ID: 452447
Sample Name: o3ZUDIEL1v
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:25:16
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

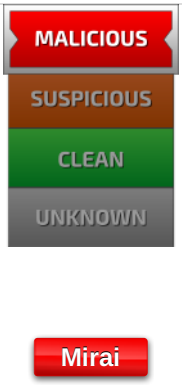
Linux Analysis Report o3ZUDIEL1v

Overview

General Information

Sample Name:	o3ZUDIEL1v
Analysis ID:	452447
MD5:	7694cfd641f9688..
SHA1:	799787af8312d8a.
SHA256:	4609b5c0e2d144..
Tags:	32 elf mirai renesas
Infos:	

Detection

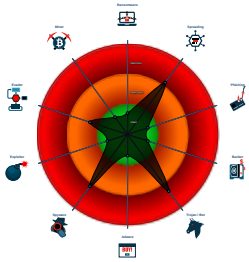


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Opens /sys/class/net/* files useful f…
- Sample tries to kill many processes…
- Uses known network protocols on no…
- Creates hidden files and/or directories
- Detected TCP or UDP traffic on non…
- Enumerates processes within the "p…
- Reads system information from the …
- Sample has stripped symbol table
- Sample listens on a socket

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452447
Start date:	22.07.2021
Start time:	11:25:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	o3ZUDIEL1v
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:	mal76.spre.troj.spyw.lin@0/8@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu1**
- o3ZUDIEL1v (PID: 4576, Parent: 4497, MD5: 7694cfd641f968883d3bf665edb563db) Arguments: /usr/bin/qemu-sh4 /tmp/o3ZUDIEL1v
  - o3ZUDIEL1v New Fork (PID: 4582, Parent: 4576)
    - o3ZUDIEL1v New Fork (PID: 4830, Parent: 4582)
    - o3ZUDIEL1v New Fork (PID: 4831, Parent: 4582)
      - o3ZUDIEL1v New Fork (PID: 4833, Parent: 4831)
        - o3ZUDIEL1v New Fork (PID: 4840, Parent: 4833)
        - o3ZUDIEL1v New Fork (PID: 4841, Parent: 4833)
      - o3ZUDIEL1v New Fork (PID: 4835, Parent: 4831)
      - o3ZUDIEL1v New Fork (PID: 4836, Parent: 4831)
  - o3ZUDIEL1v New Fork (PID: 4583, Parent: 4576)
  - o3ZUDIEL1v New Fork (PID: 4584, Parent: 4576)
    - o3ZUDIEL1v New Fork (PID: 4587, Parent: 4584)
    - o3ZUDIEL1v New Fork (PID: 4588, Parent: 4584)
    - o3ZUDIEL1v New Fork (PID: 4596, Parent: 4584)
- systemd New Fork (PID: 4602, Parent: 1)
- sshd (PID: 4602, Parent: 1, MD5: 661b2a2da3b6c7d7ef41d0b9da1caa3b) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 4614, Parent: 1)
- NetworkManager (PID: 4614, Parent: 1, MD5: 43dcb4efce9c2c522442ae62538bf659) Arguments: /usr/sbin/NetworkManager --no-daemon
- systemd New Fork (PID: 4628, Parent: 1)
- nm-online (PID: 4628, Parent: 1, MD5: ac72f7c256e548d273a5133a245a1638) Arguments: /usr/bin/nm-online -s -q --timeout=30
- systemd New Fork (PID: 4641, Parent: 1)
- nm-dispatcher (PID: 4641, Parent: 1, MD5: 7d4ef829ade49b564256f3f295f9c826) Arguments: /usr/lib/NetworkManager/nm-dispatcher
  - nm-dispatcher New Fork (PID: 4665, Parent: 4641)
  - 01ifupdown (PID: 4665, Parent: 4641, MD5: 299819a8e64f00a1edbdfc99d05a8594) Arguments: /bin/sh -e /etc/NetworkManager/dispatcher.d/01ifupdown none hostname
- systemd New Fork (PID: 4654, Parent: 1)
- systemd-hostnamed (PID: 4654, Parent: 1, MD5: b05764f1a40963131ea2e1cd585f4139) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 4679, Parent: 1)
- snapd (PID: 4679, Parent: 1, MD5: 416402f94a949af355c09e8bccfa0eb0) Arguments: /usr/lib/snapd/snapd
- systemd New Fork (PID: 4698, Parent: 1)
- iscsiadm (PID: 4698, Parent: 1, MD5: b9363fe8099be776e324a481e209d7c4) Arguments: /sbin/iscsiadm -k 0 2
- systemd New Fork (PID: 4722, Parent: 1)
- sshd (PID: 4722, Parent: 1, MD5: 661b2a2da3b6c7d7ef41d0b9da1caa3b) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 4774, Parent: 1)
- systemd-hostnamed (PID: 4774, Parent: 1, MD5: b05764f1a40963131ea2e1cd585f4139) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 4797, Parent: 1)
- snapd (PID: 4797, Parent: 1, MD5: 416402f94a949af355c09e8bccfa0eb0) Arguments: /usr/lib/snapd/snapd
- systemd New Fork (PID: 4818, Parent: 1)
- sshd (PID: 4818, 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
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

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)

Opens /sys/class/net/* files useful for querying network interface information

Uses known network protocols on non-standard ports

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

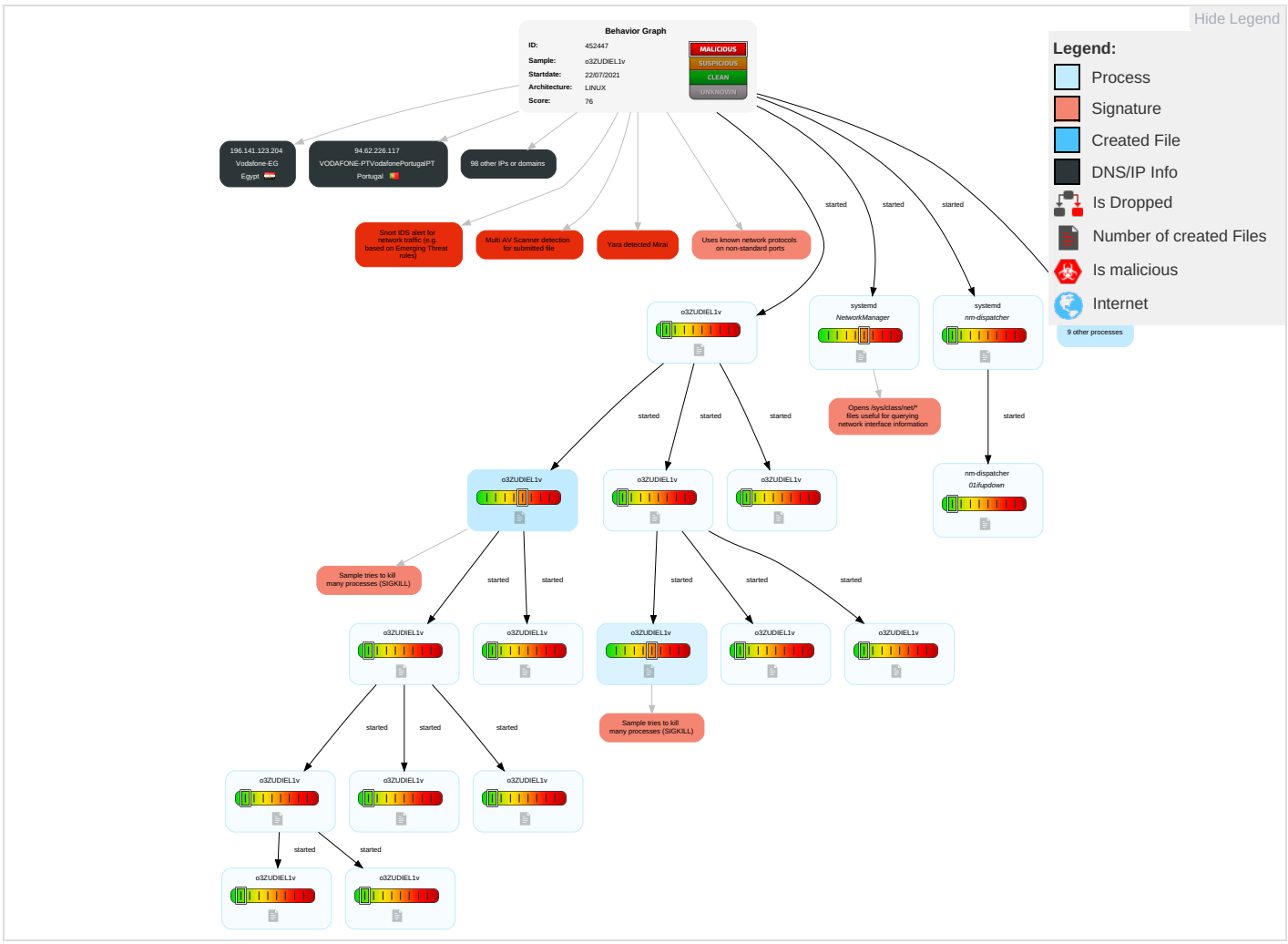
Mitre Att&ck Matrix

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	Hidden Files and Directories 1	OS Credential Dumping 1	Security Software Discovery 1	Remote Services	Network Information Discovery 1	Exfiltration Over Other Network Medium	Non-Standard Port 1 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
o3ZUDIEL1v	51%	Virustotal		Browse
o3ZUDIEL1v	54%	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
94.57.15.174	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
41.176.104.101	unknown	Egypt		36992	ETISALAT-MISREG	false
177.143.85.24	unknown	Brazil		28573	CLAROSABR	false
200.152.186.20	unknown	Brazil		28589	ConvexInternetSolutionsBR	false
17.184.46.217	unknown	United States		714	APPLE-ENGINEERINGUS	false
73.226.46.247	unknown	United States		7922	COMCAST-7922US	false
184.37.225.215	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
98.244.88.33	unknown	United States		7922	COMCAST-7922US	false
154.167.155.34	unknown	Ghana		30986	SCANCOMGH	false
98.8.113.19	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
80.74.154.57	unknown	Switzerland		21069	ASN-METANETRoutingpeeringissuesnocmetanetchCH	false
48.253.161.173	unknown	United States		2686	ATGS-MMD-ASUS	false
253.192.253.242	unknown	Reserved		unknown	unknown	false
135.202.153.120	unknown	United States		14962	NCR-252US	false
99.243.234.87	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
164.184.8.135	unknown	United States		37717	EL-KhawarizmiTN	false
189.218.211.120	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	false
75.175.113.219	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
102.241.10.95	unknown	Tunisia		36926	CKL1-ASNKE	false
13.128.106.59	unknown	United States		7018	ATT-INTERNET4US	false
154.50.188.217	unknown	United States		174	COGENT-174US	false
125.102.176.51	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
37.200.37.141	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
184.135.113.232	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
94.174.138.249	unknown	United Kingdom		5089	NTLGB	false
159.172.75.207	unknown	United States		10223	UECOMM-AUUecommLtdAU	false
