Mirai

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- 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…
- Sample listens on a socket
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626473
Start date and time: 14/05/202204:14:29	2022-05-14 04:14:29 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	csqe8VS0YI
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:	mal60.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/csqe8VS0YI
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- csqe8VS0YI (PID: 6230, Parent: 6123, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/csqe8VS0YI
  - csqe8VS0YI New Fork (PID: 6232, Parent: 6230)
    - csqe8VS0YI New Fork (PID: 6329, Parent: 6232)
    - csqe8VS0YI New Fork (PID: 6331, Parent: 6232)
      - csqe8VS0YI New Fork (PID: 6333, Parent: 6331)
        - csqe8VS0YI New Fork (PID: 6347, Parent: 6333)
        - csqe8VS0YI New Fork (PID: 6349, Parent: 6333)
      - csqe8VS0YI New Fork (PID: 6335, Parent: 6331)
      - csqe8VS0YI New Fork (PID: 6336, Parent: 6331)
  - csqe8VS0YI New Fork (PID: 6233, Parent: 6230)
  - csqe8VS0YI New Fork (PID: 6235, Parent: 6230)
    - csqe8VS0YI New Fork (PID: 6238, Parent: 6235)
      - csqe8VS0YI New Fork (PID: 6340, Parent: 6238)
      - csqe8VS0YI New Fork (PID: 6341, Parent: 6238)
    - csqe8VS0YI New Fork (PID: 6239, Parent: 6235)
    - csqe8VS0YI New Fork (PID: 6240, Parent: 6235)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

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

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

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

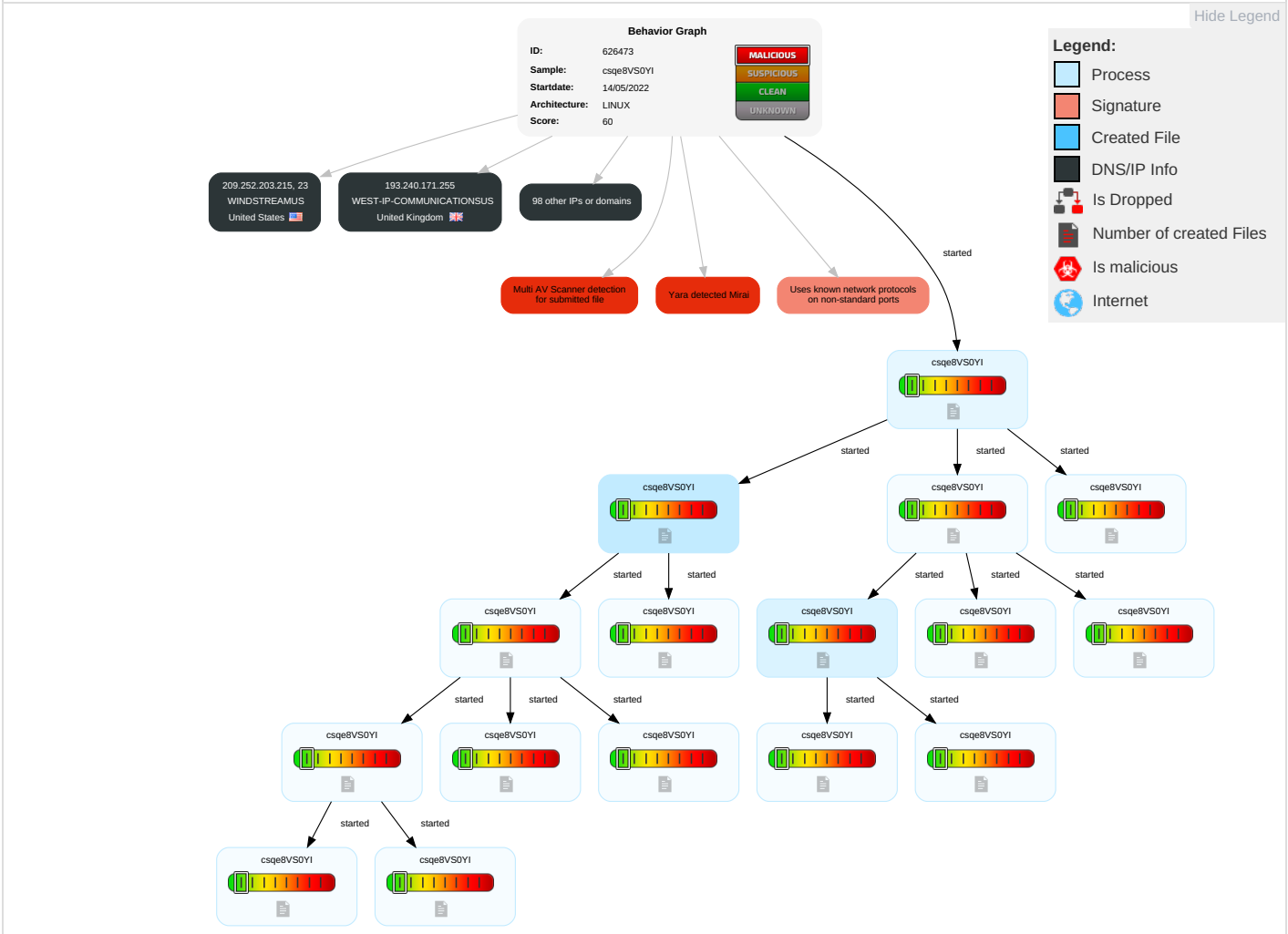
Mitre Att&ck Matrix

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	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 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
csqe8VS0YI	54%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

