ID: 518867
Sample Name: QSjpGBd7Gv
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:58:29
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

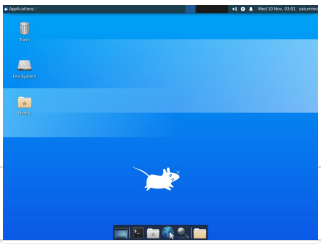
Linux Analysis Report QSjpGBd7Gv

Overview

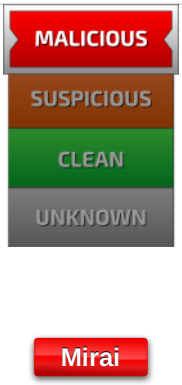
General Information

Sample Name:	QSjpGBd7Gv
Analysis ID:	518867
MD5:	3de8c33cfff4c68…
SHA1:	f07c77c2dafdbe2..
SHA256:	0c6a90a805954a..
Tags:	32 arm elf mirai
Infos:	

Most interesting Screenshot:



Detection

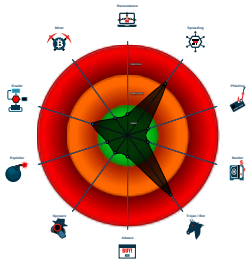


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on no…
- Sample tries to kill many processes…
- Connects to many ports of the same…
- Sample has stripped symbol table
- HTTP GET or POST without a user …
- 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 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:	518867
Start date:	10.11.2021
Start time:	02:58:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QSjpGBd7Gv
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:	mal76.spre.troj.lin@0/2@0/0
Warnings:	Show All

Process Tree

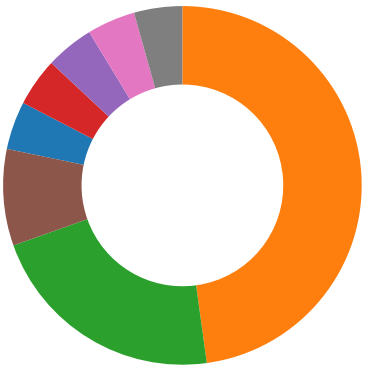
- **system is lnxubuntu20**
- QSjpGBd7Gv (PID: 5240, Parent: 5114, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/QSjpGBd7Gv
  - QSjpGBd7Gv New Fork (PID: 5242, Parent: 5240)
  - QSjpGBd7Gv New Fork (PID: 5243, Parent: 5240)
  - QSjpGBd7Gv New Fork (PID: 5245, Parent: 5240)
    - QSjpGBd7Gv New Fork (PID: 5248, Parent: 5245)
    - QSjpGBd7Gv New Fork (PID: 5249, Parent: 5245)
    - QSjpGBd7Gv New Fork (PID: 5251, Parent: 5245)
    - QSjpGBd7Gv New Fork (PID: 5252, Parent: 5245)
    - QSjpGBd7Gv New Fork (PID: 5255, Parent: 5245)
- systemd New Fork (PID: 5280, Parent: 1)
  - sshd (PID: 5280, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5281, Parent: 1)
  - sshd (PID: 5281, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- 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)

Uses known network protocols on non-standard ports

Connects to many ports of the same IP (likely port scanning)

System Summary:

Sample tries to kill many processes (SIGKILL)

