ID: 519456
Sample Name: uRQVqbl0sQ
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 19:01:48
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

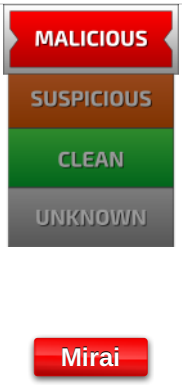
Linux Analysis Report uRQVqbl0sQ

Overview

General Information

Sample Name:	uRQVqbl0sQ
Analysis ID:	519456
MD5:	b3912b6cc3cc37…
SHA1:	dcf11bf6eb7dc7c…
SHA256:	0d6118773c685f8…
Tags:	32 elf mirai renesas
Infos:	

Detection

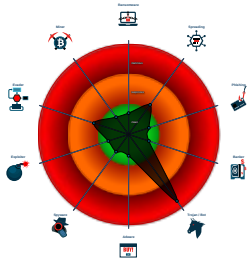


Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Uses known network protocols on no…
- Yara signature match
- Sample has stripped symbol table
- 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…
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

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:	519456
Start date:	10.11.2021
Start time:	19:01:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uRQVqbl0sQ
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:	mal92.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- uRQVqbl0sQ (PID: 5248, Parent: 5110, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/uRQVqbl0sQ
  - uRQVqbl0sQ New Fork (PID: 5250, Parent: 5248)
  - uRQVqbl0sQ New Fork (PID: 5251, Parent: 5248)
  - uRQVqbl0sQ New Fork (PID: 5252, Parent: 5248)
    - uRQVqbl0sQ New Fork (PID: 5256, Parent: 5252)
    - uRQVqbl0sQ New Fork (PID: 5257, Parent: 5252)
    - uRQVqbl0sQ New Fork (PID: 5258, Parent: 5252)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
uRQVqbl0sQ	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11040:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x110b0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11120:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11190:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11200:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11470:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x114c4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11518:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1156c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x115c0:$xo1: oMXKNNC\x0D\x17\x0C\x12
uRQVqbl0sQ	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x106c4:$x1: POST /cdn-cgi/ • 0x10ec0:$s1: LCOGQGPTGP • 0x10950:$s3: CFOKLKQVPCVMP • 0x10a74:$s4: QWRGPTKQMP • 0x10a44:$s5: HWCLVGAJ
uRQVqbl0sQ	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x106c4:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
uRQVqbl0sQ	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
uRQVqbl0sQ	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

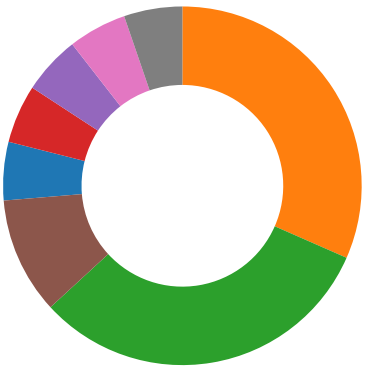
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5257.1.0000000021824ec1.000000001e5cec84.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x414:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x488:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x4fc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x570:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5e4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x864:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x8bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x914:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x96c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9c4:$xo1: oMXKNNC\x0D\x17\x0C\x12
5248.1.0000000021824ec1.000000001e5cec84.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x414:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x488:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x4fc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x570:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5e4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x864:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x8bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x914:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x96c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9c4:$xo1: oMXKNNC\x0D\x17\x0C\x12
5248.1.000000008e3e6270.00000000577ea06f.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11040:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x110b0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11120:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11190:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11200:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11470:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x114c4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11518:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1156c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x115c0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5248.1.000000008e3e6270.00000000577ea06f.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x106c4:$x1: POST /cdn-cgi/ • 0x10ec0:$s1: LCOGQGPTGP • 0x10950:$s3: CFOKLKQVPCVMP • 0x10a74:$s4: QWRGPTKQMP • 0x10a44:$s5: HWCLVGAJ
5248.1.000000008e3e6270.00000000577ea06f.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x106c4:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
Click to see the 13 entries				

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:

Antivirus / Scanner detection for submitted sample

Networking:

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

Uses known network protocols on non-standard ports

System Summary:

Malicious sample detected (through community Yara rule)

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

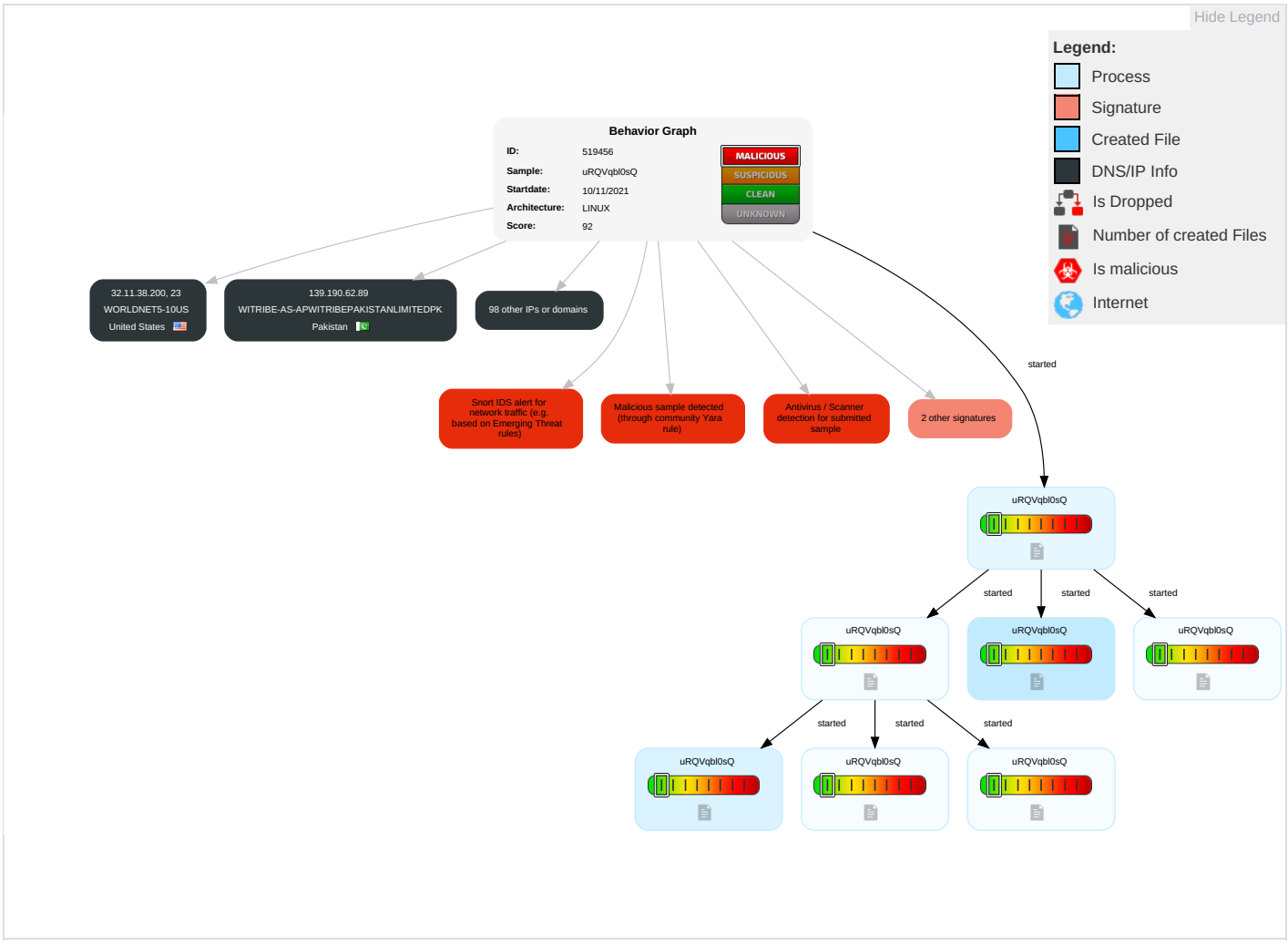
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
uRQVqbl0sQ	100%	Avira	LINUX/Mirai.bonb	

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
221.132.139.15	unknown	Japan		4721	JCNJupiterTelecommunicationsCoLtdJP	false
16.128.90.38	unknown	United States		unknown	unknown	false
254.17.65.139	unknown	Reserved		unknown	unknown	false
244.244.194.236	unknown	Reserved		unknown	unknown	false
212.234.251.210	unknown	France		3215	FranceTelecom-OrangeFR	false
220.232.97.168	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
198.246.6.47	unknown	United States		16489	WEBSTERUS	false
89.3.170.244	unknown	France		21502	ASN-NUMERICABLEFR	false
68.114.130.223	unknown	United States		20115	CHARTER-20115US	false
200.176.122.250	unknown	Brazil		22548	NucleodeInfeCoorddoPontoBR-NICBR	false
151.162.61.165	unknown	United States		45025	EDN-ASUA	false
185.244.103.18	unknown	Estonia		202635	SERVERFARMEE	false
119.47.138.206	unknown	Japan		7679	QTNETQTnetIncJP	false
165.112.93.230	unknown	United States		3527	NIH-NETUS	false
92.190.53.176	unknown	France		12479	UNI2-ASES	false
5.242.193.103	unknown	Sweden		1257	TELE2EU	false
104.220.195.178	unknown	United States		11404	AS-WAVE-1US	false
244.126.127.109	unknown	Reserved		unknown	unknown	false
218.57.164.61	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
195.52.156.254	unknown	Germany		12312	ECOTELDE	false
18.141.201.6	unknown	United States		16509	AMAZON-02US	false
53.21.24.250	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
207.142.148.42	unknown	United States		27229	WEBHOST-ASN1US	false
218.171.14.104	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
92.202.25.135	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
103.181.76.144	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
86.253.44.190	unknown	France		3215	FranceTelecom-OrangeFR	false
223.16.26.120	unknown	Hong Kong		18116	HGC-AS-APHGCGlobalCommunicationsLimitedHK	false
58.135.118.66	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
155.54.8.208	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
43.126.67.228	unknown	Japan		4249	LILLY-ASUS	false
253.40.131.78	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
201.41.94.26	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
85.251.205.254	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
27.170.232.227	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
114.115.199.72	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
13.32.10.46	unknown	United States		7018	ATT-INTERNET4US	false
92.171.195.197	unknown	France		3215	FranceTelecom-OrangeFR	false
248.250.252.65	unknown	Reserved		unknown	unknown	false
141.11.125.3	unknown	United Kingdom		3215	FranceTelecom-OrangeFR	false
69.82.241.181	unknown	United States		6167	CELLCO-PARTUS	false
32.11.38.200	unknown	United States		8030	WORLDNET5-10US	false
48.57.70.72	unknown	United States		2686	ATGS-MMD-ASUS	false
193.163.92.214	unknown	Denmark		1935	FR-RENATER-LIMOUSINReseauRegionalLimousinEU	false
246.115.0.143	unknown	Reserved		unknown	unknown	false
146.40.33.191	unknown	United States		197938	TRAVIANGAMESDE	false
253.150.99.23	unknown	Reserved		unknown	unknown	false
75.168.160.245	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
202.45.105.247	unknown	Australia		4739	INTERNODE-ASInternodePtyLtdAU	false
35.188.107.17	unknown	United States		15169	GOOGLEUS	false
37.209.0.142	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
72.46.16.160	unknown	United States		62833	HUDSONFIBERNETUS	false
5.112.252.160	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
139.230.139.168	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
197.96.148.24	unknown	South Africa		3741	ISZA	false
152.142.62.161	unknown	United States		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
39.162.171.8	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
184.121.172.5	unknown	United States		7922	COMCAST-7922US	false
102.126.15.78	unknown	Sudan		36972	MTNSD	false
240.181.11.98	unknown	Reserved		unknown	unknown	false
35.32.155.175	unknown	United States		36375	UMICH-AS-5US	false
113.184.12.149	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
195.194.212.211	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
35.75.185.27	unknown	United States		16509	AMAZON-02US	false
18.53.34.31	unknown	United States		3	MIT-GATEWAYSUS	false
47.169.7.58	unknown	United States		5650	FRONTIER-FRTRUS	false
244.216.167.217	unknown	Reserved		unknown	unknown	false
220.184.151.140	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
159.71.142.201	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
159.130.98.227	unknown	Norway		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
170.211.198.3	unknown	United States		21852	DISNW1US	false
220.96.250.128	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
203.6.38.83	unknown	Australia		9466	UUNET-JP-APUUNETJapanLimitedJP	false
36.228.252.69	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
105.221.136.145	unknown	South Africa		16637	MTNNS-ASZA	false
139.190.62.89	unknown	Pakistan		38547	WITRIBE-AS-APWITRIBEPAKISTANLIMITEDPK	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
76.154.169.141	unknown	United States		7922	COMCAST-7922US	false
91.176.208.16	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
147.87.33.23	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
144.57.21.205	unknown	Sweden		39052	SKANSKANET-ASSE	false
41.165.255.14	unknown	South Africa		36937	Neotel-ASZA	false
42.165.178.193	unknown	China		4249	LILLY-ASUS	false
85.125.243.155	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
142.58.38.188	unknown	Canada		11105	SFU-ASCA	false
169.82.255.8	unknown	United States		37611	AfrihostZA	false
60.43.113.150	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
121.185.252.163	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
53.204.40.144	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
100.233.7.7	unknown	United States		21928	T-MOBILE-AS21928US	false
104.123.190.215	unknown	United States		1299	TELIANETTeliaCarrierEU	false
242.12.196.250	unknown	Reserved		unknown	unknown	false
241.155.135.243	unknown	Reserved		unknown	unknown	false
102.139.101.79	unknown	Cote D'ivoire		36974	AFNET-ASCI	false
104.238.62.56	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	false
125.123.119.138	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
93.171.194.111	unknown	Czech Republic		61308	PVONET-ASRU	false
206.201.134.194	unknown	United States		17158	DATTO-BOSUS	false
181.106.193.94	unknown	Argentina		7303	TelecomArgentinaSAAR	false
70.86.14.48	unknown	United States		36351	SOFTLAYERUS	false
105.213.73.143	unknown	South Africa		16637	MTNNS-ASZA	false

Runtime Messages

Command:	/tmp/uRQVqbl0sQ
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	luciferisback ~un~stable~
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
165.112.93.230	hoho.arm	Get hash	malicious	Browse	
185.244.103.18	KXM253rCpW	Get hash	malicious	Browse	
195.52.156.254	wZ6O9wSQ4e	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
JCNJupiterTelecommunicationsCoLtdJP	p9rySh9WA4	Get hash	malicious	Browse	• 122.255.155.156

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8VANaS473t	Get hash	malicious	Browse	• 118.86.253.0
	anWxzNav9N	Get hash	malicious	Browse	• 111.90.2.168
	Xs0PMn85CN	Get hash	malicious	Browse	• 111.90.2.141
	iSdOB1UKQv	Get hash	malicious	Browse	• 221.132.139.43
	MMpysQ37RU	Get hash	malicious	Browse	• 112.137.96.139
	b3astmode.x86	Get hash	malicious	Browse	• 202.72.65.51
	94VG.x86	Get hash	malicious	Browse	• 110.93.55.88
	H8aSSMrsHO	Get hash	malicious	Browse	• 202.72.77.40
	x86	Get hash	malicious	Browse	• 114.134.127.190
	aTgXpPzFPV	Get hash	malicious	Browse	• 114.142.142.160
	sora.arm	Get hash	malicious	Browse	• 122.255.155.129
	jew.arm7	Get hash	malicious	Browse	• 202.72.65.63
	index_2021-09-30-12_54	Get hash	malicious	Browse	• 111.90.2.180
	b2wx6oZNsC	Get hash	malicious	Browse	• 203.89.37.217
	l88za3KqVX	Get hash	malicious	Browse	• 118.83.139.163
	sora.x86	Get hash	malicious	Browse	• 118.87.216.235
	k3dBuYbiCS	Get hash	malicious	Browse	• 118.87.246.111
	7b388AC1Fw	Get hash	malicious	Browse	• 111.90.108.145
	jew.arm7	Get hash	malicious	Browse	• 116.70.152.2
FranceTelecom-OrangeFR	QXFOZ3Cshc	Get hash	malicious	Browse	• 90.11.32.62
	sora.arm	Get hash	malicious	Browse	• 90.33.89.227
	lDawzTbABc	Get hash	malicious	Browse	• 90.18.247.113
	DVHEnaPp2d	Get hash	malicious	Browse	• 81.251.145.37
	HwcNrhNfZg	Get hash	malicious	Browse	• 83.195.96.126
	0LuSWzDmJG	Get hash	malicious	Browse	• 81.55.21.90
	cdglTQfNsE	Get hash	malicious	Browse	• 90.41.229.243
	arm7	Get hash	malicious	Browse	• 141.194.211.199
	x86	Get hash	malicious	Browse	• 62.161.114.230
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 193.252.45.45
	arm6	Get hash	malicious	Browse	• 86.201.52.84
	qgxgn5fQU1	Get hash	malicious	Browse	• 81.51.92.80
	BS0Dxmu2go	Get hash	malicious	Browse	• 90.123.158.171
	LAQh74RNEl	Get hash	malicious	Browse	• 86.214.221.128
	Kz2SeJpaxw	Get hash	malicious	Browse	• 86.210.41.166
	O4aHLhCviL	Get hash	malicious	Browse	• 195.6.118.226
	RrK5lgZ6gZ	Get hash	malicious	Browse	• 90.1.88.136
	BKyU0T5xcw	Get hash	malicious	Browse	• 86.252.106.139
	skonwRkAlJ	Get hash	malicious	Browse	• 109.212.215.140
	jyTZMJKPD2	Get hash	malicious	Browse	• 81.255.86.112

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, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.6966877269303895
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	uRQVqbl0sQ
File size:	74740
MD5:	b3912b6cc3cc37dedb72c478cb3b8a11
SHA1:	dcf11bf6eb7dc7cb78cc4b1155539a61946682be
SHA256:	0d6118773c685f8e28933621ea9069678136d09a361bab004229ea414aa89ab
SHA512:	85eae79e85dea4c78201fc872e98cb09b2c3f2be16de08ccf39387304dfeeb4135bbeb02dce1c8f54a54448c753d2c4b59c373cf18e1a01f598e44137a27e525
SSDEEP:	1536:XasfEz/gLltKgh5KcJfX6Ll0TAs3Y5m2CVaoYCBd2:XVIYL+yKcJil00+2MVaoY7
File Content Preview:	.ELF.....*.....@.4...d".....4. ...(.....@...@..... ... B.. B.$.....Q.td....././"O.n.....#.*@.....#.*@.....o&O.n...l....././../../a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	74340
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

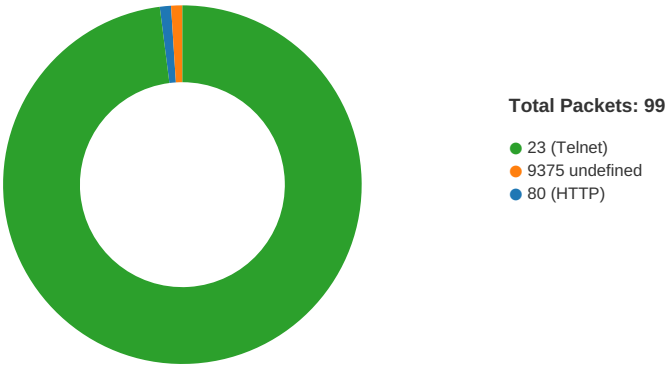
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0x105c0	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x4106a0	0x106a0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4106c4	0x106c4	0x12cc	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x422000	0x12000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x422008	0x12008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x422014	0x12014	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x422224	0x12224	0x4d8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x12224	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	0x400000	0x400000	0x11990	0x11990	4.7253	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x12000	0x422000	0x422000	0x224	0x6fc	1.7004	0x6	RW	0x10000		.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: uRQVqbl0sQ PID: 5248 Parent PID: 5110

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	/tmp/uRQVqbl0sQ
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: uRQVqbl0sQ PID: 5250 Parent PID: 5248

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: uRQVqbl0sQ PID: 5251 Parent PID: 5248

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uRQVqbl0sQ PID: 5252 Parent PID: 5248

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uRQVqbl0sQ PID: 5256 Parent PID: 5252

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: uRQVqbl0sQ PID: 5257 Parent PID: 5252

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: uRQVqbl0sQ PID: 5258 Parent PID: 5252

General

Start time:	19:02:35
Start date:	10/11/2021
Path:	/tmp/uRQVqbl0sQ
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9