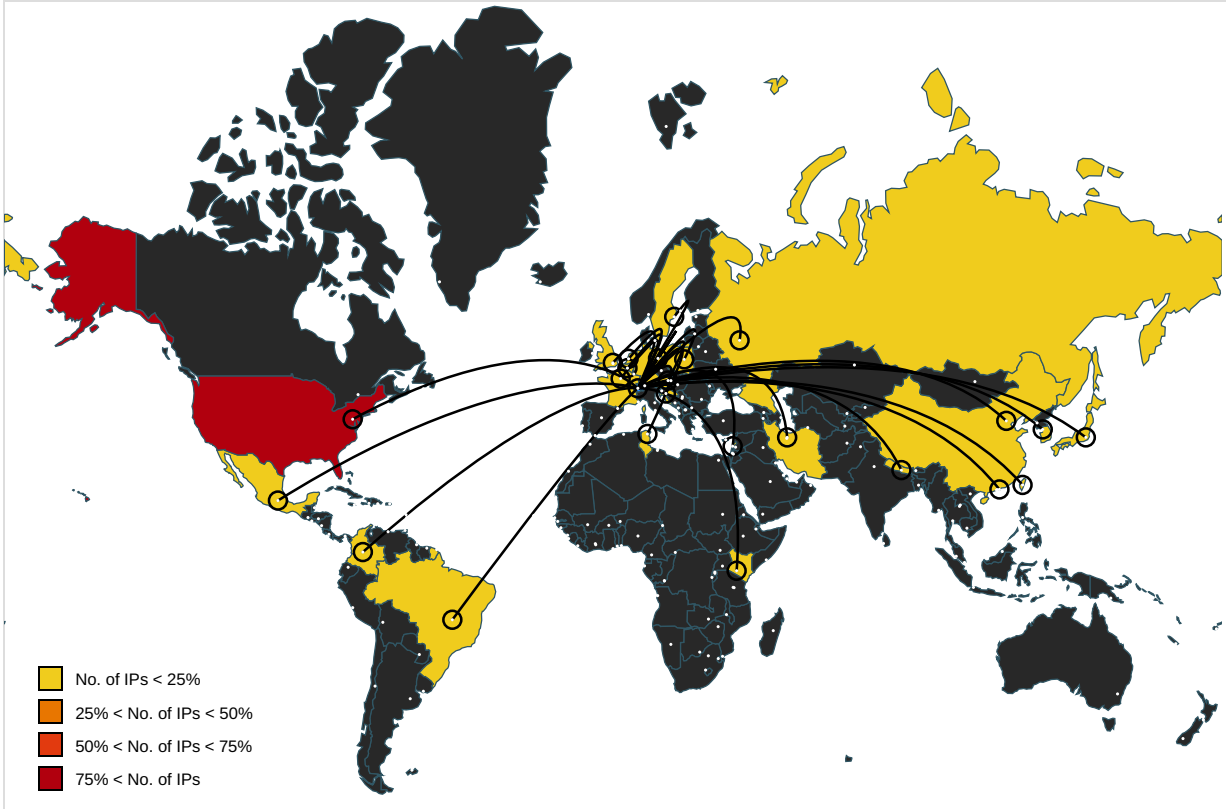
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
158.192.236.239	unknown	France		9159	CreditAgricoleFR	false
47.238.157.74	unknown	United States		20115	CHARTER-20115US	false
23.71.43.196	unknown	United States		7922	COMCAST-7922US	false
145.209.166.104	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
60.117.131.82	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
76.106.206.30	unknown	United States		7922	COMCAST-7922US	false
182.248.57.101	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
220.104.136.94	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
36.253.250.150	unknown	Nepal		38565	NCELL-AS-NPNcellPvtLtdNP	false
90.251.212.247	unknown	United Kingdom		5378	VodafoneGB	false
253.30.98.154	unknown	Reserved		unknown	unknown	false
53.189.202.203	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
60.86.254.10	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
69.142.24.95	unknown	United States		7922	COMCAST-7922US	false
196.102.183.56	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
121.126.241.161	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
63.211.32.11	unknown	United States		3356	LEVEL3US	false
167.20.171.244	unknown	United States		11273	FDCSGNETUS	false
78.36.89.177	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
125.137.19.123	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
194.96.24.204	unknown	Austria		1901	EUNETAT-ASA1TelekomAustriaAGAT	false
16.66.203.61	unknown	United States		unknown	unknown	false
157.25.81.76	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
78.119.21.74	unknown	France		8228	CEGETEL-ASFR	false
71.119.37.51	unknown	United States		701	UUNETUS	false
61.58.244.28	unknown	Taiwan; Republic of China (ROC)		9676	SAVECOM-TWSaveComInternationInc TW	false
110.90.152.15	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
191.64.65.243	unknown	Colombia		26611	COMCELSACO	false
157.247.81.176	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
164.171.252.182	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
157.169.11.71	unknown	France		2418	FR-ASNBLOCK2FR-MAN-SOPHIA-ANTIPOLISEU	false
247.23.178.56	unknown	Reserved		unknown	unknown	false
199.77.160.247	unknown	United States		3549	LVLT-3549US	false
141.72.50.93	unknown	Germany		553	BELWUEBelWue-KoordinationEU	false
197.2.168.196	unknown	Tunisia		37705	TOPNETTN	false
122.93.82.223	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
57.198.102.60	unknown	Belgium		2686	ATGS-MMD-ASUS	false
171.206.181.115	unknown	United States		10794	BANKAMERICAUS	false
72.12.236.220	unknown	United States		23175	POGOZONEUS	false
5.106.241.192	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
117.142.77.183	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
185.57.37.79	unknown	United Kingdom		202206	MOTIVEGB	false
4.45.158.73	unknown	United States		3356	LEVEL3US	false
86.9.17.184	unknown	United Kingdom		5089	NTLGB	false
175.253.176.76	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
149.22.102.39	unknown	United States		48945	IFNL-ASGB	false
123.213.36.98	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.240.171.255	unknown	United Kingdom		32880	WEST-IP-COMMUNICATIONSUS	false
46.225.224.140	unknown	Iran (ISLAMIC Republic Of)		56402	DADEHGOSTAR-ASAS12880-DataCommunicationCompanyofIran	false
77.37.132.41	unknown	Russian Federation		42610	NCNET-ASRU	false
82.13.54.81	unknown	United Kingdom		5089	NTLGB	false
108.243.44.253	unknown	United States		7018	ATT-INTERNET4US	false
