ID: 680646
Sample Name: CLqMCUCXCO
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:11:37
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

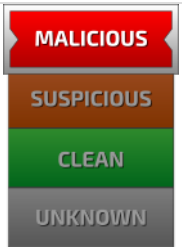
CLqMCUCXCO

Overview

General Information

Sample Name:	CLqMCUCXCO
Analysis ID:	680646
MD5:	0d9bef8f8f31226..
SHA1:	1f9e60bbbbf572c..
SHA256:	a0ef9bb1cde6cc…
Tags:	32 elf intel mirai
Infos:	

Detection



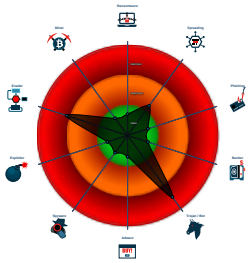
Mirai

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
- 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:	35.0.0 Citrine
Analysis ID:	680646
Start date and time: 08/08/202223:11:37	2022-08-08 23:11:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CLqMCUCXCO
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/CLqMCUCXCO
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- CLqMCUCXCO (PID: 6225, Parent: 6124, MD5: 0d9bef8f8f3122657c1861adf01c3eab) Arguments: /tmp/CLqMCUCXCO
  - CLqMCUCXCO New Fork (PID: 6226, Parent: 6225)
    - CLqMCUCXCO New Fork (PID: 6317, Parent: 6226)
    - CLqMCUCXCO New Fork (PID: 6318, Parent: 6226)
      - CLqMCUCXCO New Fork (PID: 6319, Parent: 6318)
        - CLqMCUCXCO New Fork (PID: 6327, Parent: 6319)
        - CLqMCUCXCO New Fork (PID: 6328, Parent: 6319)
      - CLqMCUCXCO New Fork (PID: 6322, Parent: 6318)
      - CLqMCUCXCO New Fork (PID: 6323, Parent: 6318)
    - CLqMCUCXCO New Fork (PID: 6227, Parent: 6225)
    - CLqMCUCXCO New Fork (PID: 6228, Parent: 6225)
      - CLqMCUCXCO New Fork (PID: 6229, Parent: 6228)
        - CLqMCUCXCO New Fork (PID: 6320, Parent: 6229)
        - CLqMCUCXCO New Fork (PID: 6321, Parent: 6229)
      - CLqMCUCXCO New Fork (PID: 6230, Parent: 6228)
      - CLqMCUCXCO New Fork (PID: 6231, Parent: 6228)
- **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
6320.1.0000000008048000.0000000008057000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6320.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xd2a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd2b4:$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 • 0xd2c8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd2dc:$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 • 0xd2f0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd304:$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 • 0xd318:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd32c:$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 • 0xd340:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd354:$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 • 0xd368:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd37c:$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 • 0xd390:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3a4:$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 • 0xd3b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3cc:$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 • 0xd3e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3f4:$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 • 0xd408:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd41c:$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 • 0xd430:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6320.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xd7f8:$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

Source	Rule	Description	Author	Strings
6320.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x5710:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3
6320.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Mirai_88de437f	unknown	unknown	• 0xa482:$a: 24 08 8B 4C 24 04 85 D2 74 0D 31 C0 89 F6 C6 04 08 00 40 39 D0
Click to see the 67 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

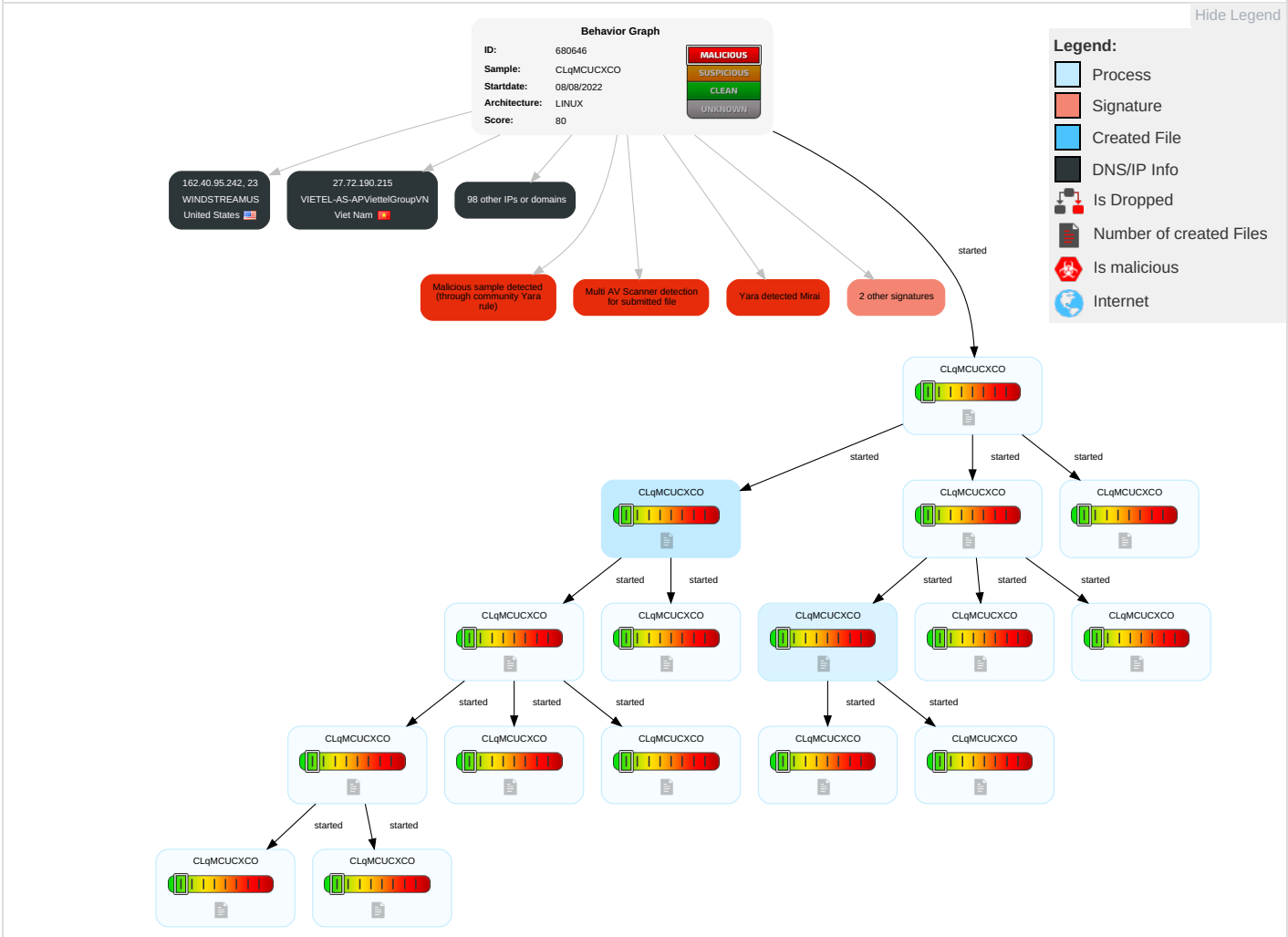
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated Files or Information	1 OS Credential Dumping	System Service 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
CLqMCUCXCO	39%	Virustotal		Browse
CLqMCUCXCO	56%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

