ID: 516358
Sample Name: QISwaj96QZ
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:26:48
Date: 05/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report QISwaj96QZ 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Process Tree 3
Yara Overview 4
Initial Sample 4
PCAP (Network Traffic) 4
Memory Dumps 4
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 5
Malware Configuration 5
Behavior Graph 6
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted IPs 7
Public 7
Runtime Messages 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
Static ELF Info 11
ELF header 11
Sections 11
Program Segments 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 12
System Behavior 12
Analysis Process: QISwaj96QZ PID: 5238 Parent PID: 5112 12
General 12
File Activities 12
File Read 12
Analysis Process: QISwaj96QZ PID: 5242 Parent PID: 5238 12
General 12
Analysis Process: QISwaj96QZ PID: 5243 Parent PID: 5238 12
General 12
Analysis Process: QISwaj96QZ PID: 5246 Parent PID: 5243 13
General 13
Analysis Process: QISwaj96QZ PID: 5247 Parent PID: 5243 13
General 13

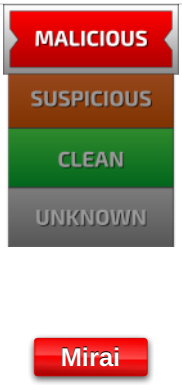
Linux Analysis Report QISwaj96QZ

Overview

General Information

Sample Name:	QISwaj96QZ
Analysis ID:	516358
MD5:	50484af9fb1e9cb..
SHA1:	810a2ce65be134..
SHA256:	d43c6fda493518d.
Tags:	32 arm elf mirai
Infos:	

Detection

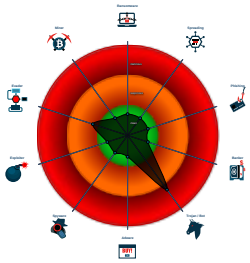


Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...
- Sample listens on a socket

Classification



Analysis Advice

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

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	516358
Start date:	05.11.2021
Start time:	11:26:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QISwaj96QZ
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:	mal64.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- QISwaj96QZ (PID: 5238, Parent: 5112, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/QISwaj96QZ
  - QISwaj96QZ New Fork (PID: 5242, Parent: 5238)
  - QISwaj96QZ New Fork (PID: 5243, Parent: 5238)
    - QISwaj96QZ New Fork (PID: 5246, Parent: 5243)
    - QISwaj96QZ New Fork (PID: 5247, Parent: 5243)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
QISwaj96QZ	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x114c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x115a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11618:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11688:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x118f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1194c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11a48:$xo1: oMXKNNC\x0D\x17\x0C\x12

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
5246.1.000000005c15cc02.000000007fed13cd.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x2ec:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x360:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x3d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x448:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x4bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x73c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x794:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7ec:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x844:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x89c:$xo1: oMXKNNC\x0D\x17\x0C\x12
5246.1.00000000fac4855c.000000001b65e999.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x114c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x115a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11618:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11688:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x118f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1194c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11a48:$xo1: oMXKNNC\x0D\x17\x0C\x12
5242.1.000000005c15cc02.000000007fed13cd.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x2ec:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x360:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x3d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x448:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x4bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x73c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x794:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7ec:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x844:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x89c:$xo1: oMXKNNC\x0D\x17\x0C\x12
5242.1.00000000fac4855c.000000001b65e999.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x114c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x115a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11618:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11688:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x118f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1194c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11a48:$xo1: oMXKNNC\x0D\x17\x0C\x12
5238.1.00000000fac4855c.000000001b65e999.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x114c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x115a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11618:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11688:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x118f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1194c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x119f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11a48:$xo1: oMXKNNC\x0D\x17\x0C\x12

Click to see the 1 entries

Jbx Signature Overview

- AV Detection
- Networking
- System Summary
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

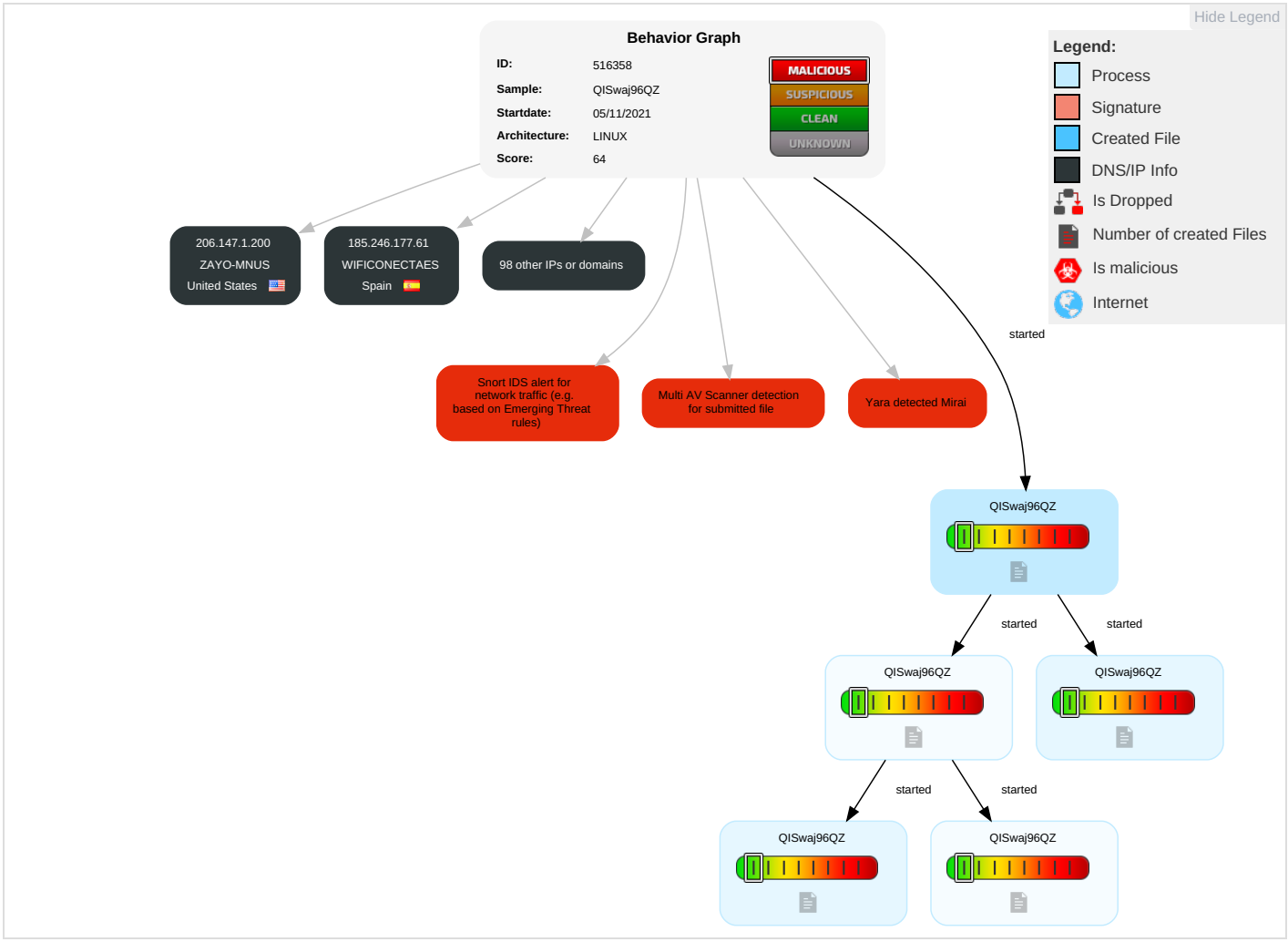
Mitre Att&ck Matrix

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	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	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	Non-Standard Port 1	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	Application Layer Protocol 1	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
QISwaj96QZ	45%	Virustotal		Browse
QISwaj96QZ	45%	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

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
170.232.245.244	unknown	United States		21833	TRINITY-ISUS	false
210.184.23.225	unknown	Hong Kong		4058	CITICTEL-CPC-AS4058CITICTelecomInternationalCPCLimited	false
76.155.68.109	unknown	United States		7922	COMCAST-7922US	false
187.163.236.152	unknown	Mexico		6503	AxtelSABdeCVMX	false
67.21.35.150	unknown	United States		12189	AS12189US	false
40.169.199.194	unknown	United States		4249	LILLY-ASUS	false
199.49.192.65	unknown	United States		201204	GFIS-AS-DE	false
178.142.75.22	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
154.203.73.158	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
32.179.68.47	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
149.148.126.173	unknown	Austria		2494	MUWNETMUWNETAutonomousSystemAT	false
107.114.210.58	unknown	United States		7018	ATT-INTERNET4US	false
66.121.29.141	unknown	United States		7132	SBIS-ASUS	false
89.11.228.91	unknown	Norway		15659	NEXTGENTELNEXTGENTELAutonomousSystemNO	false
122.251.58.10	unknown	Japan		18077	C-ABLEYamaguchiCableVisionCoLtdJP	false
69.69.153.108	unknown	United States		2379	CENTURYLINK-LEGACY-EMBARQ-WNPKUS	false
78.202.31.26	unknown	France		12322	PROXADFR	false
154.38.166.244	unknown	United States		174	COGENT-174US	false
210.207.11.78	unknown	Korea Republic of		9861	HIAM-AS-KRHiAssetManagementCoLtdKR	false
160.248.25.98	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
36.155.143.109	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
48.82.49.35	unknown	United States		2686	ATGS-MMD-ASUS	false
149.142.83.227	unknown	United States		52	UCLAUS	false
176.231.124.99	unknown	Israel		12400	PARTNER-ASIL	false
63.137.70.194	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
102.5.127.220	unknown	unknown		36926	CKL1-ASNKE	false
185.246.177.61	unknown	Spain		203534	WIFICONECTAES	false
24.237.186.6	unknown	United States		8047	GCIUS	false
125.12.239.172	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
98.33.163.83	unknown	United States		7922	COMCAST-7922US	false
174.225.164.161	unknown	United States		22394	CELLCOUS	false
133.114.229.38	unknown	Japan		2522	PPP-EXPJapanNetworkInformationCenterJP	false
123.179.198.100	unknown	China		4809	CHINATELECOM-CORE-WAN-CN2ChinaTelecomNextGenerationCarr	false
147.249.204.48	unknown	United States		6419	IDDUS	false
145.192.49.241	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
206.147.1.200	unknown	United States		7821	ZAYO-MNUS	false
139.241.235.103	unknown	United States		27066	DNIC-ASBLK-27032-27159US	false
201.105.160.238	unknown	Mexico		8151	UninetSAdeCVMX	false
88.236.146.218	unknown	Turkey		9121	TTNETTR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.35.98.22	unknown	United States		33363	BHN-33363US	false
109.67.199.181	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
189.23.63.69	unknown	Brazil		4230	CLAROSABR	false
49.196.95.142	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
180.250.40.206	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	false
84.234.183.211	unknown	Norway		29695	ALTIBOX_ASNorwayNO	false
119.54.40.164	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
49.142.241.38	unknown	Korea Republic of		7623	HCNGYEONGBUK-AS-KRGyeongbukCableTVKR	false
5.119.70.184	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
126.41.184.57	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
166.29.157.42	unknown	United States		206	CSC-IGN-AMERUS	false
223.74.172.172	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
155.41.18.6	unknown	United States		111	BOSTONU-ASUS	false
82.17.192.176	unknown	United Kingdom		5089	NTLGB	false
90.158.71.157	unknown	Turkey		9021	ISNETTR	false
17.140.196.174	unknown	United States		714	APPLE-ENGINEERINGUS	false
40.99.120.36	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
195.41.24.251	unknown	Denmark		3292	TDCTDCASDK	false
209.53.152.194	unknown	Canada		852	ASN852CA	false
189.141.254.196	unknown	Mexico		8151	UninetSAdeCVMX	false
68.255.218.247	unknown	United States		31759	LARABIDAUS	false
219.53.238.216	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
204.162.252.162	unknown	United States		3356	LEVEL3US	false
114.26.71.138	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
136.102.253.39	unknown	United States		60311	ONEFMCH	false
110.77.227.100	unknown	Thailand		131090	CAT-IDC-4BYTENET-AS-APCATTELECOMPublicCompanyLtdCATT	false
199.125.126.248	unknown	United States		14265	US-TELEPACIFICUS	false
134.13.160.111	unknown	United States		270	AS270US	false
147.211.36.210	unknown	Australia		132029	ASN-TELSTRA-02TelstraPtyLtdAU	false
128.124.105.48	unknown	Ukraine		21497	UMC-ASUA	false
47.244.18.113	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
138.138.23.138	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
174.18.18.220	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
207.246.242.194	unknown	United States		53824	LIQUIDWEBUS	false
89.163.190.7	unknown	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
190.189.255.45	unknown	Argentina		10481	TelecomArgentinaSAAR	false
148.24.125.151	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
13.168.58.86	unknown	United States		7018	ATT-INTERNET4US	false
217.96.183.241	unknown	Poland		5617	TPNETPL	false
141.94.188.2	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
126.51.16.235	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
124.98.93.127	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
77.230.62.128	unknown	Spain		12430	VODAFONE_ESES	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.87.175.167	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
178.214.69.222	unknown	Palestinian Territory Occupied		51336	GEMZOPS	false
92.100.125.89	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
18.112.168.135	unknown	United States		3	MIT-GATEWAYSUS	false
8.255.117.244	unknown	United States		3356	LEVEL3US	false
198.140.20.204	unknown	United States		7726	FITC-ASUS	false
207.137.185.84	unknown	United States		10708	SELECTNET-ASUS	false
104.107.70.86	unknown	United States		3462	HINETDataCommunicationBusinessGroupTW	false
191.42.68.35	unknown	Brazil		7738	TelemarNorteLesteSABR	false
133.13.47.233	unknown	Japan		17960	RAINS-ASUniversityoftheRyukyusJP	false
208.163.31.171	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
44.109.194.201	unknown	United States		7377	UCSDUS	false
189.238.171.224	unknown	Mexico		8151	UninetSAdeCVMX	false
70.239.19.13	unknown	United States		7018	ATT-INTERNET4US	false
1.184.119.109	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
185.22.138.65	unknown	Poland		199057	AMPLUS-ASPL	false
180.199.137.188	unknown	Japan		18126	CTCXChubuTelecommunicationsCompanyIncJP	false
211.144.212.184	unknown	China		23853	CNNIC-DSNET-APShanghaiDataSolutionCoLtdCN	false

Runtime Messages

Command:	/tmp/QISwaj96QZ
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	JEW was here lol
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
65.35.98.22	vHVNRpNhIs	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRINITY-ISUS	XyMjGu74RX	Get hash	malicious	Browse	• 170.232.234.11
COMCAST-7922US	YYcy9gLbBC	Get hash	malicious	Browse	• 25.9.55.225
	bZ3EzTJKiD	Get hash	malicious	Browse	• 25.103.19.112
	rMwxCtXmuJ	Get hash	malicious	Browse	• 50.193.183.4
	fukfKHAGMe	Get hash	malicious	Browse	• 25.47.75.214
	uV1rj8v43F	Get hash	malicious	Browse	• 73.83.249.228
	WsoVopfjnC	Get hash	malicious	Browse	• 96.120.46.53
	mL883e3xGw	Get hash	malicious	Browse	• 76.120.108.203

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	v7Tqrjux9l	Get hash	malicious	Browse	• 68.52.189.69
	X8q5ELl79g	Get hash	malicious	Browse	• 96.66.130.36
	xd.arm7	Get hash	malicious	Browse	• 73.84.16.179
	xd.x86	Get hash	malicious	Browse	• 76.142.58.160
	auzkes	Get hash	malicious	Browse	• 73.184.255.188
	Tx60OCR2cN	Get hash	malicious	Browse	• 173.167.21 1.118
	HdZIgkO5be	Get hash	malicious	Browse	• 73.37.39.244
	Rvg3MFzKNR	Get hash	malicious	Browse	• 68.58.240.26
	B94t90Yyoz	Get hash	malicious	Browse	• 25.148.189.217
	QX4Kudvf1x	Get hash	malicious	Browse	• 73.207.81.13
	QsSD7q2BRO	Get hash	malicious	Browse	• 76.140.121.154
	b3astmode.x86	Get hash	malicious	Browse	• 76.18.177.109
	b3astmode.arm	Get hash	malicious	Browse	• 184.127.14 6.165
CITICTEL-CPC-AS4058CITICTelecomInternationalCPCLimited	xd.arm7	Get hash	malicious	Browse	• 203.85.123.25
	1bL17EUgTk	Get hash	malicious	Browse	• 152.101.82.212
	vLqyyo55oA	Get hash	malicious	Browse	• 202.90.2.219
	nLfUJu0kEA	Get hash	malicious	Browse	• 202.72.16.2
	yqYt9HH2OY	Get hash	malicious	Browse	• 152.101.28.112
	LsgCcJSqnz	Get hash	malicious	Browse	• 210.184.2.190
	sora.x86	Get hash	malicious	Browse	• 152.101.7.97
	2dv5TkS2qu	Get hash	malicious	Browse	• 210.184.2.189
	sora.x86	Get hash	malicious	Browse	• 202.66.98.245
	6epEGXQkCa	Get hash	malicious	Browse	• 202.76.41.145
	DDy9cpZuI8	Get hash	malicious	Browse	• 210.184.2.187
	BinName.arm7	Get hash	malicious	Browse	• 202.66.98.248
	UDJcMOWp4H	Get hash	malicious	Browse	• 202.76.107.217
	TJXA3eIJsJ	Get hash	malicious	Browse	• 202.88.105.180
	wGGBiv7Qsa	Get hash	malicious	Browse	• 203.85.146.108
	1isequal9.x86	Get hash	malicious	Browse	• 203.85.111.11
	4A7rphFZrY	Get hash	malicious	Browse	• 210.184.23.245
	.exe	Get hash	malicious	Browse	• 152.101.233.97
	39file.exe	Get hash	malicious	Browse	• 152.101.233.57

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), s tatically linked, stripped
Entropy (8bit):	6.071033145102414
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	QISwaj96QZ
File size:	74748
MD5:	50484af9fb1e9cbb08d0559c6f6c4795
SHA1:	810a2ce65be134a31337c5aa6be31218854b0762

General

SHA256:	d43c6fda493518d67a8a1e7554af594f51576292dbac6cb3e0b1730fcc058d90
SHA512:	a29074aeb417ff7acb2443a1cbcb545593b650345bd4ed2fa8513122c14852427ea187ce1e5f6f41779d5a19049c46a3e996b8c9d09a1ef977631faff2f9755f
SSDEEP:	1536:LwqRXwawW7iFZ+IzqsAcBs9bgr9lz6BvRrZJX6OePNs1dq3:LwqaS8dzV0sPqvZ7XIPWdq
File Content Preview:	.ELF...a.....(.....4...l".....4. ...(.....`..`.....`..`..... ... .,...@.....Q.td.....-...L."...C.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	74348
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

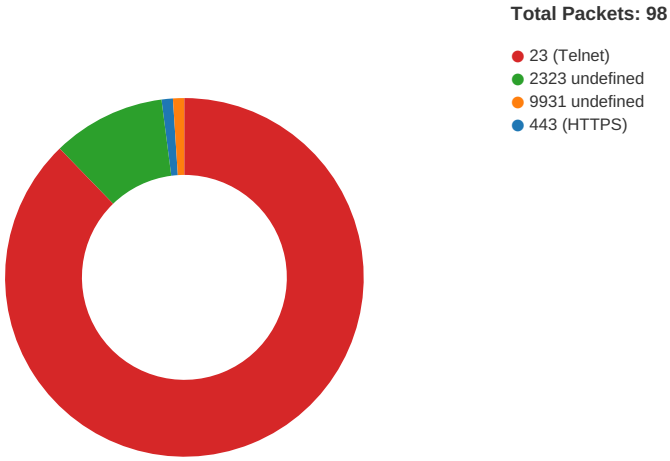
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x10eb0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x18f60	0x10f60	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x18f74	0x10f74	0xeec	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x22000	0x12000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x22008	0x12008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x22014	0x12014	0x218	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x2222c	0x1222c	0x314	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1222c	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	0x8000	0x8000	0x11e60	0x11e60	3.2877	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x12000	0x22000	0x22000	0x22c	0x540	1.6863	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: QISwaj96QZ PID: 5238 Parent PID: 5112

General

Start time:	11:27:31
Start date:	05/11/2021
Path:	/tmp/QISwaj96QZ
Arguments:	/tmp/QISwaj96QZ
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: QISwaj96QZ PID: 5242 Parent PID: 5238

General

Start time:	11:27:32
Start date:	05/11/2021
Path:	/tmp/QISwaj96QZ
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QISwaj96QZ PID: 5243 Parent PID: 5238

General

Start time:	11:27:32
Start date:	05/11/2021
Path:	/tmp/QISwaj96QZ

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QISwaj96QZ PID: 5246 Parent PID: 5243

General

Start time:	11:27:32
Start date:	05/11/2021
Path:	/tmp/QISwaj96QZ
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QISwaj96QZ PID: 5247 Parent PID: 5243

General

Start time:	11:27:32
Start date:	05/11/2021
Path:	/tmp/QISwaj96QZ
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1