ID: 452443
Sample Name: RzBo7FFhaM
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:16:44
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

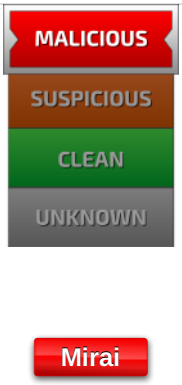
Linux Analysis Report RzBo7FFhaM

Overview

General Information

Sample Name:	RzBo7FFhaM
Analysis ID:	452443
MD5:	5f2b063b3423065.
SHA1:	bca27e6bc1806e..
SHA256:	dfd80dcc5c2b9f5…
Tags:	32 elf intel mirai
Infos:	

Detection

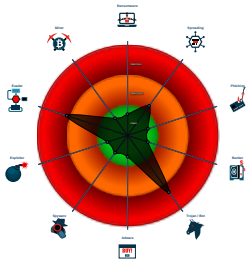


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Sample is packed with UPX
- Uses known network protocols on no…
- Detected TCP or UDP traffic on non…
- Enumerates processes within the "p…
- Sample contains only a LOAD segm…
- Sample listens on a socket
- Sample tries to kill a process (SIGK…

Classification



General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452443
Start date:	22.07.2021
Start time:	11:16:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RzBo7FFhaM
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Analysis Mode:	default
Detection:	MAL
Classification:	mal72.troj.evad.lin@0/2@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu1**
- RzBo7FFhaM (PID: 4567, Parent: 4497, MD5: 5f2b063b3423065cc1c6ea63979c6f46) Arguments: /tmp/RzBo7FFhaM
  - RzBo7FFhaM New Fork (PID: 4569, Parent: 4567)
    - RzBo7FFhaM New Fork (PID: 4607, Parent: 4569)
    - RzBo7FFhaM New Fork (PID: 4608, Parent: 4569)
      - RzBo7FFhaM New Fork (PID: 4611, Parent: 4608)
        - RzBo7FFhaM New Fork (PID: 4617, Parent: 4611)
        - RzBo7FFhaM New Fork (PID: 4618, Parent: 4611)
      - RzBo7FFhaM New Fork (PID: 4612, Parent: 4608)
      - RzBo7FFhaM New Fork (PID: 4613, Parent: 4608)
  - RzBo7FFhaM New Fork (PID: 4570, Parent: 4567)
  - RzBo7FFhaM New Fork (PID: 4571, Parent: 4567)
    - RzBo7FFhaM New Fork (PID: 4572, Parent: 4571)
      - RzBo7FFhaM New Fork (PID: 4609, Parent: 4572)
      - RzBo7FFhaM New Fork (PID: 4610, Parent: 4572)
    - RzBo7FFhaM New Fork (PID: 4573, Parent: 4571)
    - RzBo7FFhaM New Fork (PID: 4574, Parent: 4571)
- systemd New Fork (PID: 4594, Parent: 1)
- sshd (PID: 4594, Parent: 1, MD5: 661b2a2da3b6c7d7ef41d0b9da1caa3b) 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
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection

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

Data Obfuscation:

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection:

Hooking and other Techniques for Hiding and Protection:
Uses known network protocols on non-standard ports

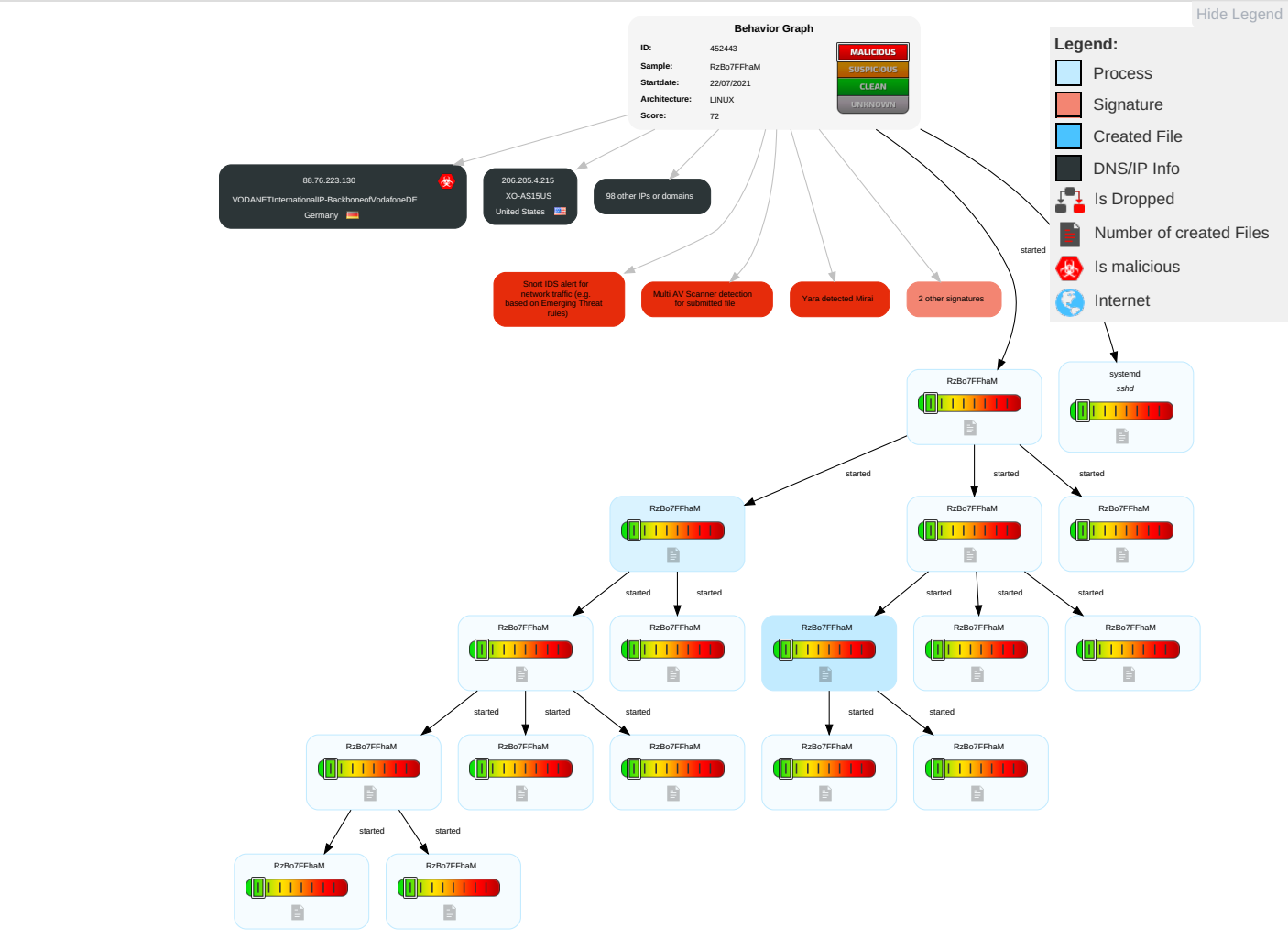
Mitre Att&ck Matrix

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	Obfuscated Files or Information 1	OS Credential Dumping 1	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Standard Port 1 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RzBo7FFhaM	37%	Virustotal		Browse
RzBo7FFhaM	41%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
136.46.33.136	unknown	United States		16591	GOOGLE-FIBERUS	false
183.242.10.118	unknown	China		56048	CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN	false
42.192.16.245	unknown	China		4249	LILLY-ASUS	false
171.242.137.96	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
36.48.216.249	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
174.210.64.248	unknown	United States		22394	CELLCOUS	false
123.220.91.171	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
9.165.14.249	unknown	United States		3356	LEVEL3US	false
111.169.5.91	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
119.219.35.126	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
112.23.65.213	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
38.223.94.1	unknown	United States		174	COGENT-174US	false
179.208.175.235	unknown	Brazil		28573	CLAROSABR	false
75.30.223.231	unknown	United States		7018	ATT-INTERNET4US	false
152.77.20.251	unknown	France		1942	FR-TIGRETOileInformatiqueGRENobloiseEU	false
208.100.207.179	unknown	United States		27553	TELNETUS	false
68.217.157.227	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
118.96.77.178	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
108.233.118.254	unknown	United States		7018	ATT-INTERNET4US	false
196.179.131.38	unknown	Tunisia		37693	TUNISIANATN	false
8.125.184.31	unknown	United States		3356	LEVEL3US	false
201.13.201.98	unknown	Brazil		27699	TELEFONICABRASILSABR	false
99.162.223.238	unknown	United States		7018	ATT-INTERNET4US	false
62.52.13.78	unknown	Germany		6805	TDDE-ASN1DE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.0.112.242	unknown	United States		7029	WINDSTREAMUS	false
108.115.74.39	unknown	United States		10507	SPCSUS	false
207.137.79.229	unknown	United States		174	COGENT-174US	false
47.131.200.161	unknown	Canada		34533	ESAMARA-ASRU	false
70.223.58.85	unknown	United States		22394	CELLCOUS	false
40.134.48.97	unknown	United States		7029	WINDSTREAMUS	false
36.143.104.9	unknown	China		24547	CMNET-V4HEBEI-AS-APHebeiMobileCommunicationCompanyLimit	false
206.205.4.215	unknown	United States		2828	XO-AS15US	false
202.173.50.0	unknown	Taiwan; Republic of China (ROC)		9671	TRADEVAN-AS-APTrade-VanInformaitonServicesCoTW	false
162.53.22.186	unknown	Canada		22910	LOBLAW-COMPANIESCA	false
5.144.113.88	unknown	Russian Federation		8359	MTSRU	false
213.152.62.159	unknown	United Kingdom		12513	ECLIPSEGB	false
191.185.136.140	unknown	Brazil		28573	CLAROSABR	false
190.105.124.240	unknown	Argentina		27984	VerTvSAAR	false
188.221.85.54	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
141.78.55.169	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
243.158.2.206	unknown	Reserved		unknown	unknown	false
93.36.234.186	unknown	Italy		12874	FASTWEBIT	false
201.219.1.123	unknown	Ecuador		28006	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEPEC	false
204.140.211.61	unknown	United States		226	LOS-NETTOS-ASUS	false
216.102.77.63	unknown	United States		23369	SCOEUS	false
102.253.185.135	unknown	South Africa		5713	SAIX-NETZA	false
80.64.57.116	unknown	United Kingdom		5413	AS5413GB	false
252.247.7.105	unknown	Reserved		unknown	unknown	false
60.104.208.231	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
94.204.216.81	unknown	United Arab Emirates		15802	DU-AS1AE	false
71.235.103.14	unknown	United States		7922	COMCAST-7922US	false
145.137.6.97	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
39.149.103.81	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
83.164.244.184	unknown	Austria		35369	LINZAG-TELEKOM-ASAT	false
247.64.171.23	unknown	Reserved		unknown	unknown	false
147.146.113.251	unknown	United States		2152	CSUNET-NWUS	false
154.24.24.138	unknown	United States		174	COGENT-174US	false
160.225.231.81	unknown	Angola		11259	ANGOLATELECOMAO	false
255.122.221.38	unknown	Reserved		unknown	unknown	false
249.95.62.212	unknown	Reserved		unknown	unknown	false
154.161.58.47	unknown	Ghana		30986	SCANCOMGH	false
85.33.66.139	unknown	Italy		3269	ASN-IBSNAZIT	false
201.124.158.106	unknown	Mexico		8151	UninetSAdeCVMX	false
112.245.183.76	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
179.211.42.59	unknown	Brazil		28573	CLAROSABR	false
126.1.4.74	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
117.105.41.9	unknown	Singapore		10010	TOKAITOKAICommunicationsCorporationJP	false
35.71.106.231	unknown	United States		237	MERIT-AS-14US	false
122.195.46.203	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
242.244.62.65	unknown	Reserved		unknown	unknown	false
31.100.75.39	unknown	United Kingdom		12576	EELtdGB	false
254.161.12.30	unknown	Reserved		unknown	unknown	false
209.241.155.125	unknown	United States		3356	LEVEL3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
249.16.13.87	unknown	Reserved		unknown	unknown	false
151.176.50.159	unknown	Germany		45025	EDN-ASUA	false
126.203.49.252	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
188.48.187.235	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
119.219.35.173	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
209.161.133.172	unknown	United States		4043	MIC-ASNUS	false
110.71.105.232	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
187.82.196.65	unknown	Brazil		26615	TIMSABR	false
187.82.196.67	unknown	Brazil		26615	TIMSABR	false
79.241.228.42	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
101.61.228.21	unknown	Italy		210278	SKYIT-BBIT	false
46.28.163.180	unknown	Spain		199312	MEGAVISTAES	false
61.199.63.21	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
150.223.252.28	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
159.156.178.59	unknown	Switzerland		34578	BEDAGCH	false
88.76.223.130	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	true
34.176.183.173	unknown	United States		2686	ATGS-MMD-ASUS	false
73.170.89.85	unknown	United States		7922	COMCAST-7922US	false
9.59.159.161	unknown	United States		3356	LEVEL3US	false
27.190.168.100	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
136.235.237.43	unknown	United States		33235	SANJUANUS	false
81.9.255.221	unknown	Spain		12338	EUSKALTELES	false
110.222.168.171	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
147.13.127.2	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
246.249.140.24	unknown	Reserved		unknown	unknown	false
193.144.167.193	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
251.222.125.13	unknown	Reserved		unknown	unknown	false

Runtime Messages

Command:	/tmp/RzBo7FFhaM
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VIETEL-AS-APViettelGroupVN	s54l0GKMh9	Get hash	malicious	Browse	• 115.76.248.177
	92CRMNlBq8	Get hash	malicious	Browse	• 171.234.129.42
	YazlX01sZD	Get hash	malicious	Browse	• 171.235.102.241
	jhUxzb7jPW	Get hash	malicious	Browse	• 171.242.238.121
	FawDB415Y0	Get hash	malicious	Browse	• 171.244.89.44
	Vk3A1yJJMg	Get hash	malicious	Browse	• 171.226.193.181
	rnQYDw7A4G	Get hash	malicious	Browse	• 27.72.64.111
	FN0ZF2Nm21	Get hash	malicious	Browse	• 171.226.193.151
	Xlojlgo2gb	Get hash	malicious	Browse	• 171.235.72.9
	AD0cHN7dR2	Get hash	malicious	Browse	• 171.242.137.51
	o0z4JJpYNf	Get hash	malicious	Browse	• 171.242.238.145
	0aC0TBcdxb	Get hash	malicious	Browse	• 27.77.89.33
	Rb5g620lnp	Get hash	malicious	Browse	• 27.66.4.75
	2Mg6rkHj0G.exe	Get hash	malicious	Browse	• 27.72.107.215
	uOGIhyiQuh.exe	Get hash	malicious	Browse	• 171.252.242.5
	segYCksCNt.exe	Get hash	malicious	Browse	• 27.72.151.9
	Jiif5YqIlM.exe	Get hash	malicious	Browse	• 27.72.107.215
	Ol802S6Msi.exe	Get hash	malicious	Browse	• 27.72.107.215
	buhy005VdX.exe	Get hash	malicious	Browse	• 27.72.107.215
	nO50RHxIfz.exe	Get hash	malicious	Browse	• 27.72.107.215
GOOGLE-FIBERUS	Xr3hmBQcmw	Get hash	malicious	Browse	• 136.41.234.96
	rxfttQnoO5	Get hash	malicious	Browse	• 136.37.58.28
	qgQgEjI283	Get hash	malicious	Browse	• 136.62.91.237
	YazlX01sZD	Get hash	malicious	Browse	• 136.61.172.253
	wZ6O9wSQ4e	Get hash	malicious	Browse	• 136.45.143.132
	nT7K5GG5km	Get hash	malicious	Browse	• 99.198.164.146
	bdOPjE89ck.dll	Get hash	malicious	Browse	• 136.63.121.184
	mssecsvc.exe	Get hash	malicious	Browse	• 136.56.86.243
	qYed15XPrg.exe	Get hash	malicious	Browse	• 136.40.21.229
CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN	U5q75RGCmQ	Get hash	malicious	Browse	• 223.202.82.200
	Dvf7OP92yJ	Get hash	malicious	Browse	• 183.242.8.85
	nh4k2eRHvx	Get hash	malicious	Browse	• 120.247.64.126
	mssecsvc.exe	Get hash	malicious	Browse	• 117.134.85.82
	this_message_in_html.html	Get hash	malicious	Browse	• 117.121.28.5
LILLY-ASUS	d8dgn3wGJL	Get hash	malicious	Browse	• 43.152.190.246
	92CRMNlBq8	Get hash	malicious	Browse	• 43.116.24.113
	5qpsqg7U0G	Get hash	malicious	Browse	• 43.86.6.1
	U5q75RGCmQ	Get hash	malicious	Browse	• 42.128.100.146
	U4r9W64doy	Get hash	malicious	Browse	• 43.108.134.117
	CefN2XNyFi	Get hash	malicious	Browse	• 43.72.210.9
	MD5OxTSc6i	Get hash	malicious	Browse	• 42.9.212.148
	Qka3fi8NpL	Get hash	malicious	Browse	• 43.4.159.55
	xjYvqOne1t	Get hash	malicious	Browse	• 42.172.219.145
	SUpODCSauS	Get hash	malicious	Browse	• 43.26.93.139
	rxfttQnoO5	Get hash	malicious	Browse	• 40.216.186.163
	CGjf615z6v	Get hash	malicious	Browse	• 40.35.223.43
	u47x3rc20t	Get hash	malicious	Browse	• 43.90.242.232
	SvmxfeZM5Z	Get hash	malicious	Browse	• 42.14.120.137
	TFG18FA4eD	Get hash	malicious	Browse	• 40.183.20.12
	eAtDhymLzp	Get hash	malicious	Browse	• 42.219.241.34
	zWumjXhWWz	Get hash	malicious	Browse	• 40.58.230.116
	qgQgEjI283	Get hash	malicious	Browse	• 42.128.38.237
	e4qhQIKEim	Get hash	malicious	Browse	• 40.197.113.210
	zhPAQB7FPV	Get hash	malicious	Browse	• 42.142.72.94

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/4594/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:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:F:F
MD5:	25DA75E0CA42D728137E6F430666FF54
SHA1:	0FD6EDF398457D24C110D2AA9EEF6759A844A6B8
SHA-256:	52B059B061BAC9D562A68810104B14F8CA461975F247C5443C85F166C646B979
SHA-512:	C015EA4577A3F7FD126D43263A521A82BB728086E01F0787B6A1A36F794EC60D47204C36A3EA4C5897C776D7FD8C4EE96413413FD2E7E2DBA198CF3C5A00FCF
Malicious:	false
Reputation:	low
Preview:	4594.

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.871311316303272
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	RzBo7FFhaM
File size:	24728
MD5:	5f2b063b3423065cc1c6ea63979c6f46
SHA1:	bca27e6bc1806e26a0f547d275e06e5d6c39b5dc
SHA256:	dfd80dcc5c2b9f51fcd45bc6e4b494aa777500ef769c17e7aa9d63287adb92b1
SHA512:	427290c951a552f82ac701334b8c8b5c223798af98398f6aeca964d271983060371ee4dada5a646cb7c598e45f3a82d0ee00ad0e0cb82cb9c9754dea332c6388
SSDEEP:	384:MvDKKQOcRpmYLdn6RBOFRFt5rUF81uiSSlCo3AnupVFNqnrrd1NEZgO8UXWozPLb:i/QOC0Yhn6ROHWF09cwNPFCnNBxcWCcE

General

File Content Preview:	.ELF.....g..4.....4. ...(....._..._..... .....W...W.....Q.td.....tUPX!.. .....Z.....?d..ELF.....d.....4.,..4. (.....k.-.#.`..... .....?..P.....d..I

Static ELF Info

ELF header

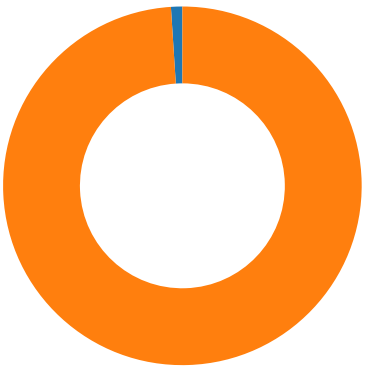
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xc067a0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0xc01000	0xc01000	0x5f9b	0x5f9b	4.5569	0x5	R E	0x1000		
LOAD	0x700	0x8055700	0x8055700	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 98

- 23 (Telnet)
- 1312 undefined

TCP Packets

System Behavior

Analysis Process: RzBo7FFhaM PID: 4567 Parent PID: 4497

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	/tmp/RzBo7FFhaM
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4569 Parent PID: 4567

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

File Activities

File Read

Directory Enumerated

Analysis Process: RzBo7FFhaM PID: 4607 Parent PID: 4569

General

Start time:	11:19:07
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4608 Parent PID: 4569

General

Start time:	11:19:07
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4611 Parent PID: 4608

General

Start time:	11:19:07
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4617 Parent PID: 4611

General

Start time:	11:19:12
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4618 Parent PID: 4611

General

Start time:	11:19:12
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4612 Parent PID: 4608

General

Start time:	11:19:07
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4613 Parent PID: 4608

General

Start time:	11:19:07
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4570 Parent PID: 4567

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4571 Parent PID: 4567

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4572 Parent PID: 4571

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

File Activities

File Read

Directory Enumerated

Analysis Process: RzBo7FFhaM PID: 4609 Parent PID: 4572

General

Start time:	11:19:07
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4610 Parent PID: 4572

General

Start time:	11:19:07

Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4573 Parent PID: 4571

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: RzBo7FFhaM PID: 4574 Parent PID: 4571

General

Start time:	11:17:18
Start date:	22/07/2021
Path:	/tmp/RzBo7FFhaM
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	5f2b063b3423065cc1c6ea63979c6f46

Analysis Process: systemd PID: 4594 Parent PID: 1

General

Start time:	11:17:24
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sshd PID: 4594 Parent PID: 1

General

Start time:	11:17:24
Start date:	22/07/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	791024 bytes
MD5 hash:	661b2a2da3b6c7d7ef41d0b9da1caa3b

File Activities

File Read

File Written

Directory Enumerated