ID: 626465
Sample Name: VQemUYjLmL
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:00:30
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

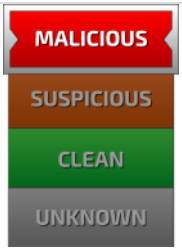
VQemUYjLmL

Overview

General Information

Sample Name:	VQemUYjLmL
Analysis ID:	626465
MD5:	9bf5c9ac9cacd5…
SHA1:	b57f925cbdad94..
SHA256:	9cae0351a33e4b..
Tags:	32 elf intel mirai
Infos:	

Detection



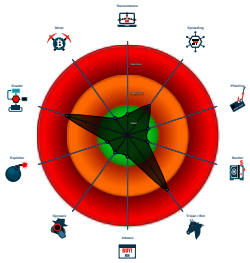
Mirai

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- 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…
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

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:	626465
Start date and time: 14/05/202204:00:30	2022-05-14 04:00:30 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VQemUYjLmL
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.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/VQemUYjLmL
PID:	6227
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- VQemUYjLmL (PID: 6227, Parent: 6122, MD5: 9bf5c9ac9cacd58b0d008938167c3d7d) Arguments: /tmp/VQemUYjLmL
  - VQemUYjLmL New Fork (PID: 6228, Parent: 6227)
    - VQemUYjLmL New Fork (PID: 6320, Parent: 6228)
    - VQemUYjLmL New Fork (PID: 6322, Parent: 6228)
      - VQemUYjLmL New Fork (PID: 6323, Parent: 6322)
        - VQemUYjLmL New Fork (PID: 6329, Parent: 6323)
        - VQemUYjLmL New Fork (PID: 6330, Parent: 6323)
      - VQemUYjLmL New Fork (PID: 6324, Parent: 6322)
      - VQemUYjLmL New Fork (PID: 6325, Parent: 6322)
    - VQemUYjLmL New Fork (PID: 6229, Parent: 6227)
    - VQemUYjLmL New Fork (PID: 6230, Parent: 6227)
      - VQemUYjLmL New Fork (PID: 6231, Parent: 6230)
        - VQemUYjLmL New Fork (PID: 6319, Parent: 6231)
        - VQemUYjLmL New Fork (PID: 6321, Parent: 6231)
      - VQemUYjLmL New Fork (PID: 6232, Parent: 6230)
      - VQemUYjLmL New Fork (PID: 6233, Parent: 6230)
- **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

Data Obfuscation

Sample is packed with UPX

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

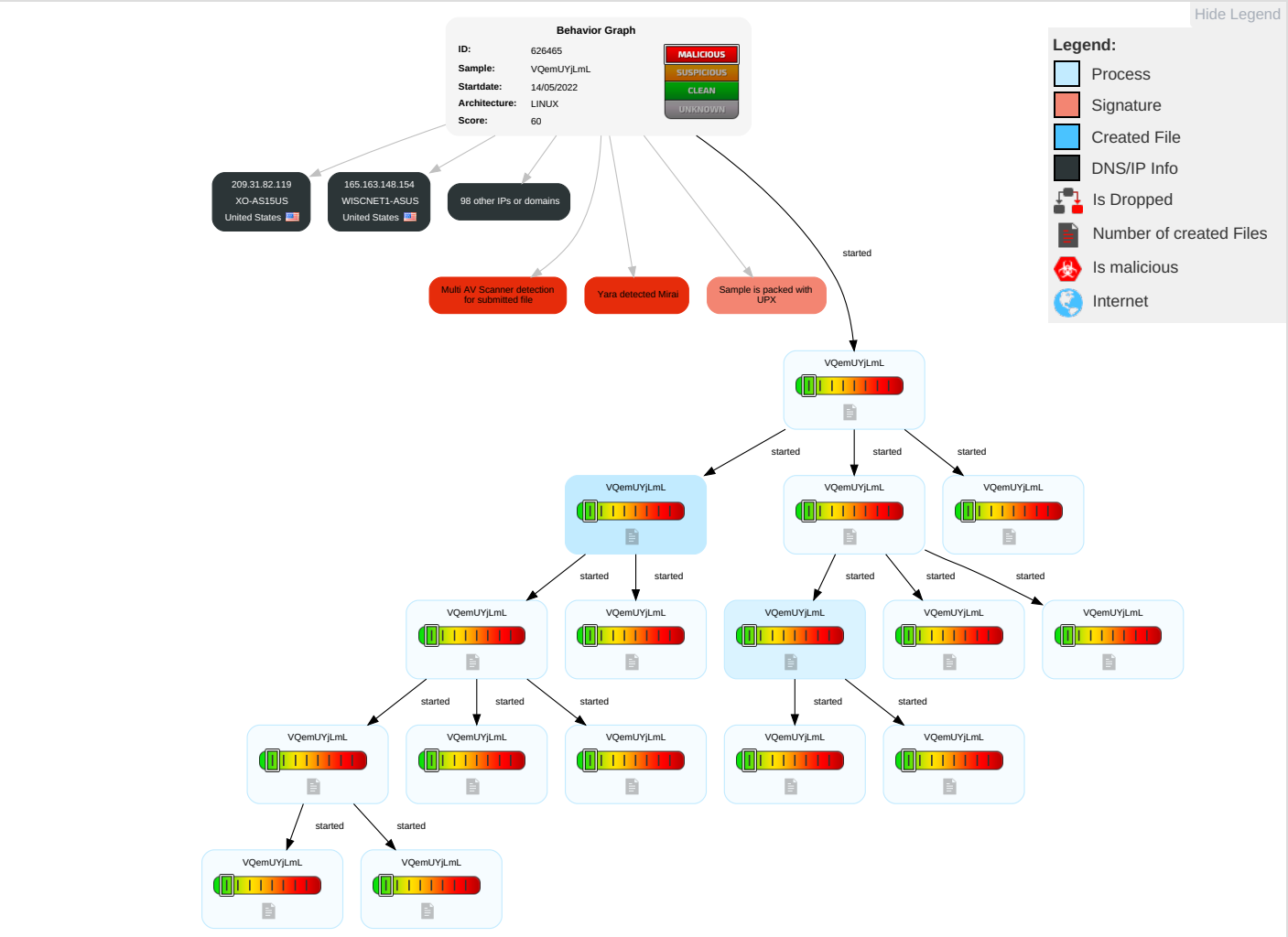
Mitre Att&ck Matrix

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 Obfuscated Files or Information	1 OS Credential Dumping	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
VQemUYjLmL	41%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

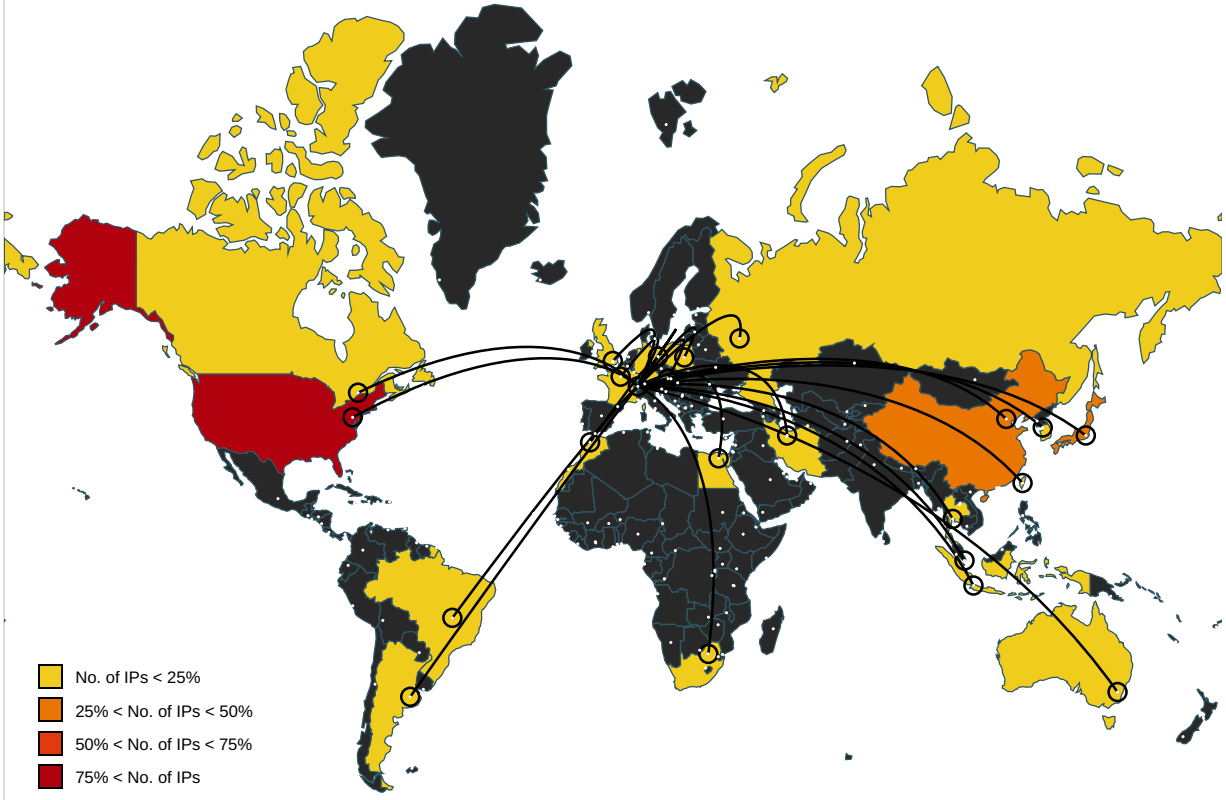
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.90.232.168	unknown	France		15557	LDCOMNETFR	false
133.76.4.145	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
44.14.96.139	unknown	United States		7377	UCSDUS	false
48.114.250.98	unknown	United States		2686	ATGS-MMD-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
180.7.246.116	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
18.54.163.197	unknown	United States		3	MIT-GATEWAYSUS	false
60.226.69.21	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
36.71.246.248	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
219.18.123.206	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
174.183.29.88	unknown	United States		7922	COMCAST-7922US	false
104.167.150.185	unknown	United States		54119	BOINGO-MDUUS	false
129.2.240.5	unknown	United States		27	UMDNETUS	false
180.83.51.239	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
83.20.34.90	unknown	Poland		5617	TPNETPL	false
114.215.215.176	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
100.237.194.125	unknown	United States		21928	T-MOBILE-AS21928US	false
157.78.204.8	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
181.11.124.60	unknown	Argentina		7303	TelecomArgentinaSAAR	false
211.232.248.235	unknown	Korea Republic of		17854	CABLELINE-AS-KRTbroadjeonjubroadcastKR	false
46.111.148.192	unknown	Russian Federation		2854	ROSPRINT-ASRU	false
165.163.148.154	unknown	United States		2381	WISCNET1-ASUS	false
172.218.17.202	unknown	Canada		852	ASN852CA	false
122.117.14.241	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
2.163.240.249	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
247.196.142.63	unknown	Reserved		unknown	unknown	false
86.104.240.210	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
160.172.158.31	unknown	Morocco		6713	IAM-ASMA	false
72.141.103.237	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
110.114.57.238	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
188.22.62.4	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
60.181.24.12	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.118.143.153	unknown	Japan		13041	CESCA-ACES	false
122.207.7.246	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
169.1.9.95	unknown	South Africa		37611	AfrihostZA	false
32.47.84.117	unknown	United States		7018	ATT-INTERNET4US	false
133.86.79.15	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
167.249.143.193	unknown	Brazil		265191	SapucaiaComercioeinformaticaltda-meBR	false
12.133.82.82	unknown	United States		7018	ATT-INTERNET4US	false
189.59.13.46	unknown	Brazil		18881	TELEFONICABRASILSABR	false
81.2.167.134	unknown	Germany		48945	IFNL-ASGB	false
223.39.61.40	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
161.162.127.148	unknown	United States		263740	CorporacionLaceibanetsocietyHN	false
47.77.27.116	unknown	United States		9500	VODAFONE-TRANSIT-ASVodafoneNZLtdNZ	false
45.75.223.36	unknown	United Kingdom		49425	DIGITAL-REALTY-UKGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.157.80.169	unknown	United States		10507	SPCSUS	false
243.114.242.13	unknown	Reserved		unknown	unknown	false
111.105.27.172	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
165.190.212.86	unknown	United States		8122	DQNASUS	false
63.185.84.28	unknown	United States		1239	SPRINTLINKUS	false
207.48.145.200	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
61.201.19.84	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
44.161.29.169	unknown	United States		7377	UCSDUS	false
8.182.167.78	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
87.74.186.30	unknown	United Kingdom		25310	ASN-CWACCESSGB	false
48.170.71.32	unknown	United States		2686	ATGS-MMD-ASUS	false
120.170.161.61	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
91.34.209.170	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
167.97.254.148	unknown	United States		2055	LSU-1US	false
27.220.236.35	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
162.197.117.219	unknown	United States		7018	ATT-INTERNET4US	false
1.74.87.160	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
97.20.82.172	unknown	United States		22394	CELLCOUS	false
196.94.216.24	unknown	Morocco		6713	IAM-ASMA	false
110.127.67.241	unknown	China		134810	CMNET-JILIN-AS-APChinaMobileGroupJiLincommunicationsco	false
245.151.17.52	unknown	Reserved		unknown	unknown	false
5.117.38.89	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
61.121.4.183	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
47.112.150.22	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
171.90.160.62	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
195.210.114.17	unknown	United Kingdom		207088	ADOARDGB	false
40.187.124.6	unknown	United States		4249	LILLY-ASUS	false
24.125.4.208	unknown	United States		7922	COMCAST-7922US	false
114.128.202.91	unknown	Thailand		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
91.131.88.159	unknown	Austria		1257	TELE2EU	false
17.22.101.200	unknown	United States		714	APPLE-ENGINEERINGUS	false
105.44.152.180	unknown	Egypt		37069	MOBINILEG	false
113.222.205.206	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
211.52.43.39	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
119.46.20.101	unknown	Thailand		7470	TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	false
207.10.102.26	unknown	United States		7029	WINDSTREAMUS	false
175.44.144.191	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
111.71.144.64	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.191.43.142	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
44.60.240.93	unknown	United States		7377	UCSDUS	false
106.140.171.118	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
97.4.220.39	unknown	United States		22394	CELLCOUS	false
4.189.101.243	unknown	United States		3356	LEVEL3US	false
250.57.112.223	unknown	Reserved		unknown	unknown	false
96.224.76.167	unknown	United States		701	UUNETUS	false
207.166.46.247	unknown	United States		2152	CSUNET-NWUS	false
23.164.102.139	unknown	Reserved		19382	ONCORECA	false
63.89.37.130	unknown	United States		701	UUNETUS	false
168.215.26.59	unknown	United States		10753	LVLT-10753US	false
34.194.134.3	unknown	United States		14618	AMAZON-AESUS	false
218.212.188.164	unknown	Singapore		55430	STARHUB-NGNBNStarhubLtdSG	false
249.17.189.36	unknown	Reserved		unknown	unknown	false
252.66.185.166	unknown	Reserved		unknown	unknown	false
85.9.126.180	unknown	Iran (ISLAMIC Republic Of)		49100	IR-THR-PTEIR	false
209.31.82.119	unknown	United States		2828	XO-AS15US	false
197.87.110.49	unknown	South Africa		10474	OPTINETZA	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 LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped

Entropy (8bit):	7.872106803634582
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	VQemUYjLmL
File size:	24728
MD5:	9bf5c9ac9cacd58b0d008938167c3d7d
SHA1:	b57f925cbdad949ad41db5c57c0774a2cbf6d282
SHA256:	9cae0351a33e4b4c74263920dd8f1fee4e03d14022ff2caf631d367023b53fa8
SHA512:	e595bab9f1fa5f84f3b6bc201f49057846cb947e04fd7f012536db2db15e5a70e43d74a67807b09be6882f0e87e5347b5867228aee5296948c8a99326da19165
SSDEEP:	384:MVDKKQOcRpmYLdn6RBOFRFt5rUFt1diSAlCo3AnupsFNYrk4d1NEZgO8UXWozPLP:w/QOC0Yhn6ROHWFjicwNqFOXnNBxc8cv
TLSH:	A9B2E195E6FB27C3C2D19336E07C994DA2B21AC00746441B2109B64EA3DB60F47FF7A5
File Content Preview:	.ELF.....g..4.....4. ...(....._..._.....W...W.....Q.td.....tUPX!.....Z.....?d..ELF.....d.....4.,..4. (.....k.-.#.`.....?..P.....d..I

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

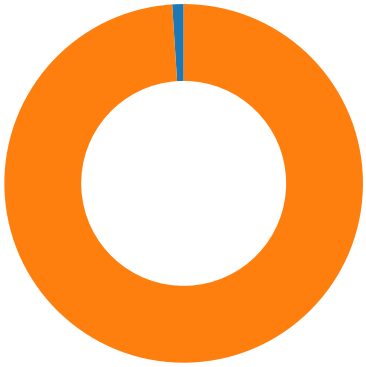
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0xc01000	0xc01000	0x5f9b	0x5f9b	4.5549	0x5	R E	0x1000		
LOAD	0x700	0x8055700	0x8055700	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 98

- 23 (Telnet)
- 1312 undefined



TCP Packets

System Behavior

Analysis Process: VQemUYjLmL PID: 6227, Parent PID: 6122

General

Start time:	04:01:17
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	/tmp/VQemUYjLmL
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: 6228, Parent PID: 6227

General

Start time:	04:01:17
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

File Activities

File Read

Directory Enumerated

Analysis Process: VQemUYjLmL PID: 6320, Parent PID: 6228

General

Start time:	04:04:09
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: 6322, Parent PID: 6228

General

Start time:	04:04:09

Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6323**, Parent PID: **6322**

General

Start time:	04:04:09
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6329**, Parent PID: **6323**

General

Start time:	04:04:14
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6330**, Parent PID: **6323**

General

Start time:	04:04:14
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6324**, Parent PID: **6322**

General

Start time:	04:04:09
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6325**, Parent PID: **6322**

General

Start time:	04:04:09
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6229**, Parent PID: **6227**

General

Start time:	04:01:17

Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6230**, Parent PID: **6227**

General

Start time:	04:01:17
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6231**, Parent PID: **6230**

General

Start time:	04:01:17
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

File Activities

File Read

Directory Enumerated

Analysis Process: VQemUYjLmL PID: **6319**, Parent PID: **6231**

General

Start time:	04:04:09
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6321**, Parent PID: **6231**

General

Start time:	04:04:09
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

Analysis Process: VQemUYjLmL PID: **6232**, Parent PID: **6230**

General

Start time:	04:01:17
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d

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

General

Start time:	04:01:17
Start date:	14/05/2022
Path:	/tmp/VQemUYjLmL
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	9bf5c9ac9cacd58b0d008938167c3d7d