ID: 680658
Sample Name: I95q6K4AMy
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:40:07
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

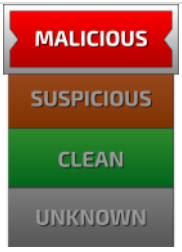
l95q6K4AMy

Overview

General Information

Sample Name:	l95q6K4AMy
Analysis ID:	680658
MD5:	a1d40f8e863472..
SHA1:	a23ea7dbd1ae98.
SHA256:	d80ab5938a57df..
Tags:	32 arm elf mirai
Infos:	

Detection



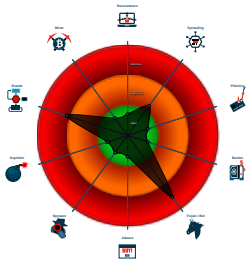
Mirai

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:	680658
Start date and time: 08/08/202223:40:07	2022-08-08 23:40:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	l95q6K4AMy
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/l95q6K4AMy
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- l95q6K4AMy (PID: 6226, Parent: 6121, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/l95q6K4AMy
  - l95q6K4AMy New Fork (PID: 6228, Parent: 6226)
    - l95q6K4AMy New Fork (PID: 6328, Parent: 6228)
    - l95q6K4AMy New Fork (PID: 6332, Parent: 6228)
      - l95q6K4AMy New Fork (PID: 6335, Parent: 6332)
        - l95q6K4AMy New Fork (PID: 6346, Parent: 6335)
        - l95q6K4AMy New Fork (PID: 6348, Parent: 6335)
      - l95q6K4AMy New Fork (PID: 6336, Parent: 6332)
      - l95q6K4AMy New Fork (PID: 6340, Parent: 6332)
  - l95q6K4AMy New Fork (PID: 6229, Parent: 6226)
  - l95q6K4AMy New Fork (PID: 6231, Parent: 6226)
    - l95q6K4AMy New Fork (PID: 6234, Parent: 6231)
      - l95q6K4AMy New Fork (PID: 6327, Parent: 6234)
      - l95q6K4AMy New Fork (PID: 6330, Parent: 6234)
    - l95q6K4AMy New Fork (PID: 6235, Parent: 6231)
    - l95q6K4AMy New Fork (PID: 6239, Parent: 6231)
- **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
6336.1.00007fd0dc017000.00007fd0dc029000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6336.1.00007fd0dc017000.00007fd0dc029000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xfc34:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfc48:$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 • 0xfc5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfc70:$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 • 0xfc84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfc98:$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 • 0xfcac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfcc0:$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 • 0xfcd4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfce8:$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 • 0xfcfc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd10:$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 • 0xfd24:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd38:$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 • 0xfd4c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd60:$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 • 0xfd74:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd88:$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 • 0xfd9c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfdb0:$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 • 0xfdc4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6336.1.00007fd0dc017000.00007fd0dc029000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x1018c:$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
6346.1.00007fd0dc017000.00007fd0dc029000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6346.1.00007fd0dc017000.00007fd0dc029000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xfc34:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfc48:$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 • 0xfc5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfc70:$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 • 0xfc84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfc98:$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 • 0xfcac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfcc0:$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 • 0xfcd4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfce8:$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 • 0xfcfc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd10:$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 • 0xfd24:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd38:$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 • 0xfd4c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd60:$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 • 0xfd74:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfd88:$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 • 0xfd9c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfdb0:$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 • 0xfdc4:$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 35 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

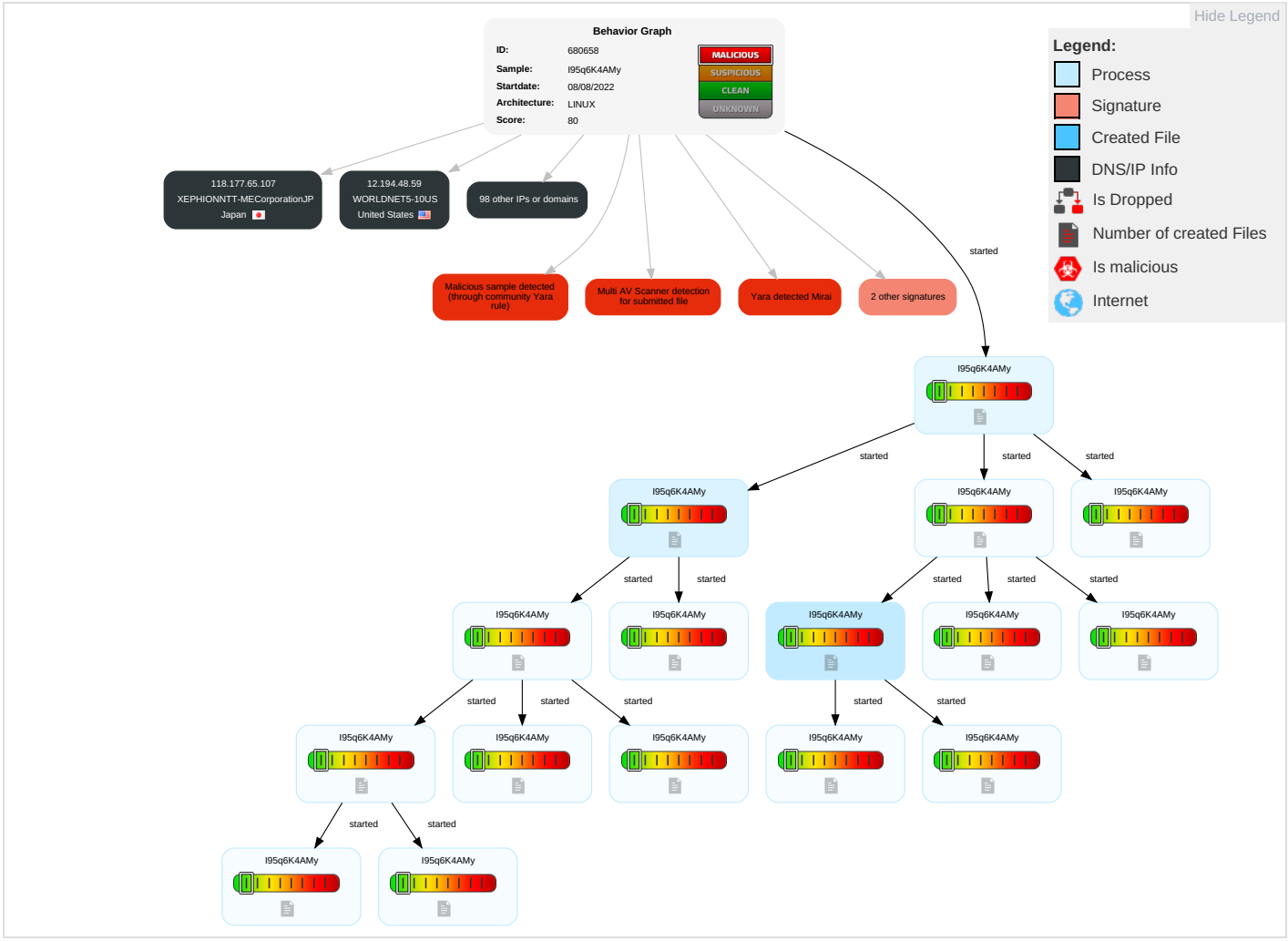
Mitre Att&ck Matrix

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
I95q6K4AMy	26%	Virustotal		Browse
I95q6K4AMy	38%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

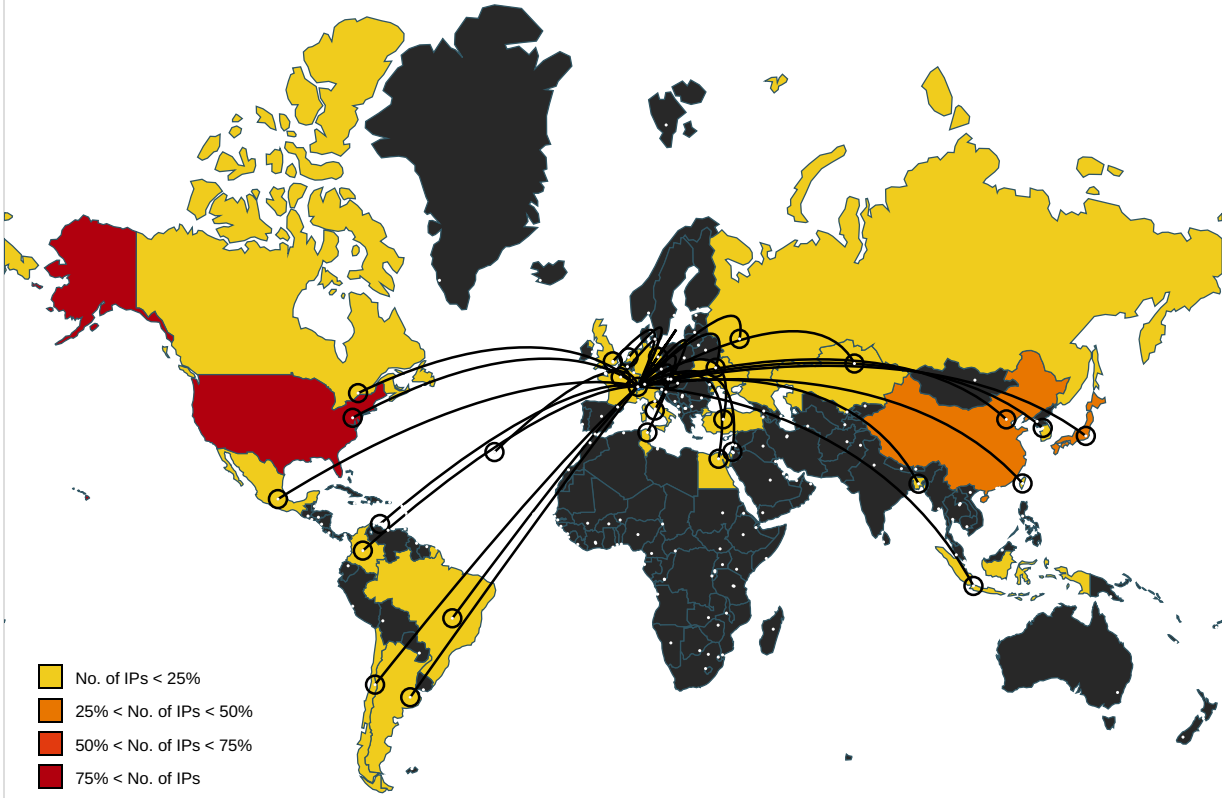
Domains and IPs

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
223.92.221.118	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
210.139.227.226	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
100.255.37.94	unknown	United States		21928	T-MOBILE-AS21928US	false
157.84.108.152	unknown	United Kingdom		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
12.194.48.59	unknown	United States		8030	WORLDNET5-10US	false
243.114.242.49	unknown	Reserved		unknown	unknown	false
18.207.133.64	unknown	United States		14618	AMAZON-AESUS	false
216.47.150.29	unknown	United States		29825	IIT-NETWORK-ASUS	false
205.241.14.240	unknown	United States		3364	CSDCO-ASUS	false
208.1.146.46	unknown	United States		1239	SPRINTLINKUS	false
150.121.57.75	unknown	China		4152	USDA-1US	false
198.123.247.37	unknown	United States		297	AS297US	false
126.149.55.110	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
178.40.197.80	unknown	Slovakia (SLOVAK Republic)		6855	SK-TELEKOMSK	false
124.80.10.191	unknown	Korea Republic of		17849	GINAMHANVIT-AS-KRTbroadGinamBroadcatingCoLtdKR	false
118.16.102.230	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
102.21.168.170	unknown	unknown		37054	Telecom-MalagasyMG	false
18.19.210.92	unknown	United States		3	MIT-GATEWAYSUS	false
136.161.34.87	unknown	United States		174	COGENT-174US	false
209.86.96.6	unknown	United States		7029	WINDSTREAMUS	false
76.204.63.38	unknown	United States		7018	ATT-INTERNET4US	false
167.246.237.231	unknown	United States		22808	RESOURCES-22808US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.233.230.44	unknown	Netherlands		15703	TRUESERVER-ASTrueServerBVASnumberNL	false
125.191.73.184	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
213.196.132.238	unknown	Switzerland		21040	DATAPARKCH	false
106.105.86.49	unknown	Taiwan; Republic of China (ROC)		18049	TINP-TWTaiwanInfrastructureNetworkTechnologieTW	false
61.196.242.205	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
53.200.167.39	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
185.105.253.172	unknown	Germany		8648	KAMP-DE	false
178.92.173.150	unknown	Ukraine		6849	UKRTELNETUA	false
66.135.90.230	unknown	United States		18897	MONTANA-SKY-NETWORKS-INCUS	false
198.250.182.80	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
121.11.16.205	unknown	China		58543	CHINATELECOM-GUANGDONG-IDCGuangdongCN	false
108.17.85.12	unknown	United States		701	UUNETUS	false
218.226.230.161	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
95.151.243.73	unknown	United Kingdom		12576	EELtdGB	false
213.52.157.157	unknown	United Kingdom		15830	EQUINIX-CONNECT-EMEAGB	false
71.93.42.159	unknown	United States		20115	CHARTER-20115US	false
12.183.68.128	unknown	United States		7018	ATT-INTERNET4US	false
82.201.225.33	unknown	Egypt		24863	LINKdotNET-ASEG	false
253.111.226.250	unknown	Reserved		unknown	unknown	false
208.127.35.15	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
202.19.217.219	unknown	Japan		7687	D-CRUISENETTOYOTADIGITALCRUISEINCORPORATEDJP	false
248.111.220.133	unknown	Reserved		unknown	unknown	false
255.187.189.150	unknown	Reserved		unknown	unknown	false
8.120.227.187	unknown	United States		3356	LEVEL3US	false
208.20.200.163	unknown	United States		1239	SPRINTLINKUS	false
252.17.232.26	unknown	Reserved		unknown	unknown	false
255.148.57.201	unknown	Reserved		unknown	unknown	false
211.182.181.20	unknown	Korea Republic of		9706	PETISNET-ASBUSANEDUCATIONRESEARCHINFORMATIONCENTERKR	false
119.28.5.218	unknown	China		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	false
81.130.63.147	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
84.229.162.133	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	false
44.67.141.103	unknown	United States		7377	UCSDUS	false
124.132.61.141	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
92.245.158.205	unknown	France		48072	ALSATIS-ASalsatiswispnetworkASFR	false
101.228.227.52	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
178.91.19.61	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
123.151.171.62	unknown	China		17638	CHINATELECOM-TJ-AS-APASNforTIANJINProvincialNetofCT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.4.170.147	unknown	Curacao		11081	UnitedTelecommunicationServicesUTSCW	false
200.244.158.139	unknown	Brazil		4230	CLAROSABR	false
173.42.243.212	unknown	United States		812	ROGERS-COMMUNICATIONSCA	false
72.144.232.184	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
196.224.103.42	unknown	Tunisia		37492	ORANGE-TN	false
222.84.82.184	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
27.0.126.86	unknown	Bangladesh		10113	EFTEL-AS-APEftelLimitedAU	false
244.69.9.240	unknown	Reserved		unknown	unknown	false
206.130.80.187	unknown	Canada		5690	VIANET-NOCA	false
186.81.231.104	unknown	Colombia		10620	TelmexColombiaSACO	false
105.88.195.67	unknown	Egypt		36992	ETISALAT-MISREG	false
125.129.129.79	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
167.199.163.161	unknown	United States		2897	GEORGIA-1US	false
60.106.72.186	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
183.33.114.154	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
178.66.27.22	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
78.177.213.154	unknown	Turkey		9121	TTNETTR	false
151.14.245.144	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
176.67.118.123	unknown	Palestinian Territory Occupied		51407	MADA-ASPS	false
125.251.7.45	unknown	Korea Republic of		38394	GOESN-AS-KRGyeonggidoSeongnamOfficeofEducationKR	false
24.1.63.186	unknown	United States		7922	COMCAST-7922US	false
152.129.212.83	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
192.224.153.94	unknown	United States		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
108.229.79.74	unknown	United States		36351	SOFTLAYERUS	false
144.87.113.133	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
172.222.135.80	unknown	United States		20115	CHARTER-20115US	false
125.51.29.229	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
141.113.207.11	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
222.209.178.155	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
150.124.136.6	unknown	United States		3955	WANG-US-1US	false
73.211.142.138	unknown	United States		7922	COMCAST-7922US	false
200.95.68.54	unknown	Mexico		8151	UninetSAdeCVMX	false
185.50.154.101	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
181.166.184.202	unknown	Argentina		10318	TelecomArgentinaSAAR	false
17.230.241.199	unknown	United States		714	APPLE-ENGINEERINGUS	false
181.163.84.100	unknown	Chile		7418	TELEFONICACHILESACL	false
118.177.65.107	unknown	Japan		9595	XEPHIONNTT-MECorporationJP	false
202.210.131.217	unknown	Japan		4686	BEKKOAMEBEKKOAMEINTERNETINCJP	false
76.108.80.243	unknown	United States		7922	COMCAST-7922US	false
59.255.163.36	unknown	China		37937	CNNIC-EGOVNET-APChinaeGovNetInformationCenterCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
39.231.53.6	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.942575235501028
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	I95q6K4AMy
File size:	27336
MD5:	a1d40f8e8634726af705363d1ce318e3
SHA1:	a23ea7dbd1ae980ef1860db2004a64c0c20753c3
SHA256:	d80ab5938a57dfbf5db4f294b4c4123320df3aad659c44683438dd4ac2553779
SHA512:	bf8a8a6a879fef0c193409f066d30e89377a79e626257aa0145d7b2334af84f673113fe7fe69a58585972ae9374a8650d24da6693af3bd6b57d037c07f650529
SSDEEP:	768:e1qDK6vmLcPO7av6T7qY+U1iL5+4UYLqKs3Uozy:/JF9CT7vniL5jUigzy
TLSH:	33C2D032B4636DF4C6B0193A7FDDC5C47D2FD2B1E6BA36B2271809E86C46442A1B174B
File Content Preview:	.ELF...a.....(.....0...4.....4. ... (.....i...i.....x...x...x.....Q.td.....s.y.UPX!.....S.....?.E.h;.}...^.....e.l..DU[j.....2d..d3.....l5.9\.wa.Q..E.&.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)

