ID: 680631
Sample Name: CQbdBGQLxY
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:40:10
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

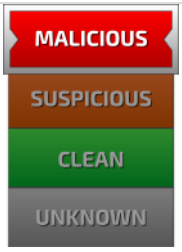
CQbdBGQLxY

Overview

General Information

Sample Name:	CQbdBGQLxY
Analysis ID:	680631
MD5:	47929fece58e2d..
SHA1:	32be30e6cb694f..
SHA256:	e62123b6b74435.
Tags:	32 elf mips mirai
Infos:	

Detection



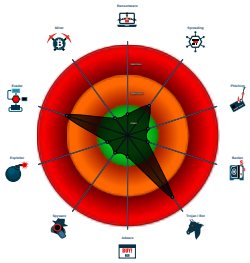
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample contains only a LOAD segm…
- Yara signature match
- 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…

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.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680631
Start date and time: 08/08/202222:40:10	2022-08-08 22:40:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CQbdBGQLxY
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:	mal80.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/CQbdBGQLxY
PID:	6231
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- CQbdBGQLxY (PID: 6231, Parent: 6124, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/CQbdBGQLxY
  - CQbdBGQLxY New Fork (PID: 6234, Parent: 6231)
    - CQbdBGQLxY New Fork (PID: 6332, Parent: 6234)
    - CQbdBGQLxY New Fork (PID: 6336, Parent: 6234)
      - CQbdBGQLxY New Fork (PID: 6339, Parent: 6336)
        - CQbdBGQLxY New Fork (PID: 6349, Parent: 6339)
        - CQbdBGQLxY New Fork (PID: 6350, Parent: 6339)
      - CQbdBGQLxY New Fork (PID: 6340, Parent: 6336)
      - CQbdBGQLxY New Fork (PID: 6342, Parent: 6336)
    - CQbdBGQLxY New Fork (PID: 6235, Parent: 6231)
    - CQbdBGQLxY New Fork (PID: 6236, Parent: 6231)
      - CQbdBGQLxY New Fork (PID: 6239, Parent: 6236)
        - CQbdBGQLxY New Fork (PID: 6331, Parent: 6239)
        - CQbdBGQLxY New Fork (PID: 6333, Parent: 6239)
      - CQbdBGQLxY New Fork (PID: 6241, Parent: 6236)
      - CQbdBGQLxY New Fork (PID: 6244, Parent: 6236)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
6349.1.00007f94a8400000.00007f94a8415000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6349.1.00007f94a8400000.00007f94a8415000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	0x13750:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13764:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13778:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1378c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x137a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x137b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x137c8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x137dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x137f0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13804:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13818:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1382c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13840:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13854:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13868:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1387c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x13890:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x138a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x138b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x138cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x138e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6349.1.00007f94a8400000.00007f94a8415000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	0x13ca8:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64
6231.1.00007f94a8400000.00007f94a8415000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6231.1.00007f94a8400000.00007f94a8415000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x13750:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13764:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13778:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1378c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x137a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x137b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x137c8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x137dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x137f0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13804:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13818:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1382c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13840:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13854:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13868:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1387c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x13890:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x138a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x138b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x138cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x138e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Click to see the 30 entries				

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

System Summary

Malicious sample detected (through community Yara rule)