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

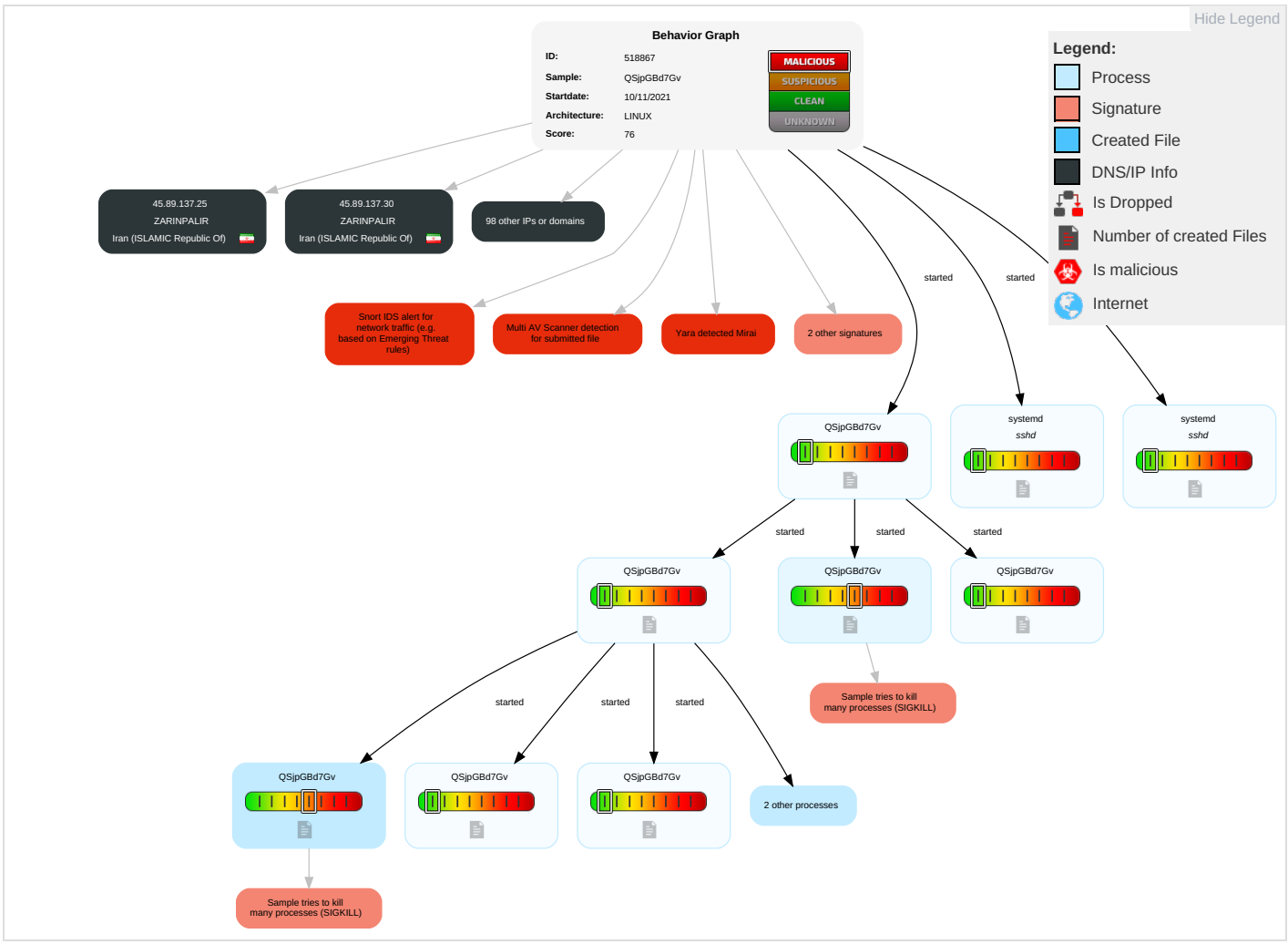
Mitre Att&ck Matrix

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	Direct Volume Access	OS Credential Dumping 1	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 Partitio
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
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	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