ELF header

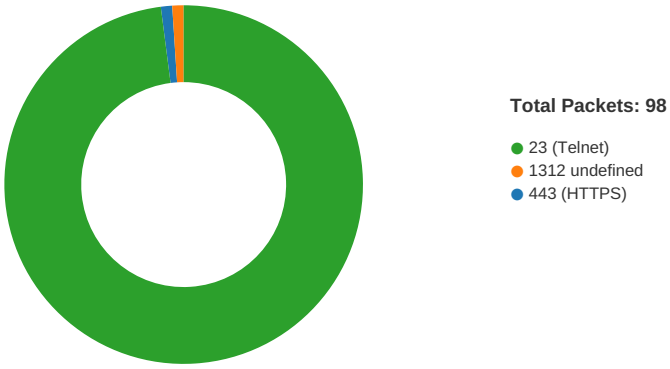
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0xd830
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section 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	0x8000	0x8000	0x69df	0x69df	7.9459	0x5	R E	0x8000		
LOAD	0x1578	0x21578	0x21578	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: I95q6K4AMy PID: 6226, Parent PID: 6121

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	/tmp/I95q6K4AMy
File size:	4956856 bytes

MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: I95q6K4AMy PID: **6228**, Parent PID: **6226**

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: I95q6K4AMy PID: **6328**, Parent PID: **6228**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: I95q6K4AMy PID: **6332**, Parent PID: **6228**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: I95q6K4AMy PID: **6335**, Parent PID: **6332**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: I95q6K4AMy PID: **6346**, Parent PID: **6335**

General

Start time:	23:43:49
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: l95q6K4AMy PID: **6348**, Parent PID: **6335**

General

Start time:	23:43:49
Start date:	08/08/2022
Path:	/tmp/l95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: l95q6K4AMy PID: **6336**, Parent PID: **6332**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/l95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: l95q6K4AMy PID: **6340**, Parent PID: **6332**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/l95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: l95q6K4AMy PID: **6229**, Parent PID: **6226**

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/l95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: l95q6K4AMy PID: **6231**, Parent PID: **6226**

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/l95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: l95q6K4AMy PID: **6234**, Parent PID: **6231**

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/l95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: I95q6K4AMy PID: **6327**, Parent PID: **6234**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: I95q6K4AMy PID: **6330**, Parent PID: **6234**

General

Start time:	23:43:44
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: I95q6K4AMy PID: **6235**, Parent PID: **6231**

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: I95q6K4AMy PID: **6239**, Parent PID: **6231**

General

Start time:	23:40:53
Start date:	08/08/2022
Path:	/tmp/I95q6K4AMy
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1