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

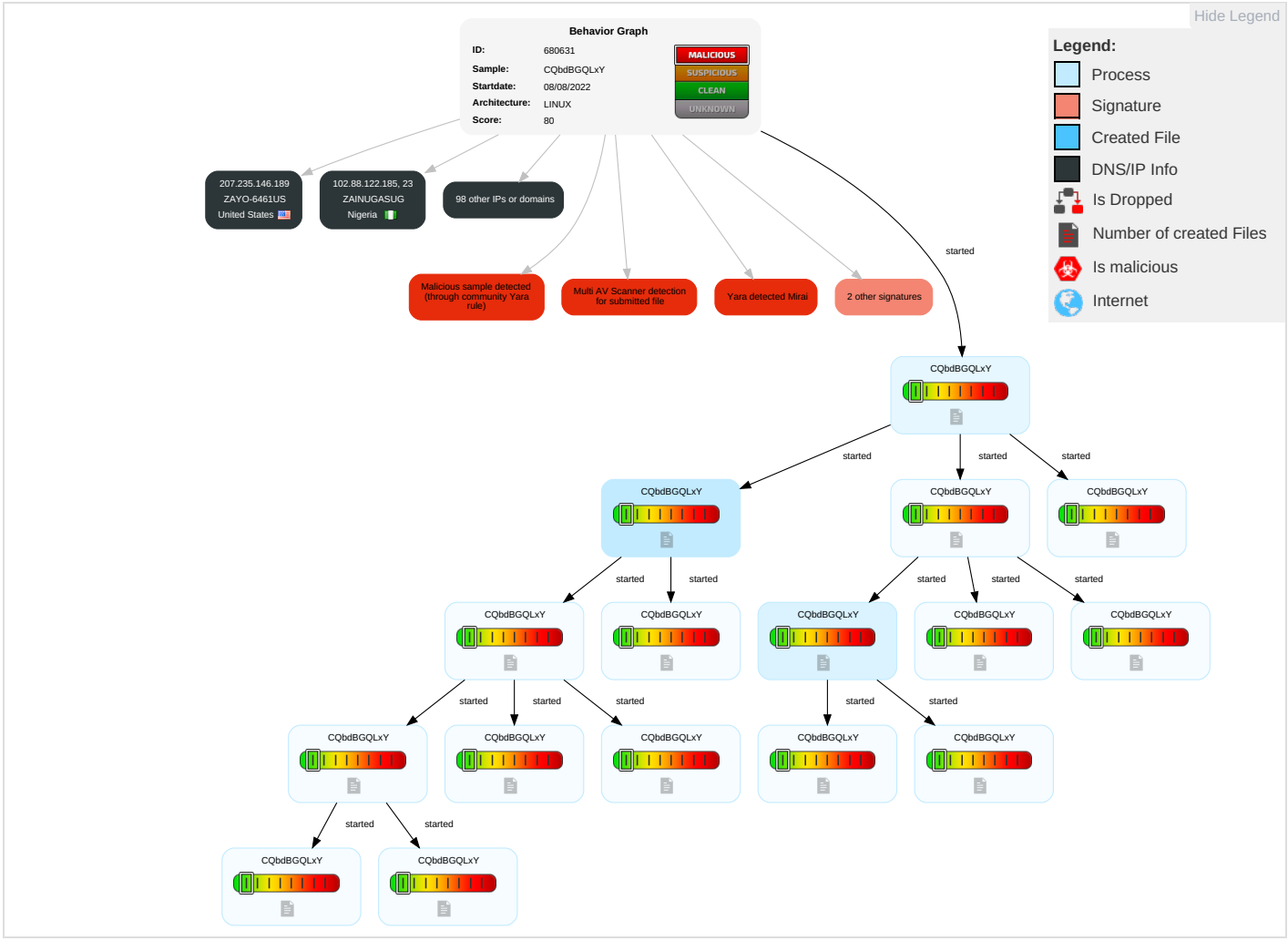
Mitre Att&ck Matrix

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	1 1 Obfuscated Files or Information	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
CQbdBGQLxY	31%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

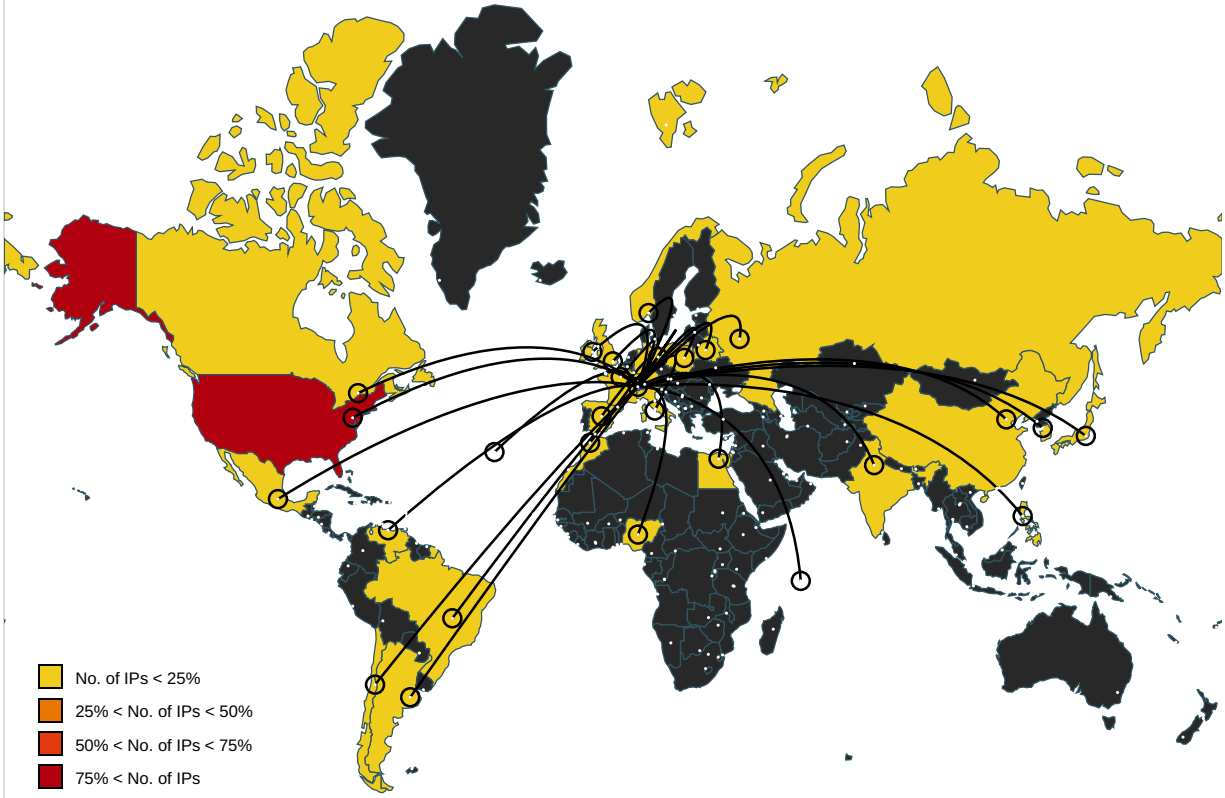
Domains and IPs

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
158.114.115.186	unknown	United States		1906	NORTHROP-GRUMMANUS	false
150.71.200.63	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
92.61.175.176	unknown	France		44334	RTLNET-ASNFR	false
168.193.227.196	unknown	United States		27435	OPSOURCE-INCUS	false
216.241.195.236	unknown	United States		26253	SCINTERNETUS	false
126.8.21.139	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
187.242.181.120	unknown	Mexico		13999	MegaCableSAdeCVMX	false
186.183.51.177	unknown	Argentina		28114	AlphaTelSAAR	false
194.138.243.190	unknown	Germany		9890	ATOSINFOTECH-SG-APATOSInformationTechnologySingaporeP	false
9.23.178.119	unknown	United States		3356	LEVEL3US	false
184.77.151.9	unknown	United States		16509	AMAZON-02US	false
217.90.37.135	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
39.95.30.225	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
161.165.220.46	unknown	United States		10695	WAL-MARTUS	false
255.29.179.209	unknown	Reserved		unknown	unknown	false
102.88.122.185	unknown	Nigeria		37075	ZAINUGASUG	false
136.21.145.8	unknown	United States		60311	ONEFMCH	false
105.188.238.139	unknown	Morocco		36925	ASMediMA	false
77.145.164.146	unknown	France		15557	LDCOMNETFR	false
98.167.23.172	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
94.134.62.55	unknown	Germany		8881	VERSATELDE	false
189.15.33.3	unknown	Brazil		53006	ALGARTELECOMSABR	false
207.235.146.189	unknown	United States		6461	ZAYO-6461US	false
173.48.189.199	unknown	United States		701	UUNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.43.161.8	unknown	United States		3	MIT-GATEWAYSUS	false
210.139.227.237	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
153.165.241.179	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
205.118.131.247	unknown	United States		210	WEST-NET-WESTUS	false
161.239.220.13	unknown	United States		396269	BPL-ASNUS	false
107.42.66.247	unknown	United States		16567	NETRIX-16567US	false
109.244.173.163	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
13.216.220.114	unknown	United States		16509	AMAZON-02US	false
27.118.193.125	unknown	Korea Republic of		17877	NEXG-AS-KRNexGCoLTDKR	false
223.30.216.231	unknown	India		9583	SIFY-AS-INSifyLimitedIN	false
90.65.88.183	unknown	France		3215	FranceTelecom-OrangeFR	false
82.209.199.193	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
207.234.30.248	unknown	United States		174	COGENT-174US	false
110.55.246.99	unknown	Philippines		6648	BAYAN-TELECOMMUNICATIONSBayanTelecommunicationsIncPH	false
19.67.92.67	unknown	United States		3	MIT-GATEWAYSUS	false
27.61.234.177	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
142.213.78.240	unknown	Canada		11489	BACICA	false
248.45.164.125	unknown	Reserved		unknown	unknown	false
194.36.194.232	unknown	France		44407	ASN-LINKTFR	false
121.226.140.134	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
194.73.176.78	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
109.114.39.46	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
175.75.128.105	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
52.0.100.66	unknown	United States		14618	AMAZON-AESUS	false
187.107.143.26	unknown	Brazil		28573	CLAROSABR	false
68.16.252.5	unknown	United States		7018	ATT-INTERNET4US	false
243.165.21.50	unknown	Reserved		unknown	unknown	false
4.125.32.240	unknown	United States		3356	LEVEL3US	false
111.48.127.50	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
190.45.54.169	unknown	Chile		22047	VTRBANDAANCHASACL	false
81.45.3.100	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
45.197.137.177	unknown	Seychelles		133201	COMING-ASABCDEGROUPCOMPANYLIMITEDHK	false
61.201.19.80	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
75.91.78.197	unknown	United States		7029	WINDSTREAMUS	false
92.150.193.44	unknown	France		3215	FranceTelecom-OrangeFR	false
70.51.151.21	unknown	Canada		577	BACOMCA	false
186.175.248.5	unknown	Chile		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
4.156.52.192	unknown	United States		3356	LEVEL3US	false
31.183.227.110	unknown	Poland		16342	TOYATOYASpzooPL	false
95.128.226.17	unknown	Russian Federation		48848	RU-TELSERVT-MIX-ASTelekomServisTatMoscowMMTS9RU	false
200.47.223.244	unknown	Venezuela		7908	BTLATAMVenezuelaSAVE	false
198.146.188.94	unknown	United States		19956	TENNESSEE-NETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
128.10.87.155	unknown	United States		17	PURDUEUS	false
197.40.144.153	unknown	Egypt		8452	TE-ASTE-ASEG	false
69.174.72.208	unknown	United States		3257	GTT-BACKBONEGTTDE	false
69.197.135.146	unknown	United States		32097	WIIUS	false
172.186.111.137	unknown	United States		7018	ATT-INTERNET4US	false
72.50.169.190	unknown	United States		12118	WVUUS	false
216.164.191.31	unknown	United States		6079	RCN-ASUS	false
35.250.210.220	unknown	United States		3549	LVLT-3549US	false
246.22.185.156	unknown	Reserved		unknown	unknown	false
182.102.87.147	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
97.16.25.170	unknown	United States		22394	CELLCOUS	false
218.124.73.228	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
2.93.165.206	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
100.171.61.116	unknown	United States		21928	T-MOBILE-AS21928US	false
192.117.120.159	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
180.137.245.19	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
223.214.104.17	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
82.147.41.177	unknown	Norway		29492	EIDSIVA-ASNNO	false
149.89.96.102	unknown	United States		12271	TWC-12271-NYCUS	false
203.87.148.36	unknown	Philippines		10139	SMARTBRO-PH-APSmartBroadbandIncPH	false
206.99.125.213	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
155.153.117.199	unknown	United States		1525	DNIC-ASBLK-01522-01526US	false
73.149.52.211	unknown	United States		7922	COMCAST-7922US	false
40.253.33.49	unknown	United States		4249	LILLY-ASUS	false
220.161.2.183	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
12.230.22.128	unknown	United States		7018	ATT-INTERNET4US	false
244.112.92.178	unknown	Reserved		unknown	unknown	false
179.39.153.57	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
14.51.227.109	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
166.4.200.124	unknown	United States		4152	USDA-1US	false
126.210.43.88	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
149.153.99.125	unknown	Ireland		1213	HEANETIE	false
173.244.199.136	unknown	United States		13213	UK2NET-ASGB	false
176.252.127.136	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.8941778942337715
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	CQbdBGQLxY
File size:	29952
MD5:	47929fece58e2d72d86fafe065d3a622
SHA1:	32be30e6cb694f2f99fe155dc732361349f71cab
SHA256:	e62123b6b7443519bfbd41179c389029d5a63f81d30a4280199cf6272996be8f
SHA512:	da3c68a4422c173e4d42eccc906a1edd5538aee6535a5b8356b74ef1441fb090106888d77aaf9b9403ba4cf54fd3692fb77bc7e20d4b93746ed05b63a1c7be87
SSDEEP:	384:d8pVWtmRsLYEpB6V8S628F0j/KcqJyNgmik8k4pDqFiapJ6u38hGvOtyrFRWGVCi:aMYHb62HScNgmIY5pJ5vOMzWO
TLSH:	29D2E0ED98B15086CB6C18FE40DC2F756E53F04133ABEA496720CC4AA6A2C4CBDD55BC
File Content Preview:	.ELF.....`..4.....4. ...(.....s...s.....p]..p]E.p]E.....UPX!d.....@]..@].....T.....?.E.h;....#.....b.L#0..L ..V...>.HZI.....yt.X.n.\...M.....K..ZA.n..0.....G..b[.....