253.11.226.229	unknown	Reserved		unknown	unknown	false
212.63.201.26	unknown	Sweden		30880	SPACEDUMP-ASThisASNislocatedonSTHIXatTulegatanStoka	false
43.90.242.228	unknown	Japan		4249	LILLY-ASUS	false
217.171.229.85	unknown	Netherlands		39647	REDHOSTING-ASNL	false
130.172.61.17	unknown	United States		12173	UAUS	false
186.253.253.55	unknown	Brazil		26615	TIMSABR	false
82.41.252.140	unknown	United Kingdom		5089	NTLGB	false
101.196.10.60	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
78.0.185.207	unknown	Croatia (LOCAL Name: Hrvatska)		5391	T-HTCroatianTelecomIncHR	false
37.140.115.105	unknown	Russian Federation		8369	INTERSVYAZ-AS38-BKomsomolskyprospektRU	false
168.92.214.232	unknown	United States		2707	FIRSTCOMM-AS1US	false
133.30.102.10	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
218.174.111.179	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
121.47.14.242	unknown	China		9811	BJGYsritcorpbeijingCN	false
154.23.227.237	unknown	United States		174	COGENT-174US	false
172.50.129.167	unknown	United States		21928	T-MOBILE-AS21928US	false
47.177.246.214	unknown	United States		5650	FRONTIER-FRTRUS	false
131.2.148.22	unknown	United States		61458	GOBIERNOAUTONOMOMUNICIPALDELAPAZBO	false
16.80.45.102	unknown	United States		unknown	unknown	false
222.58.250.219	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
38.216.139.33	unknown	United States		174	COGENT-174US	false
211.77.208.95	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
168.222.253.144	unknown	United States		2386	INS-ASUS	false
77.75.95.129	unknown	Lebanon		43019	FARAHNETLB	false
20.87.29.200	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
88.75.86.235	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
157.194.75.140	unknown	United States		4704	SANNETRakutenMobileIncJP	false
121.84.13.175	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
187.211.112.31	unknown	Mexico		8151	UninetSAdeCVMX	false
180.79.223.180	unknown	China		17429	BGCTVNETBEIJINGGEHUACATVNETWORKCOLTDCN	false
14.136.29.157	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	false
43.24.50.81	unknown	Japan		4249	LILLY-ASUS	false
253.191.50.137	unknown	Reserved		unknown	unknown	false
151.102.159.77	unknown	United States		32104	WELLMONT-TNUS	false
206.215.223.109	unknown	United States		11139	CWC-ROC-11139DM	false
249.32.109.223	unknown	Reserved		unknown	unknown	false
192.156.4.224	unknown	United States		721	DNIC-ASBLK-00721-00726US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
113.2.23.226	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
39.26.92.198	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
199.98.250.182	unknown	United States		174	COGENT-174US	false
209.252.203.215	unknown	United States		7029	WINDSTREAMUS	false
63.251.15.172	unknown	United States		32475	SINGLEHOP-LLCUS	false
184.134.171.230	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
35.188.132.78	unknown	United States		15169	GOOGLEUS	false
5.10.3.237	unknown	Germany		198726	KOMDSLDE	false
84.244.129.204	unknown	Netherlands		20495	WEDAREwd6NETBVNL	false
208.127.60.11	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
75.112.13.129	unknown	United States		33363	BHN-33363US	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, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.212939322901568
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	csqe8VS0YI
File size:	53056
MD5:	beae05ed2e1e2189d5f44fe5fe95111a
SHA1:	ad4d569675210467533e6093f3b13f805c860a28
SHA256:	a5cb465d21d9171b83bbbb658bbea9c875e421e37603f5e576c6387570fed6c6

SHA512:	950a85fe50fed766415ba25b66a321eb59ed39332815d1a3c2297549f7a68aca90fff3e7ef20c58aa0a7382c64360dc1141fbe6dfa66556931ce1d1d8c0142ea
SSDEEP:	768:mLGOe2kf9e9X9nberzI2vcv/QP3w5gFHviPuzWeHXpi2UJTMDnH638g5:mL/4f8F1eB0ApFvimzpZi2UJanHY8A
TLSH:	A8333ADAB902AD7DF98BEABE80170E0AB23123541053073777EBFC937E321549956E46
File Content Preview:	.ELF.....D...4.....4. ...(..... .....p..... .dt.Q.....NV..a....da.....N^NuNV..J9...pf>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy....N.X.....pN^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	52656
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

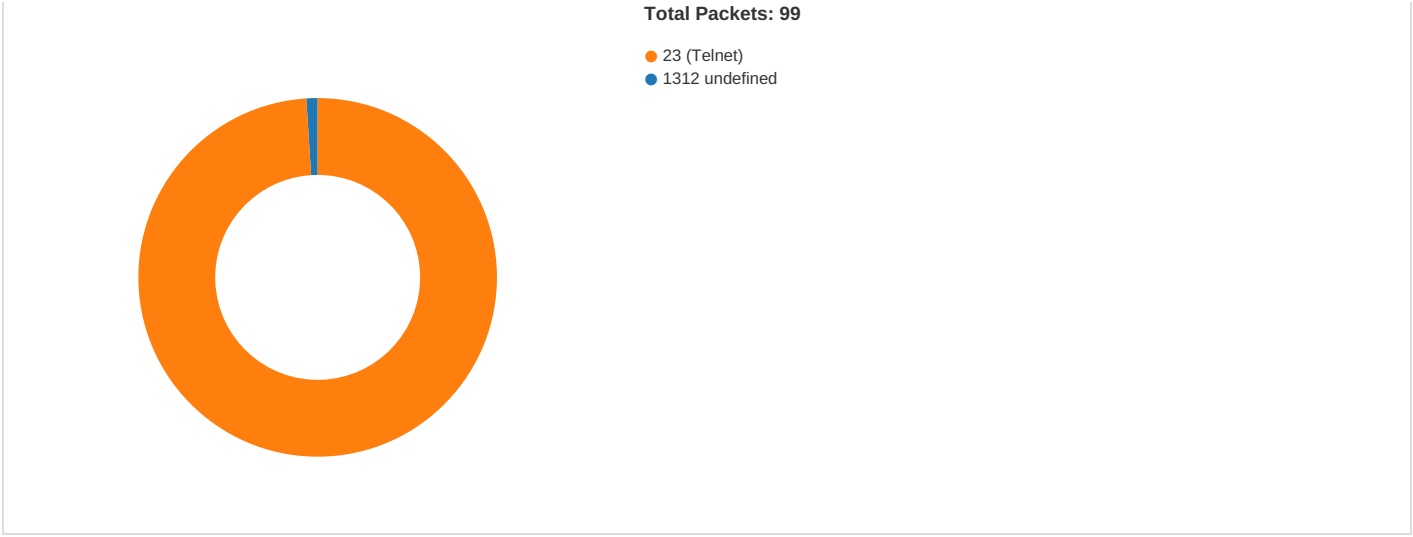
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xc5d6	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000c67e	0xc67e	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000c68c	0xc68c	0x56e	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x8000ec00	0xcc00	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8000ec08	0xcc08	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8000ec14	0xcc14	0x15c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x8000ed70	0xcd70	0x23c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xcd70	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	0x80000000	0x80000000	0xcbfa	0xcbfa	4.2327	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xcc00	0x8000ec00	0x8000ec00	0x170	0x3ac	0.2775	0x6	RW	0x2000		.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: csqe8VS0YI PID: 6230, Parent PID: 6123

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	/tmp/csqe8VS0YI
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: csqe8VS0YI PID: 6232, Parent PID: 6230

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: csqe8VS0YI PID: 6329, Parent PID: 6232

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6331**, Parent PID: **6232**

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6333**, Parent PID: **6331**

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6347**, Parent PID: **6333**

General

Start time:	04:18:10
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6349**, Parent PID: **6333**

General

Start time:	04:18:10
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6335**, Parent PID: **6331**

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6336**, Parent PID: **6331**

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6233**, Parent PID: **6230**

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6235**, Parent PID: **6230**

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6238**, Parent PID: **6235**

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: csqe8VS0YI PID: **6340**, Parent PID: **6238**

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6341**, Parent PID: **6238**

General

Start time:	04:18:05
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6239**, Parent PID: **6235**

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: csqe8VS0YI PID: **6240**, Parent PID: **6235**

General

Start time:	04:15:13
Start date:	14/05/2022
Path:	/tmp/csqe8VS0YI
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc