ID: 519630
Sample Name: gL6zNW1uNj
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:51:08
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

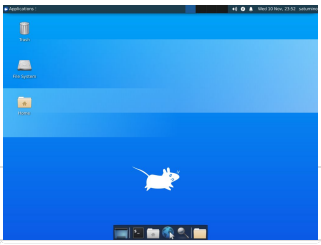
Linux Analysis Report gL6zNW1uNj

Overview

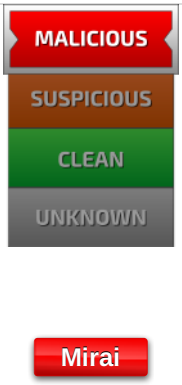
General Information

Sample Name:	gL6zNW1uNj
Analysis ID:	519630
MD5:	deee0487e17b20..
SHA1:	865c8c7d1b4d72..
SHA256:	9ad0477757b6e3..
Tags:	32 elf mirai sparc
Infos:	

Most interesting Screenshot:



Detection

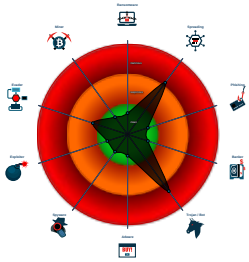


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill many processes...
- 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
- 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:	519630
Start date:	10.11.2021
Start time:	23:51:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gL6zNW1uNj
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:	mal72.spre.troj.lin@0/4@0/0
Warnings:	Show All

Process Tree

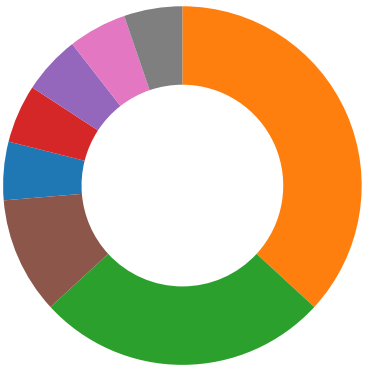
- **system is lnxubuntu20**
- gL6zNW1uNj (PID: 5239, Parent: 5117, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/gL6zNW1uNj
  - gL6zNW1uNj New Fork (PID: 5241, Parent: 5239)
    - gL6zNW1uNj New Fork (PID: 5271, Parent: 5241)
    - gL6zNW1uNj New Fork (PID: 5273, Parent: 5241)
      - gL6zNW1uNj New Fork (PID: 5275, Parent: 5273)
        - gL6zNW1uNj New Fork (PID: 5278, Parent: 5275)
        - gL6zNW1uNj New Fork (PID: 5281, Parent: 5275)
      - gL6zNW1uNj New Fork (PID: 5277, Parent: 5273)
      - gL6zNW1uNj New Fork (PID: 5280, Parent: 5273)
  - gL6zNW1uNj New Fork (PID: 5242, Parent: 5239)
  - gL6zNW1uNj New Fork (PID: 5244, Parent: 5239)
    - gL6zNW1uNj New Fork (PID: 5247, Parent: 5244)
      - gL6zNW1uNj New Fork (PID: 5298, Parent: 5247)
      - gL6zNW1uNj New Fork (PID: 5299, Parent: 5247)
    - gL6zNW1uNj New Fork (PID: 5248, Parent: 5244)
    - gL6zNW1uNj New Fork (PID: 5250, Parent: 5244)
- systemd New Fork (PID: 5270, Parent: 1)
- sshd (PID: 5270, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5286, Parent: 1)
- sshd (PID: 5286, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5297, Parent: 1)
- sshd (PID: 5297, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5304, Parent: 1)
- sshd (PID: 5304, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

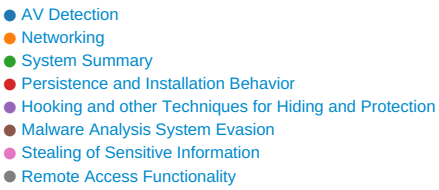
PCAP (Network Traffic)

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

Jbx Signature Overview



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:

Sample tries to kill many processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