Static ELF Info

ELF header

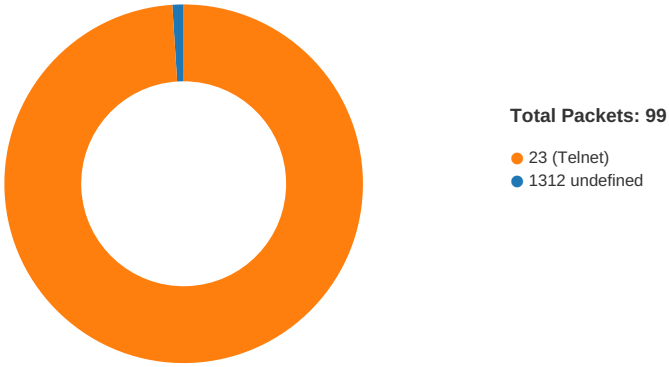
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x106080
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
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	0x100000	0x100000	0x73bd	0x73bd	7.8979	0x5	R E	0x10000		
LOAD	0x5d70	0x455d70	0x455d70	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: CQbdBGQLxY PID: 6231, Parent PID: 6124

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	/tmp/CQbdBGQLxY
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: CQbdBGQLxY PID: 6234, Parent PID: 6231

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: CQbdBGQLxY PID: 6332, Parent PID: 6234

General

Start time:	22:43:44
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: 6336, Parent PID: 6234

General

Start time:	22:43:44
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: 6339, Parent PID: 6336

General

Start time:	22:43:44
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: 6349, Parent PID: 6339

General

Start time:	22:43:49
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: 6350, Parent PID: 6339

General

Start time:	22:43:49
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: 6340, Parent PID: 6336

General

Start time:	22:43:44
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes

MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6342**, Parent PID: **6336**

General

Start time:	22:43:44
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6235**, Parent PID: **6231**

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6236**, Parent PID: **6231**

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6239**, Parent PID: **6236**

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: CQbdBGQLxY PID: **6331**, Parent PID: **6239**

General

Start time:	22:43:44
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6333**, Parent PID: **6239**

General

Start time:	22:43:44

Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6241**, Parent PID: **6236**

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: CQbdBGQLxY PID: **6244**, Parent PID: **6236**

General

Start time:	22:40:53
Start date:	08/08/2022
Path:	/tmp/CQbdBGQLxY
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9