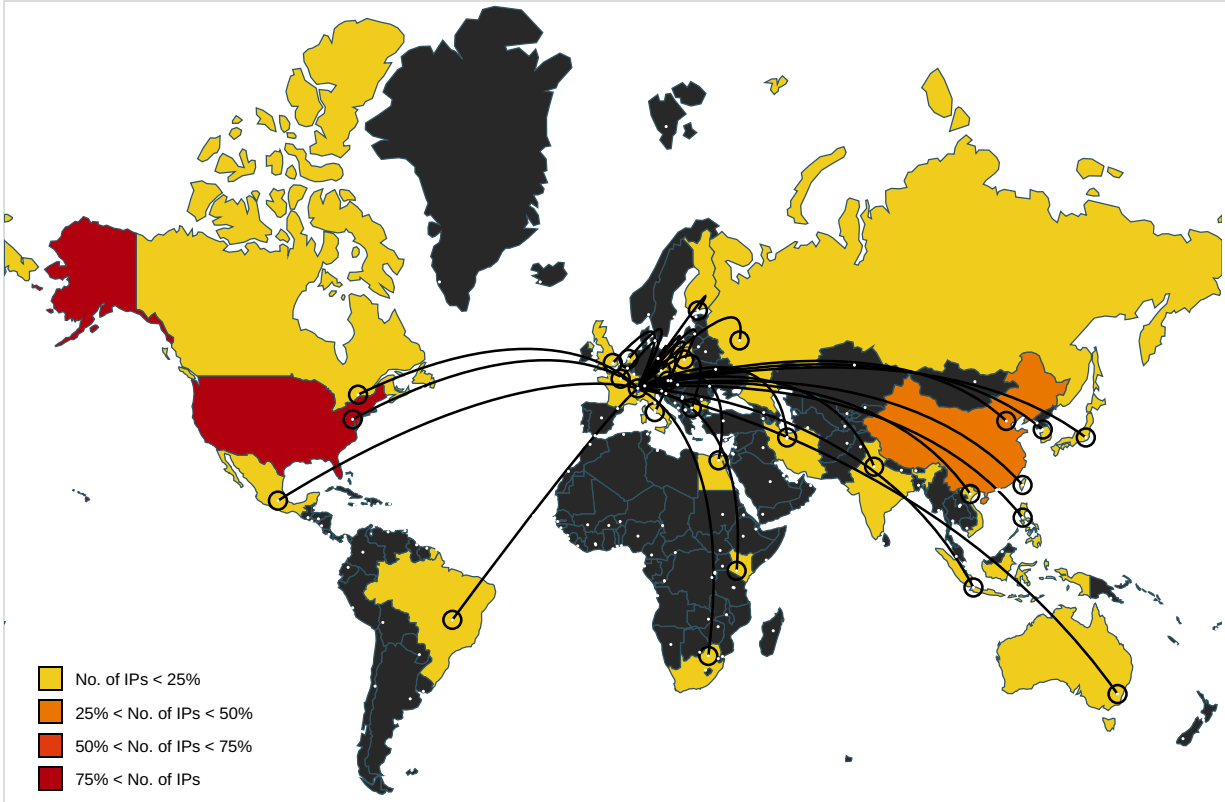
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
42.69.171.161	unknown	Taiwan; Republic of China (ROC)		4249	LILLY-ASUS	false
172.38.84.30	unknown	United States		21928	T-MOBILE-AS21928US	false
34.59.214.73	unknown	United States		2686	ATGS-MMD-ASUS	false
209.27.25.134	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
114.3.148.80	unknown	Indonesia		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
4.69.47.238	unknown	United States		3356	LEVEL3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
177.153.108.0	unknown	Brazil		27715	LocawebServicosdeInternetSABR	false
73.12.240.93	unknown	United States		7922	COMCAST-7922US	false
111.18.78.21	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
145.149.36.228	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
174.146.78.98	unknown	United States		10507	SPCSUS	false
219.56.55.60	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
119.167.80.219	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
162.40.95.242	unknown	United States		7029	WINDSTREAMUS	false
67.114.131.14	unknown	United States		7018	ATT-INTERNET4US	false
42.63.8.28	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
179.187.164.239	unknown	Brazil		18881	TELEFONICABRASILSABR	false
199.15.84.104	unknown	Canada		21775	AS-AFILIAS-REGISTRY-SERVICESCA	false
104.126.211.58	unknown	United States		16625	AKAMAI-ASUS	false
44.11.16.27	unknown	United States		7377	UCSDUS	false
20.220.220.209	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
24.226.21.21	unknown	Canada		7992	COGECOWAVECA	false
252.235.157.209	unknown	Reserved		unknown	unknown	false
185.119.218.28	unknown	Czech Republic		198167	APPTOCLOUDAppToCloudserversvpsCZ	false
116.188.238.145	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
196.24.228.7	unknown	South Africa		36982	UCTZA	false
169.9.204.201	unknown	United States		203	CENTURYLINK-LEGACY-LVLT-203US	false
185.110.97.136	unknown	France		21212	SIGFOXFR	false
126.73.1.19	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
112.236.34.178	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
255.15.2.172	unknown	Reserved		unknown	unknown	false
161.79.55.185	unknown	Brazil		2715	FundacaoCarlosChagasFilhodeAmparoaPesquisaBR	false
44.155.182.240	unknown	United States		1213	HEANETIE	false
153.74.2.118	unknown	United States		14962	NCR-252US	false
177.227.216.188	unknown	Mexico		13999	MegaCableSAdeCVMX	false
208.240.166.235	unknown	United States		4208	THE-ISERV-COMPANYUS	false
105.219.30.252	unknown	South Africa		16637	MTNNS-ASZA	false
101.161.253.77	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
146.150.30.12	unknown	United States		15169	GOOGLEUS	false
111.75.79.72	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
44.135.83.109	unknown	United States		7377	UCSDUS	false
69.1.193.170	unknown	United States		26091	INDDCUS	false
74.218.42.85	unknown	United States		10796	TWC-10796-MIDWESTUS	false
211.106.91.154	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
206.52.224.241	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
48.11.106.104	unknown	United States		2686	ATGS-MMD-ASUS	false
46.205.80.66	unknown	Poland		12912	TMPL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.5.192.223	unknown	United States		7922	COMCAST-7922US	false
45.106.6.110	unknown	Egypt		37069	MOBINILEG	false
184.193.182.209	unknown	United States		10507	SPCSUS	false
1.17.85.122	unknown	Korea Republic of		45996	GNJ-AS-KRDAOUTECHNOLOGYKR	false
167.97.21.240	unknown	United States		2055	LSU-1US	false
103.232.214.0	unknown	China		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	false
105.230.56.164	unknown	Kenya		36926	CKL1-ASNKE	false
96.135.51.166	unknown	United States		7922	COMCAST-7922US	false
180.21.226.128	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
86.55.160.156	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
144.28.237.126	unknown	United States		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
84.26.62.18	unknown	Netherlands		33915	TNF-ASNL	false
251.66.133.29	unknown	Reserved		unknown	unknown	false
251.150.175.57	unknown	Reserved		unknown	unknown	false
86.158.230.107	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
112.175.44.174	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
120.63.148.81	unknown	India		17813	MTNL-APMahanagarTelephoneNigamLimitedIN	false
167.170.59.192	unknown	United States		59447	SAYFANETTR	false
218.159.110.4	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
172.198.108.117	unknown	Australia		18747	IFX18747US	false
209.95.232.103	unknown	United States		10676	GLOBALECUS	false
221.130.31.143	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
202.175.229.220	unknown	Philippines		9658	ETPI-IDS-AS-APEasternTelecomsPhilsIncPH	false
125.255.115.5	unknown	Japan		1221	ASN-TELSTRATelstraCorporationLtdAU	false
207.63.247.0	unknown	United States		6325	ILLINOIS-CENTURYUS	false
253.80.95.162	unknown	Reserved		unknown	unknown	false
80.221.104.15	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
48.239.46.98	unknown	United States		2686	ATGS-MMD-ASUS	false
102.216.30.96	unknown	unknown		36926	CKL1-ASNKE	false
71.62.22.214	unknown	United States		7922	COMCAST-7922US	false
187.18.78.229	unknown	Brazil		22689	SercomtelParticipacoesSABR	false
79.19.93.106	unknown	Italy		3269	ASN-IBSNAZIT	false
158.220.98.173	unknown	Switzerland		8556	LEVANTISCH	false
166.177.101.119	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
123.13.43.130	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
219.179.242.156	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
249.172.233.233	unknown	Reserved		unknown	unknown	false
212.167.96.87	unknown	European Union		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
188.23.65.155	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
23.33.161.135	unknown	United States		16625	AKAMAI-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
118.193.69.175	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
205.176.123.6	unknown	United States		8103	STATE-OF-FLAUS	false
27.72.190.215	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
156.14.91.243	unknown	Italy		137	ASGARRConsortiumGARREU	false
144.91.156.168	unknown	Japan		131952	POTATO-NETAsahikawaCableTelevisionCoLtdJP	false
245.115.229.77	unknown	Reserved		unknown	unknown	false
71.69.198.211	unknown	United States		11426	TWC-11426-CAROLINASUS	false
42.139.61.221	unknown	China		4249	LILLY-ASUS	false
155.25.247.223	unknown	United States		1556	DNIC-ASBLK-01550-01601US	false
203.153.248.73	unknown	Australia		9822	AMNET-AU-APAmnetITServicesPtyLtdAU	false
109.173.24.136	unknown	Russian Federation		42610	NCNET-ASRU	false
115.40.220.193	unknown	Korea Republic of		9845	CJCKN-AS-KRLGHelloVisionCorpKR	false
5.53.131.174	unknown	Bulgaria		13124	IBGCBG	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):	7.86648515722169

TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	CLqMCUCXCO
File size:	27712
MD5:	0d9bef8f8f3122657c1861adf01c3eab
SHA1:	1f9e60bbbbf572cd3fb8f79004bacd0cdb624fc8
SHA256:	a0ef9bb1cde6cc4d41a0a4a594c631763bbfa93ee76879b372fd61a466f85590
SHA512:	4643472e4ef2edb069bdc7a8fd18528ecf2ecc639a5786c3b9e878039b3faf42fa1b9eb52e70c665d0cc7351df75c80a2619ccb2ac97977fe17e657b51646463
SSDEEP:	768:u5+Kcrb9VDJeS2KTgdTHOBcK5ZCAySapo:hlrb9ve2Tg9QB5VGq
TLSH:	1FC2E1A360F6CD03C4F2837A1E3D59A621606439634DDE2E77AA5BC837460E4657ECCB
File Content Preview:	.ELF.....Hs..4.....4. ...(.....Ck..Ck.....~...~.....Q.td.....UPX!.....P...P....._.....?d..ELF.....d.....4....4. (.....k.-.#. .....sw....$..w..\.\..A.

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:	0xc07348
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

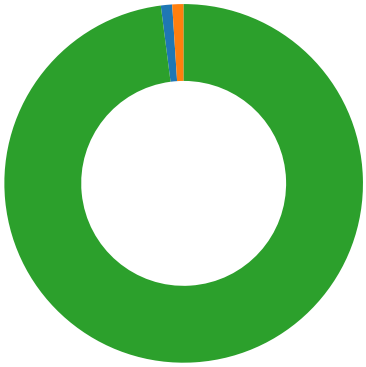
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0xc01000	0xc01000	0x6b43	0x6b43	7.8712	0x5	R E	0x1000		
LOAD	0xe80	0x8057e80	0x8057e80	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 98

- 23 (Telnet)
- 1312 undefined
- 443 (HTTPS)



TCP Packets

System Behavior

Analysis Process: CLqMCUCXCO PID: 6225, Parent PID: 6124

General

Start time:	23:12:24
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	/tmp/CLqMCUCXCO
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: 6226, Parent PID: 6225

General

Start time:	23:12:24
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

File Activities

File Read

Directory Enumerated

Analysis Process: CLqMCUCXCO PID: 6317, Parent PID: 6226

General

Start time:	23:15:16
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: 6318, Parent PID: 6226

General

Start time:	23:15:16

Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6319**, Parent PID: **6318**

General

Start time:	23:15:16
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6327**, Parent PID: **6319**

General

Start time:	23:15:21
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6328**, Parent PID: **6319**

General

Start time:	23:15:21
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6322**, Parent PID: **6318**

General

Start time:	23:15:16
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6323**, Parent PID: **6318**

General

Start time:	23:15:16
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6227**, Parent PID: **6225**

General

Start time:	23:12:24

Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6228**, Parent PID: **6225**

General

Start time:	23:12:24
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6229**, Parent PID: **6228**

General

Start time:	23:12:24
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

File Activities

File Read

Directory Enumerated

Analysis Process: CLqMCUCXCO PID: **6320**, Parent PID: **6229**

General

Start time:	23:15:16
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6321**, Parent PID: **6229**

General

Start time:	23:15:16
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6230**, Parent PID: **6228**

General

Start time:	23:12:24
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab

Analysis Process: CLqMCUCXCO PID: **6231**, Parent PID: **6228**

General

Start time:	23:12:24
Start date:	08/08/2022
Path:	/tmp/CLqMCUCXCO
Arguments:	n/a
File size:	27712 bytes
MD5 hash:	0d9bef8f8f3122657c1861adf01c3eab