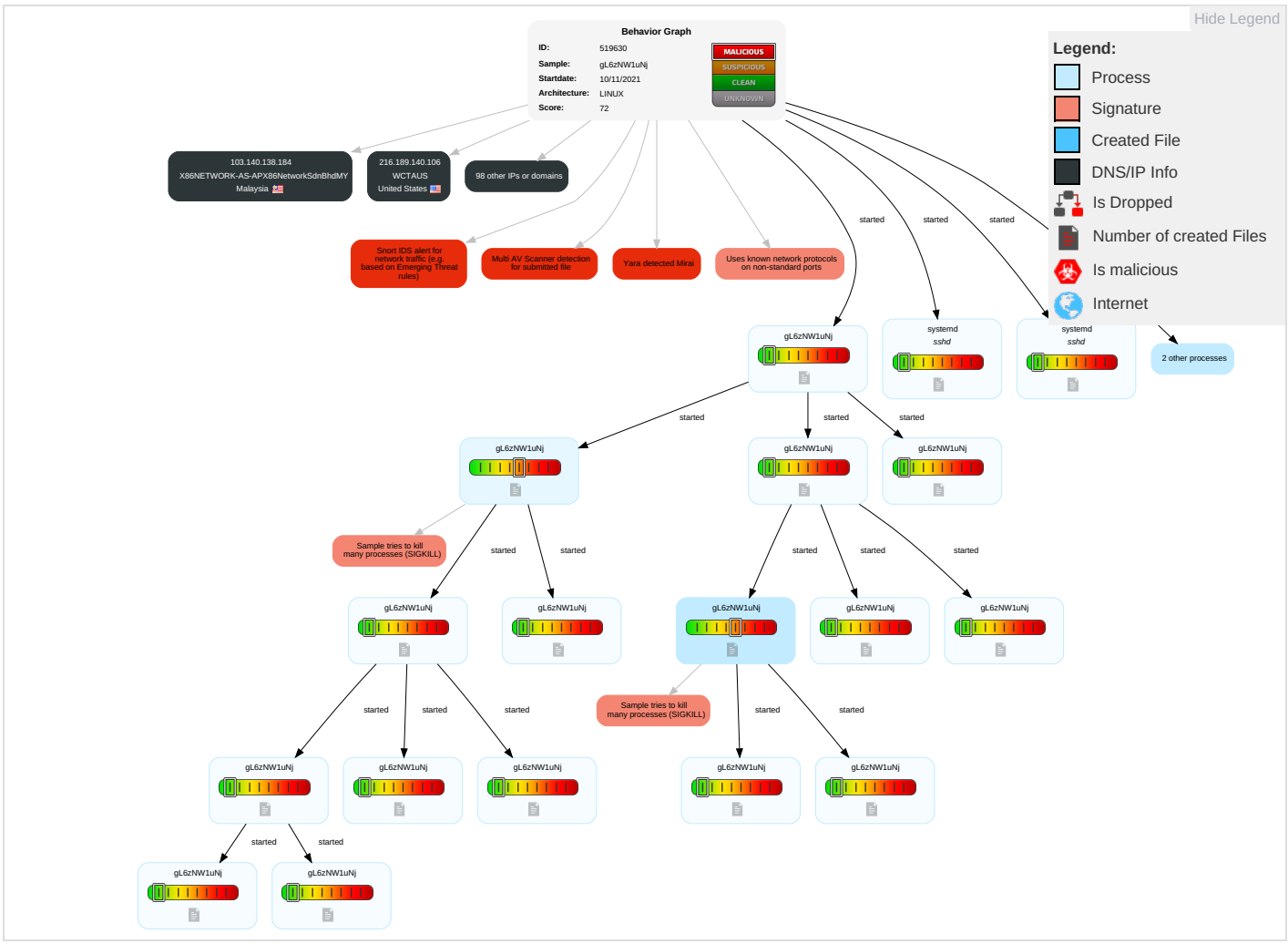
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

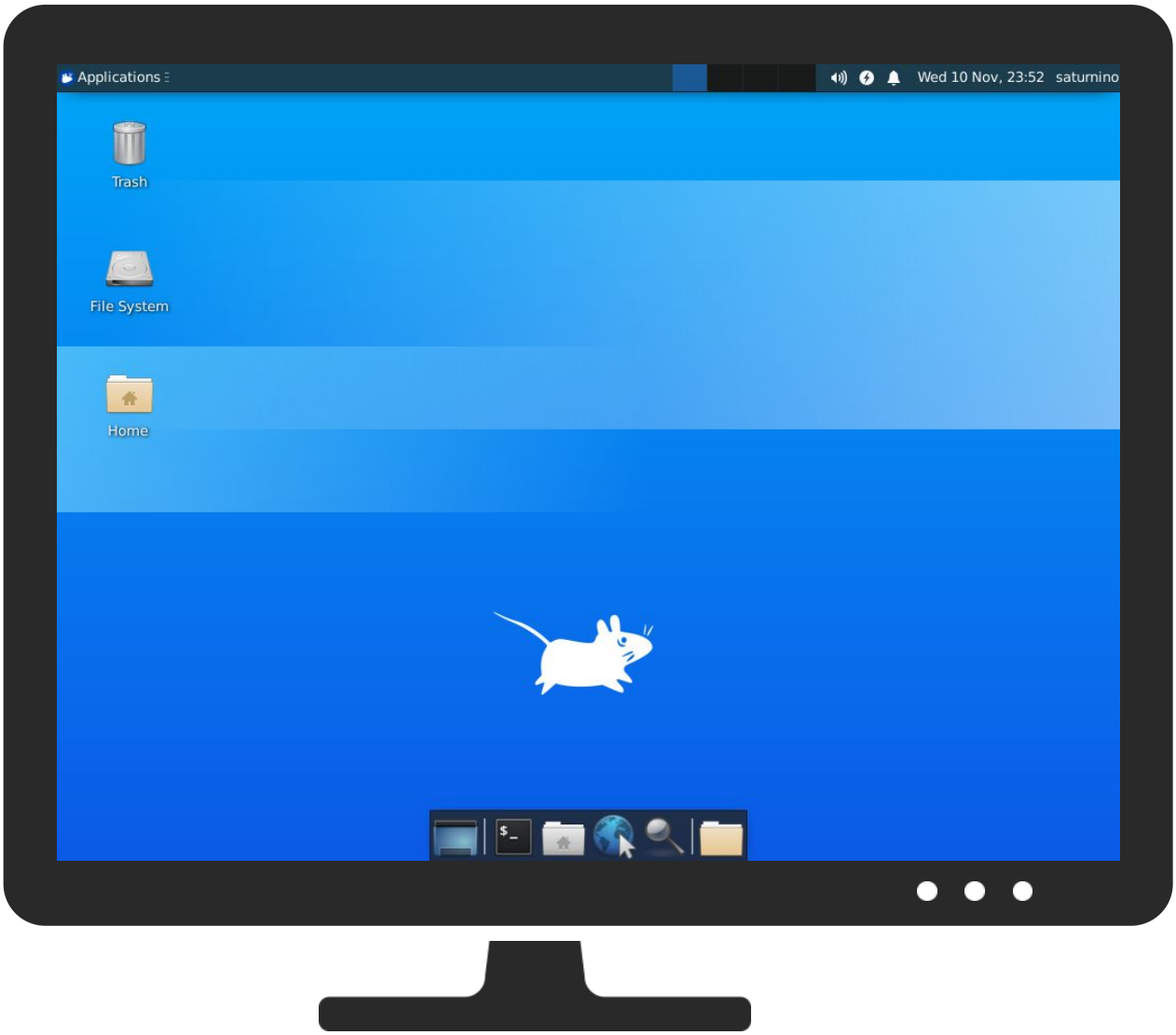
Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
gL6zNW1uNj	49%	Virustotal		Browse
gL6zNW1uNj	56%	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
197.153.61.25	unknown	Morocco		36925	ASMediMA	false
151.86.44.187	unknown	Italy		8217	ASN-ENIIT	false
107.18.149.250	unknown	United States		14654	WAYPORTUS	false
243.122.7.203	unknown	Reserved		unknown	unknown	false
83.81.157.142	unknown	Netherlands		33915	TNF-ASNL	false
170.201.71.125	unknown	United States		10995	PNCBANKUS	false
160.242.103.111	unknown	Namibia		33763	Paratus-TelecomNA	false
152.88.139.42	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
88.73.217.49	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
191.85.197.196	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
195.161.24.251	unknown	Russian Federation		8342	RTCOMM-ASRU	false
34.154.113.0	unknown	United States		2686	ATGS-MMD-ASUS	false
27.104.108.182	unknown	Singapore		4773	MOBILEONELTD-AS-APMobileOneLtdMobileInternetServicePr	false
204.189.141.189	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
85.248.170.96	unknown	Slovakia (SLOVAK Republic)		5578	AS-BENESTRABratislavaSlovakRepublicSK	false
81.43.97.163	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
9.99.10.49	unknown	United States		3356	LEVEL3US	false
193.18.64.58	unknown	Germany		41099	GLOBALREACHGB	false
78.143.58.128	unknown	Germany		34309	LINK11Link11GmbHDE	false
159.142.240.78	unknown	United States		2714	GSA-GOVUS	false
83.195.47.1	unknown	France		3215	FranceTelecom-OrangeFR	false
100.39.34.187	unknown	United States		5650	FRONTIER-FRTRUS	false
35.155.144.153	unknown	United States		16509	AMAZON-02US	false
89.82.103.245	unknown	France		5410	BOUYGTEL-ISPFR	false
206.156.198.155	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
63.15.73.8	unknown	United States		701	UUNETUS	false
102.248.204.116	unknown	South Africa		5713	SAIX-NETZA	false
247.105.76.221	unknown	Reserved		unknown	unknown	false
248.44.16.163	unknown	Reserved		unknown	unknown	false
135.205.234.119	unknown	United States		6431	ATT-RESEARCHUS	false
87.1.84.37	unknown	Italy		3269	ASN-IBSNAZIT	false
241.35.160.0	unknown	Reserved		unknown	unknown	false
246.89.40.146	unknown	Reserved		unknown	unknown	false
168.82.87.233	unknown	United States		8103	STATE-OF-FLAUS	false
65.33.229.36	unknown	United States		33363	BHN-33363US	false
5.247.253.74	unknown	Saudi Arabia		34400	ASN-ETTIHADETISALATSA	false
157.138.8.249	unknown	Italy		137	ASGARRConsortiumGARREU	false
216.202.137.20	unknown	United States		3356	LEVEL3US	false
80.248.16.53	unknown	Iceland		29689	ORIGO-ASIS	false
24.93.166.148	unknown	United States		10796	TWC-10796-MIDWESTUS	false
18.160.223.44	unknown	United States		3	MIT-GATEWAYSUS	false
157.222.204.52	unknown	United States		4704	SANNETRakutenMobileIncJP	false
213.60.172.111	unknown	Spain		12334	Galicia-SpainES	false
75.223.213.59	unknown	United States		22394	CELLCOUS	false
111.243.11.20	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
162.239.12.7	unknown	United States		7018	ATT-INTERNET4US	false
14.185.213.79	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
211.200.115.186	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
177.244.147.186	unknown	Mexico		13999	MegaCableSAdeCVMX	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.81.96.181	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
114.159.61.103	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
169.156.132.11	unknown	United States		6189	EPFL-ASUS	false
110.26.118.12	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
216.189.140.106	unknown	United States		21902	WCTAUS	false
122.109.133.175	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
179.161.68.206	unknown	Brazil		26599	TELEFONICABRASILSABR	false
95.39.201.172	unknown	Spain		12357	COMUNITELSPAINES	false
221.190.17.112	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
142.14.127.103	unknown	Canada		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
241.207.254.214	unknown	Reserved		unknown	unknown	false
169.86.62.36	unknown	United States		37611	AfrihostZA	false
207.123.43.254	unknown	United States		3356	LEVEL3US	false
122.224.85.220	unknown	China		58461	CT-HANGZHOU-IDCNo288Fu-chunRoadCN	false
193.146.135.162	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
244.39.205.7	unknown	Reserved		unknown	unknown	false
18.40.249.230	unknown	United States		3	MIT-GATEWAYSUS	false
202.93.232.234	unknown	Indonesia		38758	HYPERNET-AS-IDPTHIPERNETINDODATAID	false
155.199.164.179	unknown	United States		786	JANETJiscServicesLimitedGB	false
220.195.123.67	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
119.159.35.25	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
101.208.151.88	unknown	India		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
91.18.128.136	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
194.52.199.122	unknown	Sweden		31529	DENIC-ANYCAST-ASDNSanycastASobjectforDEDNSservice	false
23.50.220.217	unknown	United States		16625	AKAMAI-ASUS	false
98.146.118.80	unknown	United States		10838	OCEANIC-INTERNET-RRUS	false
203.168.187.234	unknown	Hong Kong		9908	HKCABLE2-HK-APHKCableTVLtdHK	false
176.212.43.225	unknown	Russian Federation		57378	ROSTOV-ASRU	false
48.38.254.123	unknown	United States		2686	ATGS-MMD-ASUS	false
53.176.103.106	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
152.223.201.108	unknown	United States		30313	IRSUS	false
102.55.170.247	unknown	Morocco		6713	IAM-ASMA	false
114.123.47.5	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
61.55.8.196	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
251.25.189.68	unknown	Reserved		unknown	unknown	false
14.120.104.110	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
68.147.7.93	unknown	Canada		6327	SHAWCA	false
97.20.172.125	unknown	United States		22394	CELLCOUS	false
41.152.76.227	unknown	Egypt		36992	ETISALAT-MISREG	false
48.131.158.196	unknown	United States		2686	ATGS-MMD-ASUS	false
106.26.169.88	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
130.252.51.239	unknown	United States		14365	ADOBE-NETUS	false
155.54.253.41	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
8.2.139.206	unknown	United States		3356	LEVEL3US	false
75.235.78.135	unknown	United States		22394	CELLCOUS	false
36.131.159.191	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
100.49.35.79	unknown	United States		701	UUNETUS	false
166.14.24.193	unknown	Switzerland		11798	ACEDATACENTERS-AS-1US	false
246.125.194.19	unknown	Reserved		unknown	unknown	false
223.218.222.111	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
103.140.138.184	unknown	Malaysia		133936	X86NETWORK-AS-APX86NetworkSdnBhdMY	false

Runtime Messages

Command:	/tmp/gL6zNW1uNj
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
ASN-ENIIT	HwcNrhNfZg	Get hash	malicious	Browse	• 151.98.27.212
	sora.arm	Get hash	malicious	Browse	• 151.96.119.3
	WhFNix8BoE	Get hash	malicious	Browse	• 151.98.75.125
	xd.x86	Get hash	malicious	Browse	• 151.96.214.151
	re2.arm7	Get hash	malicious	Browse	• 151.98.75.126
	QcXQmNSaSp	Get hash	malicious	Browse	• 151.98.27.220
	Darknet.x86	Get hash	malicious	Browse	• 151.98.75.124
	sora.arm	Get hash	malicious	Browse	• 151.86.219.27
	j1zDAEIWib	Get hash	malicious	Browse	• 151.98.75.136
	c0k7KpL89r	Get hash	malicious	Browse	• 151.96.108.147
ASMediMA	3ObdCtruss	Get hash	malicious	Browse	• 102.103.39.117
	DVHEnaPp2d	Get hash	malicious	Browse	• 105.188.238.148
	x86	Get hash	malicious	Browse	• 196.127.145.158
	fZ9Y8XVXDH	Get hash	malicious	Browse	• 45.219.30.154
	SQFoFeC1jQ	Get hash	malicious	Browse	• 197.153.85.54
	xd.x86	Get hash	malicious	Browse	• 41.93.16.194
	sora.mpsl	Get hash	malicious	Browse	• 41.87.150.68
	MePwVTNRoA	Get hash	malicious	Browse	• 45.219.30.100
	eFsSvDKams	Get hash	malicious	Browse	• 41.92.37.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Hilix.arm7	Get hash	malicious	Browse	• 45.219.30.118
	Hilix.x86	Get hash	malicious	Browse	• 45.219.30.106
	aTQ4RalkUs	Get hash	malicious	Browse	• 41.214.134.111
	8PRjJeUifB	Get hash	malicious	Browse	• 45.216.221.197
	t7WU0JjLAR	Get hash	malicious	Browse	• 41.92.113.34
	FGVOkw9did	Get hash	malicious	Browse	• 197.247.118.67
	arm7-20211101-1513	Get hash	malicious	Browse	• 196.126.207.163
	mxHkqAIYT0	Get hash	malicious	Browse	• 41.87.150.73
	Antisocial.x86	Get hash	malicious	Browse	• 45.219.30.151
	w66OTKGVFv	Get hash	malicious	Browse	• 45.219.30.100
	ydZLm6GD56	Get hash	malicious	Browse	• 45.219.30.146
WAYPORTUS	8fVDxGRR8S	Get hash	malicious	Browse	• 216.12.242.81
	P8NtIPe7f0	Get hash	malicious	Browse	• 206.59.196.119
	3AlyfRnHRd	Get hash	malicious	Browse	• 100.47.222.235
	YYcy9gLbBC	Get hash	malicious	Browse	• 107.19.227.149
	rMwxCtXmuJ	Get hash	malicious	Browse	• 107.25.250.38
	b3astmode.arm	Get hash	malicious	Browse	• 107.18.150.164
	6A9RyJXCd7	Get hash	malicious	Browse	• 100.46.121.11
	1Y2rsDBP9s	Get hash	malicious	Browse	• 107.28.67.253
	lYmYPlzghQ	Get hash	malicious	Browse	• 107.28.67.222
	gbk4XWulUo	Get hash	malicious	Browse	• 184.49.234.70
	INsMwWSMeh	Get hash	malicious	Browse	• 184.49.234.47
	WnhlYWJ5C5	Get hash	malicious	Browse	• 107.18.150.166
	1S80No4PTV	Get hash	malicious	Browse	• 107.28.20.236
	apep.x86	Get hash	malicious	Browse	• 107.18.224.74
	6NzbU4oW61	Get hash	malicious	Browse	• 107.18.200.92
	sora.arm	Get hash	malicious	Browse	• 107.18.39.9
	wL8CswnbUJ	Get hash	malicious	Browse	• 107.25.249.96
	JWCIQ6dmiX	Get hash	malicious	Browse	• 107.16.234.110
	DT5DNY63Rp	Get hash	malicious	Browse	• 107.18.102.202
	eUjl39mhBT	Get hash	malicious	Browse	• 107.25.121.193

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5286/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:	high, very likely benign file
Preview:	-1000.

/proc/5304/oom_score_adj	
Process:	/usr/sbin/sshd

/proc/5304/oom_score_adj	
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:	high, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:DVRv:JRv
MD5:	C20A7ECD1C53AD9522EEDDA05994E0FF
SHA1:	4C58A470A925D0778306B17AF553D80D949DD3DD
SHA-256:	4FA6BD7EB31F8EFFFE3EFAE78A995D530EB82462034F575AAF8163F46920EA78
SHA-512:	AC700633B219F0FC8BAADF5CA1B007794B7B2264ACC514CF4C55CE470993EC7B851D464D04A90302B91DAEB505FEE0F6E14669F2DB36B2DD7770FC4C42727C1
Malicious:	false
Reputation:	low
Preview:	5304.

Static File Info

General

File type:	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.035636042849447
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	gL6zNW1uNj
File size:	60412
MD5:	deee0487e17b20a74a1757f36e92a240
SHA1:	865c8c7d1b4d725220d58075839e1429820e3465
SHA256:	9ad0477757b6e3b5808cb2ef7b0a53c58823ab63339d8575f454341446bf2b14
SHA512:	94ea25eb83484a1f32249847cedff76bb149cf4f7b7d36f60b70ca057bf57407b381be6826734fba85cd4313a2b46f5fce4baae1373c174f2df99ff83c810c4d
SSDEEP:	768:eLobAxU6q9Hfymp0xginuYvCkLB6WsTwlC1DQdszoDaS0O+DCDp:eL0AxvSHfymp0xgunvCkV6vTMDaue
File Content Preview:	.ELF.....4...l....4. ...(.....x.....dt.Q.....@..(....@.8R.....#.....b0..`.....!..... ...@....."........`.....$ ... ...@.. .....`....

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc

ELF header

Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	60012
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

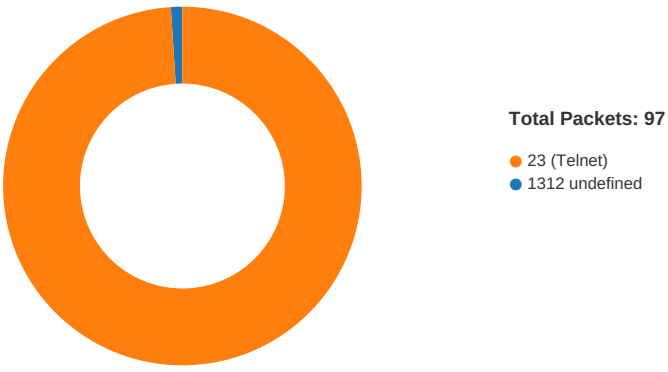
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0xe180	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1e230	0xe230	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e248	0xe248	0x668	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x2e8b4	0xe8b4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2e8bc	0xe8bc	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x2e8c8	0xe8c8	0x164	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x2ea30	0xea2c	0x288	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0xea2c	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	0x10000	0x10000	0xe8b0	0xe8b0	3.3884	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xe8b4	0x2e8b4	0x2e8b4	0x178	0x404	0.3183	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: gL6zNW1uNj PID: 5239 Parent PID: 5117

General

Start time:	23:51:50
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	/tmp/gL6zNW1uNj
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: gL6zNW1uNj PID: 5241 Parent PID: 5239

General

Start time:	23:51:50
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: gL6zNW1uNj PID: 5271 Parent PID: 5241

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5273 Parent PID: 5241

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a

File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5275 Parent PID: 5273

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5278 Parent PID: 5275

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5281 Parent PID: 5275

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5277 Parent PID: 5273

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5280 Parent PID: 5273

General

Start time:	23:51:59
Start date:	10/11/2021

Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5242 Parent PID: 5239

General

Start time:	23:51:50
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5244 Parent PID: 5239

General

Start time:	23:51:50
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5247 Parent PID: 5244

General

Start time:	23:51:50
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: gL6zNW1uNj PID: 5298 Parent PID: 5247

General

Start time:	23:52:04
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5299 Parent PID: 5247

General

Start time:	23:52:04
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5248 Parent PID: 5244

General

Start time:	23:51:50
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: gL6zNW1uNj PID: 5250 Parent PID: 5244

General

Start time:	23:51:51
Start date:	10/11/2021
Path:	/tmp/gL6zNW1uNj
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: systemd PID: 5270 Parent PID: 1

General

Start time:	23:51:58
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5270 Parent PID: 1

General

Start time:	23:51:58
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5286 Parent PID: 1

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5286 Parent PID: 1

General

Start time:	23:51:59
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5297 Parent PID: 1

General

Start time:	23:52:04
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5297 Parent PID: 1

General

Start time:	23:52:04
Start date:	10/11/2021

Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5304 Parent PID: 1

General

Start time:	23:52:05
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5304 Parent PID: 1

General

Start time:	23:52:05
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated