ID: 517128
Sample Name: rXFu2DZdQq
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:26:16
Date: 07/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

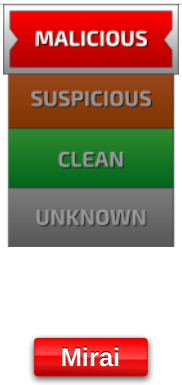
Linux Analysis Report rXFu2DZdQq

Overview

General Information

Sample Name:	rXFu2DZdQq
Analysis ID:	517128
MD5:	26a1c18159fc07b..
SHA1:	a599e8e6312864..
SHA256:	18bf54ce4c9bab8..
Tags:	32 elf mips mirai
Infos:	

Detection

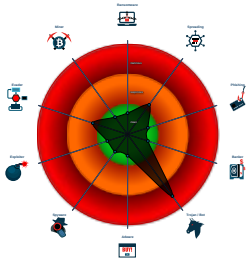


Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- 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 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:	517128
Start date:	07.11.2021
Start time:	03:26:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rXFu2DZdQq
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:	mal84.troj.lin@0/1@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- rXFu2DZdQq (PID: 5243, Parent: 5118, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/rXFu2DZdQq
  - rXFu2DZdQq New Fork (PID: 5245, Parent: 5243)
    - rXFu2DZdQq New Fork (PID: 5247, Parent: 5245)
    - rXFu2DZdQq New Fork (PID: 5249, Parent: 5245)
    - rXFu2DZdQq New Fork (PID: 5250, Parent: 5245)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
rXFu2DZdQq	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x182a0:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x18310:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x18388:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x184dc:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x18554:$xo1: zXM^[[V\x18\x02\x19\x07
rXFu2DZdQq	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x176e4:$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
rXFu2DZdQq	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

PCAP (Network Traffic)

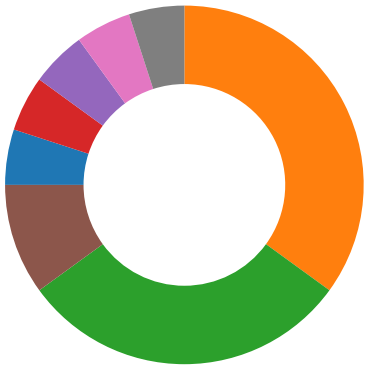
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5243.1.0000000074ad5e34.00000000461826e6.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x24f0:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x2564:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x25dc:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x2628:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x26a0:$xo1: zXM^[[V\x18\x02\x19\x07
5247.1.0000000074ad5e34.00000000461826e6.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x24f0:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x2564:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x25dc:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x2628:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x26a0:$xo1: zXM^[[V\x18\x02\x19\x07
5247.1.000000007d118295.00000000e341c292.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x182a0:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x18310:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x18388:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x184dc:$xo1: zXM^[[V\x18\x02\x19\x07 • 0x18554:$xo1: zXM^[[V\x18\x02\x19\x07
5247.1.000000007d118295.00000000e341c292.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x176e4:$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
5247.1.000000007d118295.00000000e341c292.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

Click to see the 3 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:

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

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

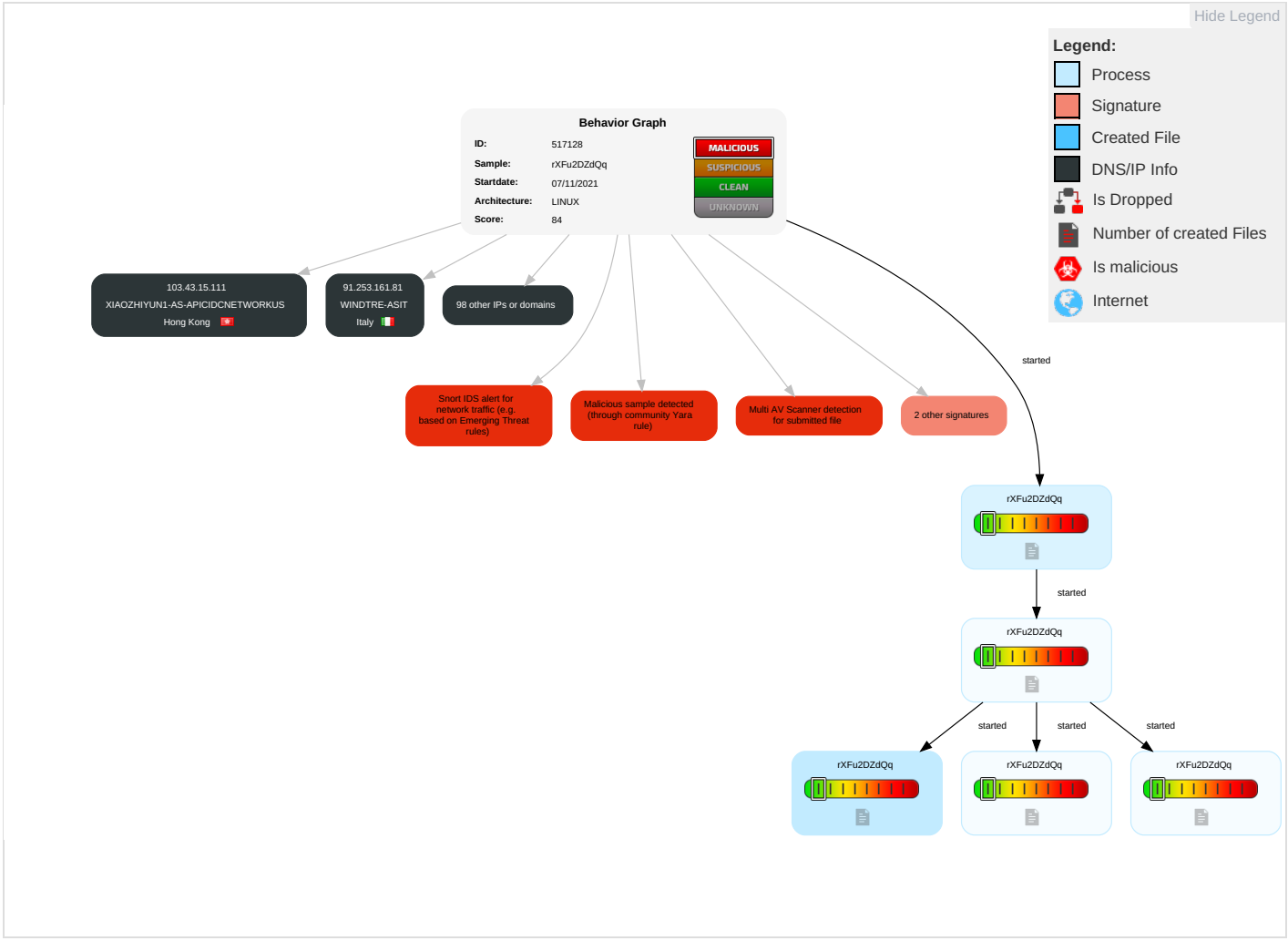
Mitre Att&ck Matrix

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
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
rXFu2DZdQq	52%	Virustotal		Browse
rXFu2DZdQq	47%	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
187.82.196.51	unknown	Brazil		26615	TIMSABR	false
216.254.75.210	unknown	United States		18566	MEGAPATH5-US	false
246.76.30.179	unknown	Reserved		unknown	unknown	false
133.144.196.27	unknown	Japan		2500	WIDE-BBWIDEProjectJP	false
4.154.245.182	unknown	United States		3356	LEVEL3US	false
108.2.91.108	unknown	United States		701	UUNETUS	false
14.231.22.123	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
146.97.25.112	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
40.210.199.224	unknown	United States		4249	LILLY-ASUS	false
81.89.1.23	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
152.41.163.246	unknown	United States		22854	CATAWBA-COLLEGEUS	false
169.163.220.214	unknown	United States		37611	AfrihostZA	false
89.91.189.85	unknown	France		5410	BOUYGTEL-ISPFR	false
172.114.72.158	unknown	United States		20001	TWC-20001-PACWESTUS	false
217.141.52.187	unknown	Italy		3269	ASN-IBSNAZIT	false
188.245.52.56	unknown	Iran (ISLAMIC Republic Of)		16322	PARSONLINETehran-IRANIR	false
124.51.222.181	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
104.100.196.170	unknown	United States		16625	AKAMAI-ASUS	false
183.218.20.92	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
96.16.111.97	unknown	United States		16625	AKAMAI-ASUS	false
166.42.58.90	unknown	United States		3372	MCI-ASNUS	false
249.7.138.132	unknown	Reserved		unknown	unknown	false
95.137.253.60	unknown	Georgia		34797	SYSTEM-NETGE	false
20.49.104.100	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
149.239.156.127	unknown	Germany		12291	DPAG-ASDeutschePostAGDE	false
16.46.126.70	unknown	United States		unknown	unknown	false
209.144.94.230	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
99.55.160.71	unknown	United States		7018	ATT-INTERNET4US	false
92.0.155.128	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
80.68.167.170	unknown	Germany		20918	PI-ASHertzstr61DE	false
93.128.152.101	unknown	Germany		6805	TDDE-ASN1DE	false
83.88.91.35	unknown	Denmark		3292	TDCTDCASDK	false
151.46.4.62	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
208.225.237.88	unknown	United States		4208	THE-ISERV-COMPANYUS	false
123.128.154.35	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
144.37.65.136	unknown	United States		2152	CSUNET-NWUS	false
245.239.236.26	unknown	Reserved		unknown	unknown	false
75.158.188.87	unknown	Canada		852	ASN852CA	false
147.22.141.223	unknown	United States		10796	TWC-10796-MIDWESTUS	false
45.178.186.249	unknown	Argentina		27690	CITYTECHSAAR	false
194.86.82.251	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
152.243.213.122	unknown	Brazil		26599	TELEFONICABRASILSABR	false
97.148.1.225	unknown	United States		6167	CELLCO-PARTUS	false
4.86.31.199	unknown	United States		3356	LEVEL3US	false
75.166.156.208	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
118.183.197.89	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
65.136.113.218	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.13.63.168	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
125.217.34.176	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
164.146.45.175	unknown	South Africa		37130	SITA-ASZA	false
173.32.114.26	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
86.137.239.164	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
218.96.204.176	unknown	China		10212	CHINAENTERCOMChinaEnterpriseCommunicationsLtdCN	false
169.133.102.109	unknown	United States		18815	AS-CITY-AND-COUNTY-OF-DENVERUS	false
82.64.122.193	unknown	France		12322	PROXADFR	false
39.241.125.132	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
198.44.255.253	unknown	United States		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
163.223.113.142	unknown	unknown		4766	KIXS-AS-KRKoreaTelecomKR	false
240.153.133.196	unknown	Reserved		unknown	unknown	false
27.161.187.209	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
164.7.60.221	unknown	France		44013	SANDVIK-ASSE	false
196.55.166.116	unknown	South Africa		53271	PHENIXCITYCABLEUS	false
220.68.20.28	unknown	Korea Republic of		18038	KNUE-AS-KRKoreaNationalUniversityofEducationKR	false
121.197.114.194	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
102.108.105.197	unknown	Tunisia		37693	TUNISIANATN	false
96.135.225.250	unknown	United States		7922	COMCAST-7922US	false
185.65.133.224	unknown	Sweden		39351	ESAB-ASSE	false
146.168.153.96	unknown	United States		26504	METRO-VA-KGUS	false
202.248.20.162	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
110.1.104.165	unknown	Japan		10013	FBDCFreeBitCoLtdJP	false
39.235.30.120	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
4.123.39.19	unknown	United States		3356	LEVEL3US	false
193.50.50.243	unknown	France		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
180.205.110.83	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
94.22.161.43	unknown	Finland		15527	ANVIASilmukkatie6VaasaFinlandFI	false
200.42.226.254	unknown	Dominican Republic		12066	ALTICEDOMINICANASADO	false
209.252.203.213	unknown	United States		7029	WINDSTREAMUS	false
145.117.208.60	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
196.218.57.177	unknown	Egypt		8452	TE-ASTE-ASEG	false
205.184.166.26	unknown	United States		1239	SPRINTLINKUS	false
12.150.44.16	unknown	United States		2386	INS-ASUS	false
218.184.12.238	unknown	Taiwan; Republic of China (ROC)		7482	APOL-ASAsiaPacificOnlineServiceIncTW	false
99.133.254.230	unknown	United States		7018	ATT-INTERNET4US	false
153.142.235.218	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
109.171.77.44	unknown	Russian Federation		15774	TTK-RTLRetailRU	false
64.47.250.241	unknown	United States		19855	MASERGYUS	false
91.253.161.81	unknown	Italy		24608	WINDTRE-ASIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.13.136.116	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
36.83.192.252	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
159.10.215.208	unknown	United States		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
47.225.135.124	unknown	United States		20115	CHARTER-20115US	false
185.100.7.101	unknown	France		35393	EURO-WEB-ASFR	false
81.92.108.120	unknown	Switzerland		41872	FLASHCABLEFlashcableNetworkCH	false
99.201.155.108	unknown	United States		10507	SPCSUS	false
117.34.51.210	unknown	China		4835	CHINANET-IDC-SNChinaTelecomGroupCN	false
162.35.203.147	unknown	United States		11363	FUJITSU-USAUS	false
103.43.15.111	unknown	Hong Kong		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	false
104.150.12.0	unknown	United States		1832	SMUUS	false
8.19.45.192	unknown	United States		40393	CROSSLINKNETWORKSUS	false
123.87.41.52	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false

Runtime Messages

Command:	/tmp/rXFu2DZdQq
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	SHORELINE BOTNET THA REAL SHIT NIGGA
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WIDE-BBWIDEProjectJP	sora.x86	Get hash	malicious	Browse	• 133.144.38.28
	jd6caIAf2C	Get hash	malicious	Browse	• 133.147.190.129
	PyZcDaysXO	Get hash	malicious	Browse	• 133.138.237.158
	8A5Aub0x7r	Get hash	malicious	Browse	• 133.144.3.145
	lCxHEay3O0	Get hash	malicious	Browse	• 163.221.181.211
	jew.x86	Get hash	malicious	Browse	• 202.249.105.233
	sora.arm7	Get hash	malicious	Browse	• 133.144.113.167
	z0x3n.x86	Get hash	malicious	Browse	• 133.144.147.44
	3DAMhv0DFI	Get hash	malicious	Browse	• 133.144.38.29
	G3kV1FpdsS	Get hash	malicious	Browse	• 133.144.14.57

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	U6lZQUtrU5	Get hash	malicious	Browse	• 133.147.184.188
	gHQh80mu53	Get hash	malicious	Browse	• 133.144.38.29
	a2EOBr2vBx	Get hash	malicious	Browse	• 133.4.232.145
	OVLzirpJIn	Get hash	malicious	Browse	• 203.178.222.174
	Kt5bCp5OtV	Get hash	malicious	Browse	• 133.144.184.45
	ICmyQqyEQF	Get hash	malicious	Browse	• 163.221.41.92
	TG42Y4Bxqh	Get hash	malicious	Browse	• 133.144.38.70
	W1233pilTq	Get hash	malicious	Browse	• 133.144.38.20
	Ym8W6Wk5bt	Get hash	malicious	Browse	• 133.146.252.174
	peach.arm	Get hash	malicious	Browse	• 133.139.135.9
MEGAPATH5-US	xd.x86	Get hash	malicious	Browse	• 74.0.107.207
	B94t90Yyoz	Get hash	malicious	Browse	• 68.164.212.33
	nY0UOuOPzl	Get hash	malicious	Browse	• 69.17.71.211
	6A9RyJXCd7	Get hash	malicious	Browse	• 68.167.50.38
	BsXhlyIHzC	Get hash	malicious	Browse	• 74.1.232.91
	aTQ4RalkUs	Get hash	malicious	Browse	• 64.81.50.147
	8VANaS473t	Get hash	malicious	Browse	• 67.100.40.24
	uohdbohpYb	Get hash	malicious	Browse	• 72.245.54.77
	oiHTZaiKnI	Get hash	malicious	Browse	• 64.145.166.184
	x86	Get hash	malicious	Browse	• 64.81.97.172
	eNrYzJWFvB	Get hash	malicious	Browse	• 74.0.4.76
	lyVSOhLA7o.dll	Get hash	malicious	Browse	• 67.102.15.117
	cosvgegE1S	Get hash	malicious	Browse	• 67.101.209.8
	uK570ZEpyQ	Get hash	malicious	Browse	• 66.135.18.131
	fzkfNBkz1C	Get hash	malicious	Browse	• 68.167.74.30
	UYnpKcFZ2s	Get hash	malicious	Browse	• 65.84.21.67
	jvilYCvWBc	Get hash	malicious	Browse	• 74.1.219.76
	Tf9ATzpdKR	Get hash	malicious	Browse	• 72.244.131.121
	H9pX0VKTN5	Get hash	malicious	Browse	• 67.102.2.139
	Z1JWqe0tZn	Get hash	malicious	Browse	• 74.211.154.5
TIMSABR	AER0hx5txK	Get hash	malicious	Browse	• 177.108.222.212
	IYcCOLfGT7	Get hash	malicious	Browse	• 191.171.55.253
	QX4Kudvf1x	Get hash	malicious	Browse	• 191.160.73.87
	sora.x86	Get hash	malicious	Browse	• 177.108.8.49
	sora.x86	Get hash	malicious	Browse	• 187.48.24.238
	sora.arm7	Get hash	malicious	Browse	• 177.28.52.138
	WmEErPtdS9	Get hash	malicious	Browse	• 177.167.27.69
	mipsel	Get hash	malicious	Browse	• 179.34.244.156
	sora.x86	Get hash	malicious	Browse	• 191.160.203.209
	Hilix.arm	Get hash	malicious	Browse	• 179.77.43.231
	BsXhlyIHzC	Get hash	malicious	Browse	• 186.228.156.194
	aTQ4RalkUs	Get hash	malicious	Browse	• 179.34.87.249
	RPov9E0iot	Get hash	malicious	Browse	• 191.175.246.1
	8VANaS473t	Get hash	malicious	Browse	• 187.81.235.224
	uohdbohpYb	Get hash	malicious	Browse	• 187.81.52.9
	yVbcX1sEtS	Get hash	malicious	Browse	• 191.133.1.14
	1Y2rsDBP9s	Get hash	malicious	Browse	• 177.167.52.25
	Ko84iLip1u	Get hash	malicious	Browse	• 179.76.101.122
	mRQwOz6Oit	Get hash	malicious	Browse	• 179.76.148.153
	u4M7XeqKtD	Get hash	malicious	Browse	• 177.29.102.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.NLxMNc (deleted)	
Process:	/tmp/rXFu2DZdQq
File Type:	ASCII text
Category:	dropped
Size (bytes):	273
Entropy (8bit):	3.550633563118011
Encrypted:	false
SSDEEP:	6:URd3dRyQTLxT/VU8VbsRyQTfz/VDM/V+4D/VH:lV9TcEbcTZMfF
MD5:	F1528465949CC4144AF716D55DF52373
SHA1:	0AF6474F0D18C3F063EA550C48C4DCFF0F099AD1
SHA-256:	776FAE47C627F31A35A05BA74BE1685847B0DAA1688F809FF97F7644FD467354
SHA-512:	9A2EDB5888B7CC41318DB75E9CCA21316341188D10D8BE917C6D600DB23CD758D636E35D56F60651EAE197BFC6A24E2DECBB0FA44A0EE7BB3A5341E127717925
Malicious:	false
Reputation:	low
Preview:	400000-41a000 r-xp 00000000 fd:00 542525 /tmp/rXFu2DZdQq.45a000-45b000 rw-p 0001a000 fd:00 542525 /tmp/rXFu2DZdQq.45b000-45e000 rw-p 00000000 00:00 0 .7f7ff000-7f800000 ---p 00000000 00:00 0 .7f800000-80000000 rw-p 00000000 00:00 0 [stack].

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.574394529956213
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	rXFu2DZdQq
File size:	108960
MD5:	26a1c18159fc07b82668d7b67c62bce3
SHA1:	a599e8e631286477fa44df15054e4fdf5c53d522
SHA256:	18bf54ce4c9bab8cfecbace5f3b8f5f3f18f85446205aea0c4420d7280671837
SHA512:	75a166f7bc3df47510984d270c01287078f0ea683b9c1ff98f09bff8fcb000e62f9118c21448350695b8f1ddd1694b0f028b12082c6b74c0689ab58ada705a65
SSDEEP:	1536:g9DYWFx+xx+AaEPilMR2jk2EkZ+BzYojKoOvDBgplbngVZ14hvG:gqWFx+xUA0OR2hEkZ+BlpZK1+v
File Content Preview:	.ELF.....`.@.4.....4. ...(.....@...@.`...`.....E...E.@....+.....Q.td.....<\ ".'!.....'.....<8".'!... .....9'.. .....<.". '!...$.....v9

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	108440
Section Header Size:	40

ELF header

Number of Section Headers:	13
Header String Table Index:	12

Sections

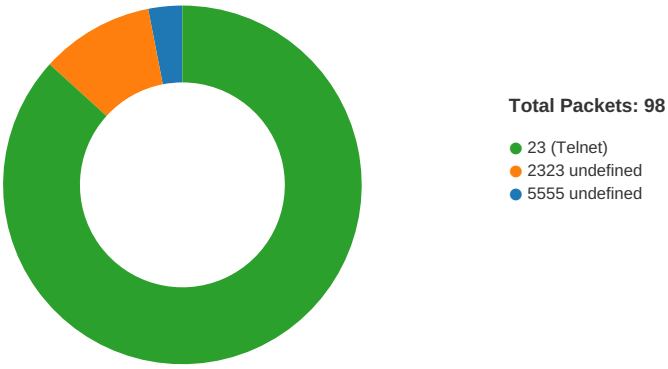
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x17560	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x417680	0x17680	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4176e0	0x176e0	0x1f80	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x45a000	0x1a000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x45a008	0x1a008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x45a020	0x1a020	0x2e0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x45a300	0x1a300	0x440	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x45a740	0x1a740	0x1c	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x45a760	0x1a740	0x2460	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x8b8	0x1a740	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x1a740	0x57	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	0x19660	0x19660	3.6781	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1a000	0x45a000	0x45a000	0x740	0x2bc0	2.3599	0x6	RW	0x10000		.ctors .dtors .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: rXFu2DZdQq PID: 5243 Parent PID: 5118

General

Start time:	03:26:57
Start date:	07/11/2021
Path:	/tmp/rXFu2DZdQq
Arguments:	/tmp/rXFu2DZdQq
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: rXFu2DZdQq PID: 5245 Parent PID: 5243

General

Start time:	03:26:58
Start date:	07/11/2021
Path:	/tmp/rXFu2DZdQq
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: rXFu2DZdQq PID: 5247 Parent PID: 5245

General

Start time:	03:26:58
Start date:	07/11/2021
Path:	/tmp/rXFu2DZdQq
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: rXFu2DZdQq PID: 5249 Parent PID: 5245

General

Start time:	03:26:58
Start date:	07/11/2021
Path:	/tmp/rXFu2DZdQq
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: rXFu2DZdQq PID: 5250 Parent PID: 5245

General

Start time:	03:26:58
Start date:	07/11/2021
Path:	/tmp/rXFu2DZdQq
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Deleted

File Read

File Written

Directory Enumerated