45.133.252.62	unknown	Netherlands		39855	MOD-EUNL	false
89.124.213.184	unknown	Ireland		25441	IBIS-ASImagineGroupLtdIE	false
4.221.60.0	unknown	United States		3356	LEVEL3US	false
171.149.128.106	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
119.50.179.73	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
144.22.49.226	unknown	Costa Rica		64102	OracleCorporationCR	false
83.63.147.62	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
38.21.161.59	unknown	United States		11738	BLIP-NETWORKSUS	false
197.90.49.91	unknown	South Africa		10474	OPTINETZA	false
253.144.162.52	unknown	Reserved		unknown	unknown	false
14.237.86.26	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
104.101.138.123	unknown	United States		16625	AKAMAI-ASUS	false
216.127.0.14	unknown	United States		7321	LNET-ASNUS	false
75.20.216.43	unknown	United States		7018	ATT-INTERNET4US	false
108.254.96.50	unknown	United States		7018	ATT-INTERNET4US	false
102.157.169.217	unknown	Tunisia		37705	TOPNETTN	false
107.173.85.99	unknown	United States		36352	AS-COLOCROSSINGUS	false
193.33.248.137	unknown	United Kingdom		25180	EXPONENTIAL-E-ASGB	false
54.140.119.74	unknown	United States		14618	AMAZON-AESUS	false
46.205.212.165	unknown	Poland		12912	TMPL	false
154.246.240.197	unknown	Algeria		36947	ALGTEL-ASDZ	false
155.206.233.9	unknown	United States		6629	NOAA-ASUS	false
95.151.218.73	unknown	United Kingdom		12576	EELtdGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.148.196.246	unknown	South Africa		5713	SAIX-NETZA	false
72.123.230.236	unknown	United States		22394	CELLCOUS	false
102.219.100.135	unknown	unknown		36926	CKL1-ASNKE	false
84.16.48.217	unknown	Slovakia (SLOVAK Republic)		31679	SLOVANET-MICRONEThttpwwwslovanetnetSK	false
124.1.198.151	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
72.144.232.184	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
115.82.160.221	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
84.84.243.132	unknown	Netherlands		1136	KPNKPNNationalEU	false
40.51.41.233	unknown	United States		4249	LILLY-ASUS	false
27.80.36.229	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
168.46.226.225	unknown	United States		1761	TDIR-CAPNETUS	false
12.82.79.93	unknown	United States		7018	ATT-INTERNET4US	false
174.228.87.97	unknown	United States		22394	CELLCOUS	false
142.165.160.6	unknown	Canada		803	SASKTELCA	false
219.39.125.115	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
190.111.28.194	unknown	Guatemala		26617	NavegacomSAGT	false
188.24.244.234	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
24.50.148.206	unknown	United States		46449	ASTREA-NORTHWI-WESTUPMIUS	false
94.62.226.117	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
146.33.108.173	unknown	United States		197938	TRAVIANGAMESDE	false
207.144.162.82	unknown	United States		21830	CSTEL-NETUS	false
187.227.62.239	unknown	Mexico		8151	UninetSAdeCVMX	false
246.144.169.176	unknown	Reserved		unknown	unknown	false
4.56.207.101	unknown	United States		3356	LEVEL3US	false
27.160.126.143	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
99.59.85.151	unknown	United States		7018	ATT-INTERNET4US	false
176.35.23.103	unknown	United Kingdom		5413	AS5413GB	false
8.167.164.251	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
182.234.160.244	unknown	Taiwan; Republic of China (ROC)		9416	MULTIMEDIA-AS-APHoshinMultimediaCenterIncTW	false
162.228.194.252	unknown	United States		7018	ATT-INTERNET4US	false
17.89.149.242	unknown	United States		714	APPLE-ENGINEERINGUS	false
85.146.145.203	unknown	Netherlands		50266	TMOBILE-THUISNL	false
200.205.200.178	unknown	Brazil		10429	TELEFONICABRASILSABR	false
153.127.220.238	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	false
241.79.122.49	unknown	Reserved		unknown	unknown	false
139.159.171.6	unknown	China		58466	CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN	false
147.154.227.167	unknown	United States		31898	ORACLE-BMC-31898US	false
194.230.199.185	unknown	Switzerland		6730	SUNRISECH	false
107.178.242.208	unknown	United States		15169	GOOGLEUS	false
168.35.27.202	unknown	United States		1761	TDIR-CAPNETUS	false
20.156.174.144	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
18.151.13.78	unknown	United States		16509	AMAZON-02US	false
244.205.159.207	unknown	Reserved		unknown	unknown	false
148.115.69.223	unknown	United States		6501	SOUTHERNETUS	false
71.9.59.212	unknown	United States		20115	CHARTER-20115US	false
98.169.101.221	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
57.141.231.87	unknown	Belgium		2686	ATGS-MMD-ASUS	false
197.202.79.100	unknown	Algeria		36947	ALGTEL-ASDZ	false
196.141.123.204	unknown	Egypt		36935	Vodafone-EG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
68.177.52.185	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
57.158.225.148	unknown	Belgium		2686	ATGS-MMD-ASUS	false

Runtime Messages

Command:	/tmp/o3ZUDIEL1v
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
ETISALAT-MISREG	8ZJ0cPowTy	Get hash	malicious	Browse	• 105.85.247.7
	U5q75RGCmQ	Get hash	malicious	Browse	• 102.59.105.224
	BTNNG17tlh	Get hash	malicious	Browse	• 105.80.209.167
	VGi1EK6T17	Get hash	malicious	Browse	• 102.59.105.238
	apep.mips	Get hash	malicious	Browse	• 105.80.110.212
	MD5OxTSc6i	Get hash	malicious	Browse	• 156.177.182.90
	rxfttQnoO5	Get hash	malicious	Browse	• 105.94.59.191
	LDWhPg4vRM	Get hash	malicious	Browse	• 156.163.86.252
	CGjf615z6v	Get hash	malicious	Browse	• 156.191.125.223
	yZEHOt8K7X	Get hash	malicious	Browse	• 156.191.172.97
	tPzL0MlKIo	Get hash	malicious	Browse	• 105.202.102.183
	IYmbrE4LVN	Get hash	malicious	Browse	• 41.65.28.162
	jhUxzb7jPW	Get hash	malicious	Browse	• 156.182.145.40
	7Pvt6Jni6p	Get hash	malicious	Browse	• 41.152.155.12
	BWG6npgduP	Get hash	malicious	Browse	• 156.188.243.149
	sap7ltEdFx	Get hash	malicious	Browse	• 105.81.245.93
	Ebl8uJRI5t	Get hash	malicious	Browse	• 156.186.86.115
	Vk3A1yJJMg	Get hash	malicious	Browse	• 197.194.23.189
	Vs7Vm7J1TR	Get hash	malicious	Browse	• 197.123.112.57
	395d6gwkWK	Get hash	malicious	Browse	• 105.205.88.238
EMIRATES-INTERNETEmiratesInternetAE	BTNNG17tlh	Get hash	malicious	Browse	• 31.219.129.233
	bPAMfuy9oa	Get hash	malicious	Browse	• 92.97.244.105
	Xr3hmBQcmw	Get hash	malicious	Browse	• 92.99.112.227
	SUpODCSauS	Get hash	malicious	Browse	• 86.99.220.36
	rxfttQnoO5	Get hash	malicious	Browse	• 5.194.181.32
	tPzL0MlKIo	Get hash	malicious	Browse	• 31.215.73.173
	sap7ltEdFx	Get hash	malicious	Browse	• 94.58.153.97
	471u0A1FPw	Get hash	malicious	Browse	• 31.219.188.62
	F1rGU2xEPh	Get hash	malicious	Browse	• 94.57.15.131
	eubqHHIQkc	Get hash	malicious	Browse	• 31.219.129.252

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ebex99Bzzw	Get hash	malicious	Browse	• 5.194.156.30
	popsmoke.mpsl	Get hash	malicious	Browse	• 31.218.10.52
	PX7gd73hY6	Get hash	malicious	Browse	• 185.78.244.190
	Rb5g620Inp	Get hash	malicious	Browse	• 92.97.244.139
	i	Get hash	malicious	Browse	• 86.99.194.78
	5NUdvEW0gj.exe	Get hash	malicious	Browse	• 217.165.81.72
	i	Get hash	malicious	Browse	• 94.57.129.29
	HU4TEm4Vr7.exe	Get hash	malicious	Browse	• 83.110.95.159
	i795zXB64c.exe	Get hash	malicious	Browse	• 86.98.122.34
	svchost.exe	Get hash	malicious	Browse	• 94.58.241.206

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/4602/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.

/proc/4722/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.

/proc/4818/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778

/proc/4818/oom_score_adj	
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:lv:lv
MD5:	600AFFBB4A2E9025B7D50F6E1814B400
SHA1:	2DE94308B4453700D378CB9EF5BC75D22949188E
SHA-256:	C0B67778CE4256AEAC48B6D9CEE4A690221DA0A6A54FE04C5205577A5E655662
SHA-512:	EAA7DEE03F55E0D28B3F86C7DE5F38D0F263B62C1211D2401DEED0BFA6C481C0925EE63EFF33EC081F8D9ECEAE3ED158BFA44966A23680D063891C6C97FD1AD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	4818.

/var/cache/snapd/sections.NnpFpn7dlFf6	
Process:	/usr/lib/snapd/snapd
File Type:	ASCII text
Category:	dropped
Size (bytes):	257
Entropy (8bit):	4.149772078213831
Encrypted:	false
SSDEEP:	6:+JwAuG+uP2J5I9W6IzvS5/GAEwKnK/JBMlvuNjpeWPnXMISz:J02Jt6W8ce+Oj8WX6
MD5:	966FD91045792732666DBA4D113B0D48
SHA1:	9DCADCCCE036C48AEADCA9632A6E8EBADC69EE18
SHA-256:	244EB764054FECCD5D77FAD9273ECC7C1B427551FA153876C889C59D1959630D
SHA-512:	DEB94A2508E4B8A26073FC1F71E71EB19D877C890BFB93FBE4E700643FA82FF78135A146AB47EC702D6FB6D4A2FDDF5257BBF5B5E6992CAB81A15CA9B43D36BA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	art-and-design.books-and-reference.development.devices-and-iot.education.entertainment.featured.finance.games.health-and-fitness.music-and-audio.news-and-weather.personalisation.photo-and-video.productivity.science.security.server-and-cloud.social.utilities

/var/cache/snapd/sections.vrLtrN1cvTrW	
Process:	/usr/lib/snapd/snapd
File Type:	ASCII text
Category:	dropped
Size (bytes):	257
Entropy (8bit):	4.149772078213831
Encrypted:	false
SSDEEP:	6:+JwAuG+uP2J5I9W6IzvS5/GAEwKnK/JBMlvuNjpeWPnXMISz:J02Jt6W8ce+Oj8WX6
MD5:	966FD91045792732666DBA4D113B0D48
SHA1:	9DCADCCCE036C48AEADCA9632A6E8EBADC69EE18
SHA-256:	244EB764054FECCD5D77FAD9273ECC7C1B427551FA153876C889C59D1959630D
SHA-512:	DEB94A2508E4B8A26073FC1F71E71EB19D877C890BFB93FBE4E700643FA82FF78135A146AB47EC702D6FB6D4A2FDDF5257BBF5B5E6992CAB81A15CA9B43D36BA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	art-and-design.books-and-reference.development.devices-and-iot.education.entertainment.featured.finance.games.health-and-fitness.music-and-audio.news-and-weather.personalisation.photo-and-video.productivity.science.security.server-and-cloud.social.utilities

Static File Info

General

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.767156628398588
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	o3ZUDIEL1v
File size:	51584
MD5:	7694cfd641f968883d3bf665edb563db
SHA1:	799787af8312d8ab137f796ce37f209bdb5797bd
SHA256:	4609b5c0e2d1442f05c576bb0097e55344de9357643019d74bce4d3d9ed49a4c
SHA512:	a177ac584adedd6031526c42d74f1f2a46894fce8583da373cd6465a919ba614e140a40e41191619b0b0881a1a9e5d47866fb4d1c452411b8c9d7aa5ff0f9756
SSDEEP:	768:jaixFwtLSYAagMo0ebH4/ZvQX3hyWfs3INgCJUU/qMCqKomQRCvs:jaQFwtOGBvQXxfs3kgCJt/qMF/RCvs
File Content Preview:	.ELF.....*.....@.4.....4. ...(.....@...@.<...<.....@...@.A.@.A.p.....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:	51184
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	0xbf40	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40c020	0xc020	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40c044	0xc044	0x5f8	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41c640	0xc640	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41c648	0xc648	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41c654	0xc654	0x15c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41c7b0	0xc7b0	0x280	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xc7b0	0x3e	0x0	0x0		0	0	1

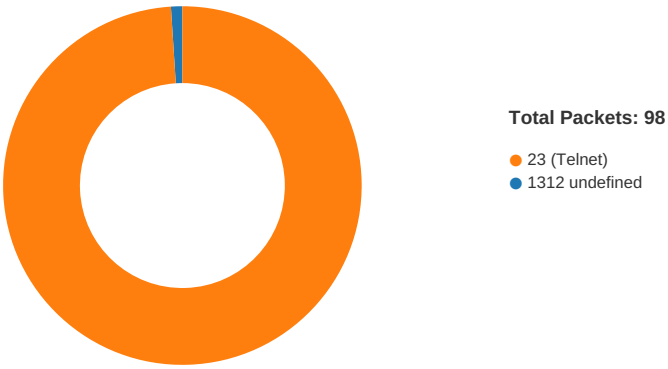
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0xc63c	0xc63c	4.6304	0x5	R E	0x10000		.init .text .fini .rodata

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0xc640	0x41c640	0x41c640	0x170	0x3f0	0.4302	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: o3ZUDIEL1v PID: 4576 Parent PID: 4497

General

Start time:	11:25:48
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	/usr/bin/qemu-sh4 /tmp/o3ZUDIEL1v
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

File Activities

File Read

Analysis Process: o3ZUDIEL1v PID: 4582 Parent PID: 4576

General

Start time:	11:25:49
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes

MD5 hash:	7694cfd641f968883d3bf665edb563db

File Activities

File Read

Directory Enumerated

Analysis Process: o3ZUDIEL1v PID: 4830 Parent PID: 4582

General

Start time:	11:27:53
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4831 Parent PID: 4582

General

Start time:	11:27:53
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4833 Parent PID: 4831

General

Start time:	11:27:53
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4840 Parent PID: 4833

General

Start time:	11:27:58
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4841 Parent PID: 4833

General

Start time:	11:27:58
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4835 Parent PID: 4831

General

Start time:	11:27:53
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4836 Parent PID: 4831

General

Start time:	11:27:53
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4583 Parent PID: 4576

General

Start time:	11:25:49
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4584 Parent PID: 4576

General

Start time:	11:25:49
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4587 Parent PID: 4584

General

Start time:	11:25:49
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

File Activities

File Read

Directory Enumerated

Analysis Process: o3ZUDIEL1v PID: 4588 Parent PID: 4584

General

Start time:	11:25:49
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: o3ZUDIEL1v PID: 4596 Parent PID: 4584

General

Start time:	11:25:49
Start date:	22/07/2021
Path:	/tmp/o3ZUDIEL1v
Arguments:	n/a
File size:	51584 bytes
MD5 hash:	7694cfd641f968883d3bf665edb563db

Analysis Process: systemd PID: 4602 Parent PID: 1

General

Start time:	11:25:55
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sshd PID: 4602 Parent PID: 1

General

Start time:	11:25:55
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

Analysis Process: systemd PID: 4614 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: NetworkManager PID: 4614 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/usr/sbin/NetworkManager
Arguments:	/usr/sbin/NetworkManager --no-daemon
File size:	2953816 bytes
MD5 hash:	43dcb4efce9c2c522442ae62538bf659

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 4628 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: nm-online PID: 4628 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/usr/bin/nm-online
Arguments:	/usr/bin/nm-online -s -q --timeout=30
File size:	14792 bytes
MD5 hash:	ac72f7c256e548d273a5133a245a1638

File Activities

File Read

Analysis Process: systemd PID: 4641 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: nm-dispatcher PID: 4641 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/usr/lib/NetworkManager/nm-dispatcher
Arguments:	/usr/lib/NetworkManager/nm-dispatcher
File size:	48656 bytes
MD5 hash:	7d4ef829ade49b564256f3f295f9c826

File Activities

File Read

Directory Enumerated

Analysis Process: nm-dispatcher PID: 4665 Parent PID: 4641

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/usr/lib/NetworkManager/nm-dispatcher
Arguments:	n/a
File size:	48656 bytes
MD5 hash:	7d4ef829ade49b564256f3f295f9c826

File Activities

Directory Enumerated

Analysis Process: 01ifupdown PID: 4665 Parent PID: 4641

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/etc/NetworkManager/dispatcher.d/01ifupdown
Arguments:	/bin/sh -e /etc/NetworkManager/dispatcher.d/01ifupdown none hostname
File size:	2146 bytes
MD5 hash:	299819a8e64f00a1edbdfc99d05a8594

File Activities

File Read

Analysis Process: systemd PID: 4654 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: systemd-hostnamed PID: 4654 Parent PID: 1

General

Start time:	11:26:18
Start date:	22/07/2021
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	339152 bytes
MD5 hash:	b05764f1a40963131ea2e1cd585f4139

File Activities

File Read

Analysis Process: systemd PID: 4679 Parent PID: 1

General

Start time:	11:26:21
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: snapd PID: 4679 Parent PID: 1

General

Start time:	11:26:21
Start date:	22/07/2021
Path:	/usr/lib/snapd/snapd
Arguments:	/usr/lib/snapd/snapd
File size:	21178072 bytes
MD5 hash:	416402f94a949af355c09e8bccfa0eb0

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Analysis Process: systemd PID: 4698 Parent PID: 1

General

Start time:	11:26:32
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: iscsiadm PID: 4698 Parent PID: 1

General

Start time:	11:26:32
Start date:	22/07/2021
Path:	/sbin/iscsiadm
Arguments:	/sbin/iscsiadm -k 0 2
File size:	754952 bytes
MD5 hash:	b9363fe8099be776e324a481e209d7c4

File Activities

File Read

Analysis Process: systemd PID: 4722 Parent PID: 1

General

Start time:	11:27:36

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

Analysis Process: sshd PID: 4722 Parent PID: 1

General

Start time:	11:27:36
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

Analysis Process: systemd PID: 4774 Parent PID: 1

General

Start time:	11:27:37
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: systemd-hostnamed PID: 4774 Parent PID: 1

General

Start time:	11:27:37
Start date:	22/07/2021
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	339152 bytes
MD5 hash:	b05764f1a40963131ea2e1cd585f4139

File Activities

File Read

Analysis Process: systemd PID: 4797 Parent PID: 1

General

Start time:	11:27:38
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: snapd PID: 4797 Parent PID: 1

General

Start time:	11:27:38
Start date:	22/07/2021
Path:	/usr/lib/snapd/snapd
Arguments:	/usr/lib/snapd/snapd
File size:	21178072 bytes
MD5 hash:	416402f94a949af355c09e8bccfa0eb0

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Analysis Process: systemd PID: 4818 Parent PID: 1

General

Start time:	11:27:39
Start date:	22/07/2021
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sshd PID: 4818 Parent PID: 1

General

Start time:	11:27:39
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