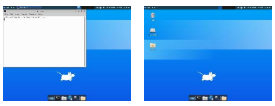
Behavior Graph

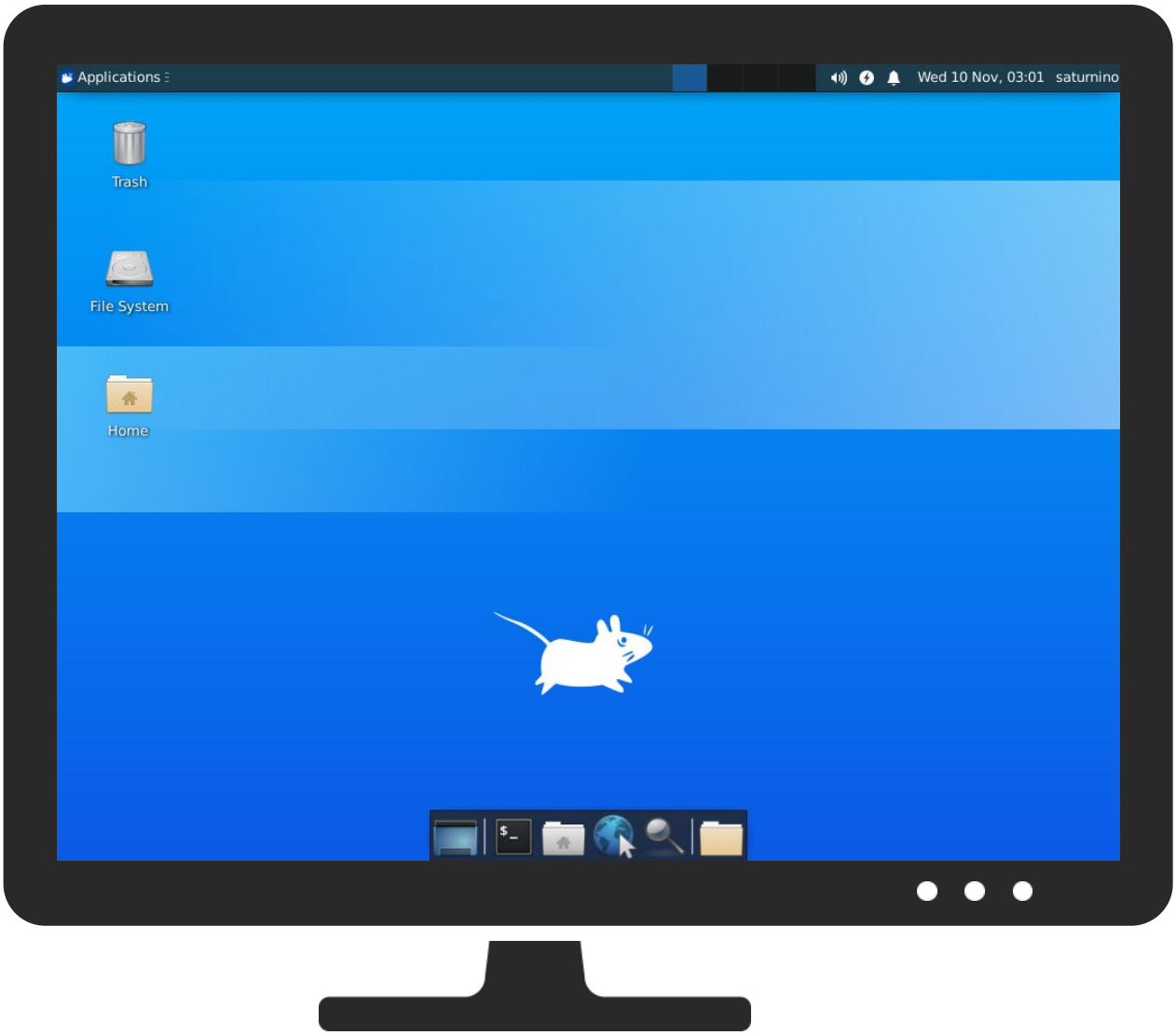


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QSjpGBd7Gv	56%	Virustotal		Browse
QSjpGBd7Gv	51%	Metadefender		Browse
QSjpGBd7Gv	75%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:52869/picdesc.xml	0%	Avira URL Cloud	safe	
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://103.3.246.123/bins/Hilix.mips	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:52869/picdesc.xml	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.196.147.253	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
65.65.79.221	unknown	United States		7018	ATT-INTERNET4US	false
205.187.136.105	unknown	United States		7029	WINDSTREAMUS	false
197.53.167.13	unknown	Egypt		8452	TE-ASTE-ASEG	false
119.238.60.126	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
91.19.190.18	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.169.219.64	unknown	France		12322	PROXADFR	false
157.31.108.185	unknown	United States		8968	BT-ITALIAIT	false
45.9.255.245	unknown	Iran (ISLAMIC Republic Of)		207409	STTSIR	false
91.57.251.125	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.120.116.220	unknown	Hungary		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
156.124.100.129	unknown	United States		393504	XNSTGCA	false
91.121.98.210	unknown	France		16276	OVHFR	false
197.96.124.92	unknown	South Africa		3741	ISZA	false
91.194.118.127	unknown	Germany		29317	SLZ-ASs-IznetDE	false
193.105.39.109	unknown	Russian Federation		34291	CINVB-ASRU	false
185.52.245.248	unknown	Germany		202113	PLANBDE	false
91.0.219.66	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.122.30.227	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
185.92.4.177	unknown	Iran (ISLAMIC Republic Of)		48903	MEHRFCPIR	false
45.50.203.138	unknown	United States		20001	TWC-20001-PACWESTUS	false
213.45.62.1	unknown	Italy		3269	ASN-IBSNAZIT	false
185.141.5.76	unknown	France		208678	E-SIFR	false
91.74.73.87	unknown	United Arab Emirates		15802	DU-AS1AE	false
185.202.158.244	unknown	Germany		42366	TERRATRANSIT-ASDE	false
91.220.89.32	unknown	Austria		51767	JOHANNITER-UNFALL-HILFEAT	false
91.146.9.29	unknown	Russian Federation		3226	MARK-ITT-ASRU	false
113.128.152.78	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
185.78.232.45	unknown	Czech Republic		39248	SIVASH-ASRU	false
103.136.218.205	unknown	India		138784	IGEPL-ASInterglobeEnterprisesPrivateLimitedIN	false
167.24.242.140	unknown	United States		7838	USAAUS	false
88.146.165.46	unknown	Czech Republic		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
91.9.184.144	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
180.167.126.71	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
156.72.230.182	unknown	United States		29975	VODACOM-ZA	false
156.249.107.27	unknown	Seychelles		139086	ONL-HKOCEANNETWORKLIMITEDHK	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.35.202.45	unknown	Norway		50304	BLIXNO	false
91.13.207.244	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
108.152.25.10	unknown	United States		16509	AMAZON-02US	false
70.136.16.245	unknown	United States		7018	ATT-INTERNET4US	false
188.50.26.244	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
156.134.164.89	unknown	United States		27174	UNASSIGNED	false
45.234.130.236	unknown	Brazil		267365	GigaTecnologiaemRedeseInternetEIRELIBR	false
185.191.41.93	unknown	Spain		56571	CABLEXES	false
185.203.135.86	unknown	Switzerland		15576	NTSCH	false
84.209.102.219	unknown	Norway		41164	GET-NOGETNorwayNO	false
91.112.149.137	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
185.51.254.88	unknown	United Kingdom		26178	ATKINS-NORTH-AMERICAUS	false
197.180.132.85	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
58.160.164.211	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
197.104.77.94	unknown	South Africa		37168	CELL-CZA	false
185.78.7.93	unknown	United Kingdom		16030	ALTECOMES	false
153.110.136.76	unknown	Norway		5619	EVRY-NO	false
91.149.99.32	unknown	Russian Federation		12958	MCCTele2RussiaNetworkRU	false
78.40.243.120	unknown	United Kingdom		33920	AQLGB	false
185.8.76.81	unknown	France		35344	SYNTEN-ASFR	false
59.115.116.67	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
180.140.198.119	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
91.231.111.231	unknown	Poland		198067	AZIMUTHIT-ASSmart4AviationGroupPL	false
91.239.171.89	unknown	Poland		59556	ADNET-ASPL	false
195.211.252.136	unknown	Ukraine		50204	ARHAT-ASUA	false
76.241.14.44	unknown	United States		7018	ATT-INTERNET4US	false
185.60.92.146	unknown	France		39605	IGUANESOLUTIONSFR	false
91.244.134.41	unknown	Ukraine		44798	PERVOMAYSK-ASUA	false
41.240.121.89	unknown	Sudan		36998	SDN-MOBITELSD	false
185.70.46.24	unknown	Belgium		57948	COBALTIPWorksBE	false
45.89.137.30	unknown	Iran (ISLAMIC Republic Of)		208675	ZARINPALIR	false
45.136.88.94	unknown	Germany		3257	GTT-BACKBONEGTTDE	false
91.223.243.30	unknown	Estonia		9130	HMS-ASRU	false
51.127.124.117	unknown	United Kingdom		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.240.33	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
91.122.255.237	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
185.178.93.91	unknown	Italy		206701	FIBRACITYIT	false
91.150.65.218	unknown	Serbia		8400	TELEKOM-ASRS	false
91.200.1.84	unknown	Ukraine		43744	ORIONCITY-ASUA	false
40.218.241.41	unknown	United States		4249	LILLY-ASUS	false
91.149.99.25	unknown	Russian Federation		12958	MCCTele2RussiaNetworkRU	false
91.26.71.209	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.170.164.12	unknown	Netherlands		48629	ICLIKLB	false
91.39.217.59	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.170.14.25	unknown	South Africa		36937	Neotel-ASZA	false
116.25.221.155	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
54.0.222.108	unknown	United States		14618	AMAZON-AESUS	false
213.243.166.203	unknown	Finland		16086	DNAFI	false
91.95.68.184	unknown	Sweden		5617	TPNETPL	false
91.19.189.208	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.60.44.239	unknown	Russian Federation		29124	ISKRATELECOM-ASSEVEN-SKYRU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.96.95.96	unknown	United States		33274	ASN-FAIRVIEWHEALTHSERVICESUS	false
185.100.7.142	unknown	France		35393	EURO-WEB-ASFR	false
41.106.43.146	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.12.117.170	unknown	Tunisia		37703	ATLAXTN	false
67.93.104.123	unknown	United States		2828	XO-AS15US	false
91.244.56.26	unknown	Ukraine		25133	MCLAUT-ASUA	false
208.106.189.131	unknown	United States		14992	CRYSTALTECHUS	false
45.97.8.6	unknown	Egypt		37069	MOBINILEG	false
45.89.137.25	unknown	Iran (ISLAMIC Republic Of)		208675	ZARINPALIR	false
143.227.164.91	unknown	United States		393296	AUGUSTANACOLLEGEROCKISLANDILUS	false
104.96.77.40	unknown	United States		20940	AKAMAI-ASN1EU	false
185.240.220.167	unknown	Czech Republic		204772	RSD-CZ	false
185.10.130.119	unknown	Russian Federation		197078	YARNET-ASRU	false

Runtime Messages

Command:	/tmp/QSjpGBd7Gv
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
197.53.167.13	arm	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ATT-INTERNET4US	fbXTgwatuJ	Get hash	malicious	Browse	• 45.25.228.40
	mips	Get hash	malicious	Browse	• 76.213.160.239
	arm	Get hash	malicious	Browse	• 99.14.0.59
	arm6	Get hash	malicious	Browse	• 68.95.62.1
	arm5	Get hash	malicious	Browse	• 108.220.13.87
	qgxgn5fQU1	Get hash	malicious	Browse	• 107.100.90.208
	BS0Dxmu2go	Get hash	malicious	Browse	• 63.241.171.255
	GB0O1NUtmJ	Get hash	malicious	Browse	• 207.104.29.24
	4DrtSJOLjr	Get hash	malicious	Browse	• 99.10.53.29
	LAQh74RNEl	Get hash	malicious	Browse	• 13.148.44.124
	dYgJ72oG4f	Get hash	malicious	Browse	• 12.24.75.138
	Kz2SeJpaxw	Get hash	malicious	Browse	• 107.116.96.43
	fMGehkjmPv	Get hash	malicious	Browse	• 71.140.64.64
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 12.52.220.201
	BKyU0T5xcw	Get hash	malicious	Browse	• 172.175.174.14
	skonwRkAlJ	Get hash	malicious	Browse	• 99.105.129.7
	ZvUGMRqJrx	Get hash	malicious	Browse	• 108.64.154.134
	jyTZMJKPD2	Get hash	malicious	Browse	• 99.173.65.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P8NtIPe7f0	Get hash	malicious	Browse	• 99.141.56.11
	OoeA4dABtV	Get hash	malicious	Browse	• 98.71.6.46
Africa-on-Cloud-ASZA	BKyU0T5xcw	Get hash	malicious	Browse	• 156.246.150.187
	2b6XF36zQq	Get hash	malicious	Browse	• 156.246.150.163
	byxEpar5Zm	Get hash	malicious	Browse	• 156.246.102.207
	s4Qw9YZtjr	Get hash	malicious	Browse	• 156.246.150.180
	meqAP2UZQj.exe	Get hash	malicious	Browse	• 156.240.150.22
	AhsMBcI8HE.exe	Get hash	malicious	Browse	• 156.240.150.22
	MNYQfZ9U6w.exe	Get hash	malicious	Browse	• 156.240.150.22
	W8k9ifCqjy.exe	Get hash	malicious	Browse	• 156.240.150.22
	NUo71b3C4p.exe	Get hash	malicious	Browse	• 156.240.150.22
	r2Nae151Pz.exe	Get hash	malicious	Browse	• 156.240.160.85
	ELEGANT MARINE.exe	Get hash	malicious	Browse	• 156.240.160.85
	Hilix.arm	Get hash	malicious	Browse	• 45.206.28.0
	Hilix.arm7	Get hash	malicious	Browse	• 45.197.31.32
	mxHkqAIYT0	Get hash	malicious	Browse	• 156.246.150.171
	w66OTKGVFv	Get hash	malicious	Browse	• 156.246.150.168
	ydZLm6GD56	Get hash	malicious	Browse	• 45.203.157.220
	OhUy3woBmb	Get hash	malicious	Browse	• 45.206.90.63
	9o6Z1wEokT	Get hash	malicious	Browse	• 156.240.70.1
	00hZyjOhZA	Get hash	malicious	Browse	• 156.228.228.21
	mP1pg0ryFA	Get hash	malicious	Browse	• 156.228.63.83
WINDSTREAMUS	x86_64	Get hash	malicious	Browse	• 74.9.152.70
	arm	Get hash	malicious	Browse	• 98.17.135.18
	arm6	Get hash	malicious	Browse	• 173.184.230.178
	4DrtSJOLjr	Get hash	malicious	Browse	• 40.134.73.47
	Kz2SeJpaxw	Get hash	malicious	Browse	• 74.8.121.17
	fMGehkjmPv	Get hash	malicious	Browse	• 209.253.40.34
	RrK5lgZ6gZ	Get hash	malicious	Browse	• 165.247.11.247
	OoeA4dABtV	Get hash	malicious	Browse	• 207.223.236.218
	YG9KkTTAgE	Get hash	malicious	Browse	• 69.95.185.164
	kkr4DrMz5L	Get hash	malicious	Browse	• 66.184.133.224
	fCca2FJVXG	Get hash	malicious	Browse	• 216.73.137.189
	QLPxrFlfKm	Get hash	malicious	Browse	• 209.125.22.247
	62G7F4Mgt0	Get hash	malicious	Browse	• 216.48.63.12
	DvwfkRaTRo	Get hash	malicious	Browse	• 66.149.234.18
	p9rySh9WA4	Get hash	malicious	Browse	• 207.217.225.243
	P82zcbRMNt	Get hash	malicious	Browse	• 216.80.250.249
	rXFu2DZdQq	Get hash	malicious	Browse	• 209.252.203.213
	AER0hx5txK	Get hash	malicious	Browse	• 174.131.208.22
	IYcCOLfGT7	Get hash	malicious	Browse	• 207.217.225.200
	AjNJHZfSOB	Get hash	malicious	Browse	• 40.138.179.159

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5281/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 -1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Co:Co
MD5:	1C6FED73033E83DA4459F2B85AD247AF
SHA1:	1D5EAD879734D1A4D955D5D5757F174066A8338A
SHA-256:	E7FEBA5833BED3FD6D9DFA3BB41A893A6860BCFC4EF933CF0B6242BD23DCD586
SHA-512:	08864AD9F6AF98209C5CD159384EB87BDF2F1320F2E36CD554A31FBB58D23F553D8CCA537C1A5A61DE71383BA34A141BB9867A9F950B27F1BC08DAC18ADF19 7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 5281.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	6.098101398246121
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	QSjpGBd7Gv
File size:	62456
MD5:	3de8c33cfff4c6823e1968520cc93dd7
SHA1:	f07c77c2dafdbe21afe740950f1e7a7e87fd763a
SHA256:	0c6a90a805954a7c5c0180c34bc4f1abff5c684f0e0214f4 26d4c438c322f3f3
SHA512:	124708777d0b85da4dbe010a5a1a64f304c4de6c1464a9 c9872c855d78b03769b5baab4f24e470a85e64a05ac32e 0f51ffe7a8db097f5ecacfa648d06e098355
SSDEEP:	1536:0yW869O3GXz/z8a5O8isr9M53e536c0PKwl5PwC +gH2:0yx6EK3wJsr+5OR6hCwl5tS
File Content Preview:	.ELF...a.....(.....4...h.....4. ...(..... .....(.....Q.td.....-...L.".... 6.....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)

ELF header

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:	62056
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	0xdb00	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x15bb0	0xdbb0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x15bc4	0xdbc4	0x1120	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1f000	0xf000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1f008	0xf008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1f014	0xf014	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1f228	0xf228	0x2e8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf228	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	0xece4	0xece4	3.3655	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0xf000	0x1f000	0x1f000	0x228	0x510	1.5772	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: QSjpGBd7Gv PID: 5240 Parent PID: 5114

General

Start time:	02:59:11
Start date:	10/11/2021

Path:	/tmp/QSjpGBd7Gv
Arguments:	/tmp/QSjpGBd7Gv
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: QSjpGBd7Gv PID: 5242 Parent PID: 5240

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: QSjpGBd7Gv PID: 5243 Parent PID: 5240

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QSjpGBd7Gv PID: 5245 Parent PID: 5240

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QSjpGBd7Gv PID: 5248 Parent PID: 5245

General

Start time:	02:59:11
Start date:	10/11/2021

Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: QSjpGBd7Gv PID: 5249 Parent PID: 5245

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QSjpGBd7Gv PID: 5251 Parent PID: 5245

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QSjpGBd7Gv PID: 5252 Parent PID: 5245

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: QSjpGBd7Gv PID: 5255 Parent PID: 5245

General

Start time:	02:59:11
Start date:	10/11/2021
Path:	/tmp/QSjpGBd7Gv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5280 Parent PID: 1

General

Start time:	02:59:27
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5280 Parent PID: 1

General

Start time:	02:59:27
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5281 Parent PID: 1

General

Start time:	02:59:28
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5281 Parent PID: 1

General

Start time:	02:59:28
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated