ID: 537271
Sample Name: SedZv73LJb
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:04:18
Date: 09/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report SedZv73LJb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Process Tree 4
Yara Overview 5
Initial Sample 5
PCAP (Network Traffic) 5
Memory Dumps 5
Jbx Signature Overview 6
Networking: 6
System Summary: 6
Data Obfuscation: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Malware Configuration 7
Behavior Graph 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Runtime Messages 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
Static ELF Info 12
ELF header 12
Program Segments 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
System Behavior 13
Analysis Process: SedZv73LJb PID: 5216 Parent PID: 5108 13
General 13
File Activities 14
File Read 14
Analysis Process: SedZv73LJb PID: 5218 Parent PID: 5216 14
General 14
File Activities 14
File Read 14
Directory Enumerated 14
Analysis Process: SedZv73LJb PID: 5220 Parent PID: 5216 14
General 14
Analysis Process: SedZv73LJb PID: 5221 Parent PID: 5216 14
General 14
Analysis Process: SedZv73LJb PID: 5224 Parent PID: 5221 14
General 14
File Activities 15
File Read 15
Directory Enumerated 15
Analysis Process: SedZv73LJb PID: 5226 Parent PID: 5221 15
General 15
Analysis Process: SedZv73LJb PID: 5229 Parent PID: 5221 15
General 15
Analysis Process: systemd PID: 5249 Parent PID: 1 15
General 15
Analysis Process: sshd PID: 5249 Parent PID: 1 15
General 15
File Activities 15

File Read 15
Directory Enumerated 16
Analysis Process: systemd PID: 5250 Parent PID: 1 16
General 16
Analysis Process: sshd PID: 5250 Parent PID: 1 16
General 16
File Activities 16
File Read 16
File Written 16
Directory Enumerated 16
Analysis Process: dash PID: 5258 Parent PID: 4331 16
General 16
Analysis Process: rm PID: 5258 Parent PID: 4331 16
General 16
File Activities 17
File Deleted 17
File Read 17

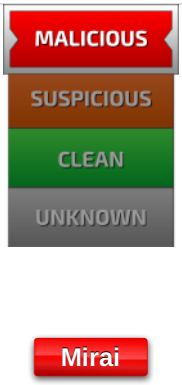
Linux Analysis Report SedZv73LJb

Overview

General Information

Sample Name:	SedZv73LJb
Analysis ID:	537271
MD5:	bdc02fe5c4e820c..
SHA1:	d49ff96bbfbd990…
SHA256:	a06645dcacd00b..
Tags:	32 elf mips mirai
Infos:	

Detection

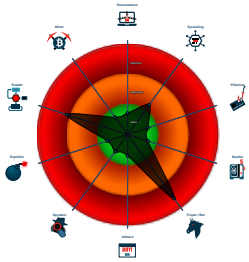


Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Sample is packed with UPX
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Detected TCP or UDP traffic on non…
- Executes the "rm" command used to…
- Sample listens on a socket
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

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:	537271
Start date:	09.12.2021
Start time:	17:04:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SedZv73LJb
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.evad.lin@0/2@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - SedZv73LJb (PID: 5216, Parent: 5108, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/SedZv73LJb
    - SedZv73LJb New Fork (PID: 5218, Parent: 5216)
    - SedZv73LJb New Fork (PID: 5220, Parent: 5216)
    - SedZv73LJb New Fork (PID: 5221, Parent: 5216)
      - SedZv73LJb New Fork (PID: 5224, Parent: 5221)
      - SedZv73LJb New Fork (PID: 5226, Parent: 5221)
      - SedZv73LJb New Fork (PID: 5229, Parent: 5221)
- systemd New Fork (PID: 5249, Parent: 1)
  - sshd (PID: 5249, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5250, Parent: 1)
  - sshd (PID: 5250, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- dash New Fork (PID: 5258, Parent: 4331)
  - rm (PID: 5258, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.FfRdbVixpI /tmp/tmp.30Eql1npMD /tmp/tmp.8ub6rio7wF
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SedZv73LJb	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x7428:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x7497:$s2: $Id: UPX • 0x7448:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

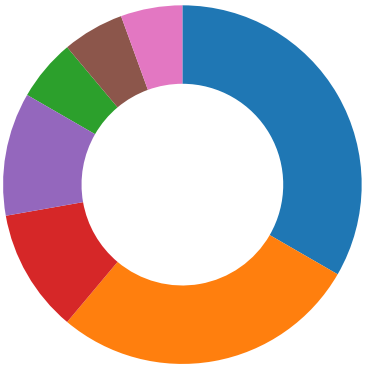
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5218.1.0000000047c7bfd3.0000000051fda745.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1414:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1488:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14fc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1570:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x15e4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1864:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1914:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x196c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19c4:$xo1: oMXKNNC\x0D\x17\x0C\x12
5226.1.0000000047c7bfd3.0000000051fda745.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1414:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1488:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14fc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1570:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x15e4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1864:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1914:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x196c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19c4:$xo1: oMXKNNC\x0D\x17\x0C\x12
5216.1.0000000047c7bfd3.0000000051fda745.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1414:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1488:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14fc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1570:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x15e4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1864:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1914:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x196c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19c4:$xo1: oMXKNNC\x0D\x17\x0C\x12
5220.1.0000000001011e93.00000000a387de8a.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x14860:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x148d0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14940:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x149b0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14a20:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14c90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14ce4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14d38:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14d8c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14de0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5220.1.0000000001011e93.00000000a387de8a.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x14190:$x1: POST /cdn-cgi/ • 0x146e0:$s1: LCOGQGPTGP

Click to see the 19 entries

Jbx Signature Overview



Click to jump to signature section

Networking:

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

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Sample is packed with UPX

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

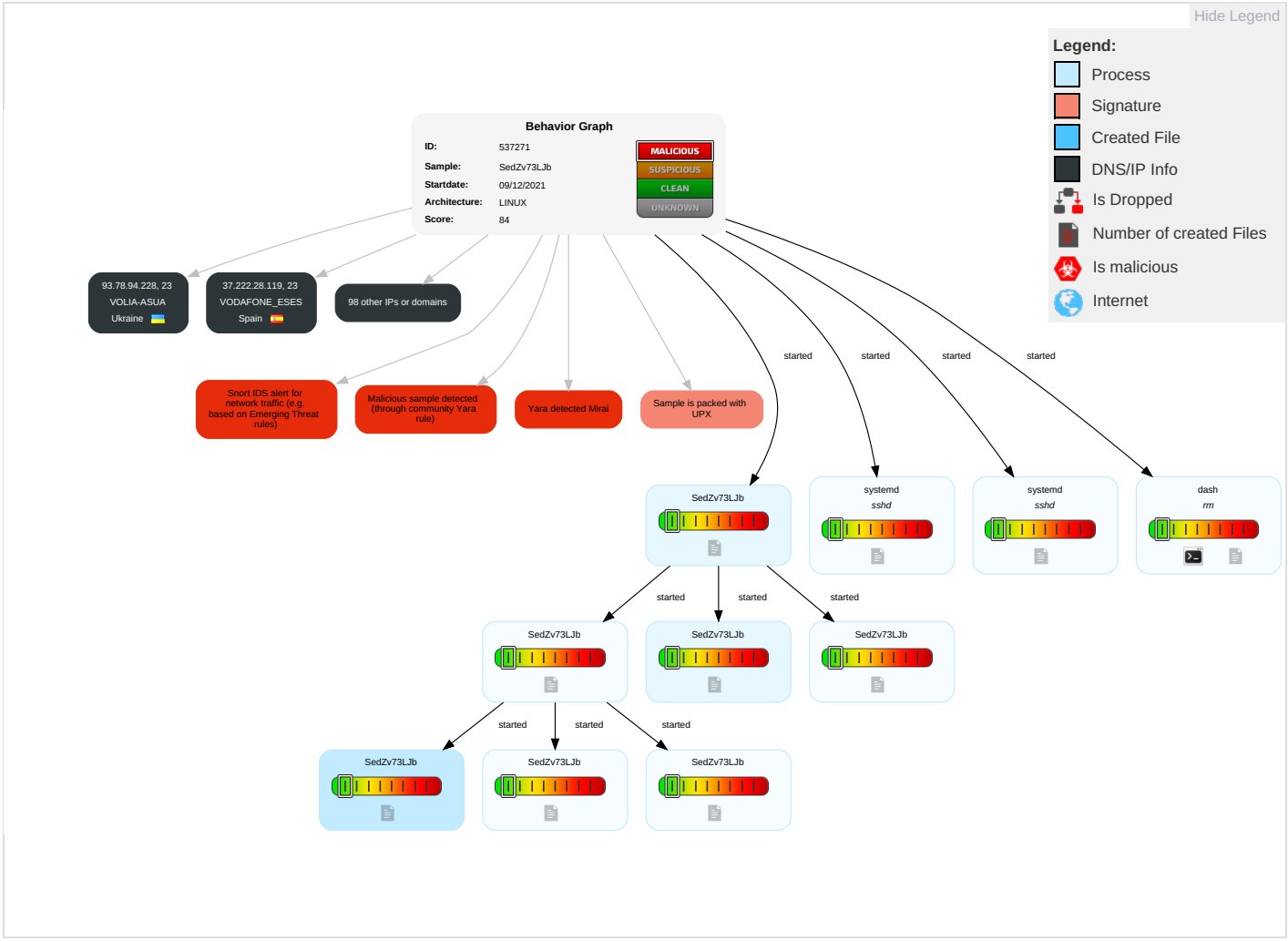
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	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	Mod Syst Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File Deletion 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock
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	Dele Devi Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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
117.19.19.122	unknown	Taiwan; Republic of China (ROC)		38197	SUNHK-DATA-AS-APSunNetworkHongKongLimited-HongKong	false
210.103.188.12	unknown	Korea Republic of		9848	SEJONGTELECOM-AS-KRSejongTelecomKR	false
200.158.224.63	unknown	Brazil		27699	TELEFONICABRASILSABR	false
121.146.235.107	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
183.163.75.205	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
118.250.121.154	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
103.40.78.108	unknown	Bangladesh		17941	BIT-ISLEEquinixJpapanEnterpriseKKJP	false
179.141.53.34	unknown	Brazil		53037	NEXTELTELECOMUNICACOESLTDABR	false
172.60.217.202	unknown	United States		21928	T-MOBILE-AS21928US	false
12.245.37.164	unknown	United States		7018	ATT-INTERNET4US	false
193.149.169.50	unknown	Denmark		15411	DANISCODK	false
188.177.15.44	unknown	Denmark		3292	TDCTDCASDK	false
2.240.29.75	unknown	Germany		6805	TDDE-ASN1DE	false
81.24.111.186	unknown	Netherlands		12414	NL-SOLCONSOLCONNL	false
31.113.67.161	unknown	United Kingdom		12576	EELtdGB	false
20.138.253.204	unknown	United States		22562	CSC-IGN-EMEAUS	false
188.247.215.88	unknown	Kazakhstan		21299	KAR-TEL-ASAlmatyRepublicofKazakhstanKZ	false
98.83.39.2	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
211.61.228.167	unknown	Korea Republic of		9457	DREAMX-ASDREAMLINECOKR	false
115.194.167.85	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
244.65.58.1	unknown	Reserved		unknown	unknown	false
124.123.173.97	unknown	India		18209	BEAMTELE-AS-APAtriaConvergenceTechnologiespvtltdIN	false
151.107.46.180	unknown	United States		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	false
135.195.71.230	unknown	United States		14962	NCR-252US	false
27.115.204.179	unknown	Korea Republic of		17871	DIGITALBUSANDONGNAM-AS-KRTBroadKR	false
77.100.21.151	unknown	United Kingdom		5089	NTLGB	false
79.25.116.8	unknown	Italy		3269	ASN-IBSNAZIT	false
39.195.134.246	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
111.199.252.113	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
218.236.172.7	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
176.41.20.117	unknown	Turkey		34984	TELLCOM-ASTR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
140.238.74.31	unknown	United States		31898	ORACLE-BMC-31898US	false
202.72.89.24	unknown	China		4721	JCNJupiterTelecommunicationsCoLtdJP	false
41.23.225.130	unknown	South Africa		29975	VODACOM-ZA	false
108.219.61.37	unknown	United States		7018	ATT-INTERNET4US	false
24.180.92.208	unknown	United States		20115	CHARTER-20115US	false
58.171.235.85	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
149.216.250.38	unknown	Germany		12422	EVONIK-ASRellinghauserStr1-11DE	false
196.17.156.92	unknown	Seychelles		56611	REBACOM-ASNL	false
40.75.37.239	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
163.181.241.19	unknown	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
185.221.109.100	unknown	Poland		200534	MSERWIS-ASPL	false
163.108.158.167	unknown	France		3215	FranceTelecom-OrangeFR	false
149.154.90.25	unknown	Italy		57144	ICCREA-ASIT	false
75.116.189.96	unknown	United States		6167	CELLCO-PARTUS	false
121.174.214.230	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
113.218.192.79	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
37.222.28.119	unknown	Spain		12430	VODAFONE_ESES	false
170.171.210.202	unknown	United States		11790	RANDOMHOUSEUS	false
48.207.191.193	unknown	United States		2686	ATGS-MMD-ASUS	false
67.203.209.166	unknown	Puerto Rico		11992	CENTENNIAL-PR	false
194.66.187.63	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
207.104.42.36	unknown	United States		7018	ATT-INTERNET4US	false
68.97.145.241	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
216.115.166.77	unknown	United States		11676	AS11676US	false
86.136.144.174	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
247.112.5.133	unknown	Reserved		unknown	unknown	false
198.198.68.40	unknown	United States		292	ESNET-WESTUS	false
154.7.186.78	unknown	United States		174	COGENT-174US	false
142.70.203.200	unknown	Canada		855	CANET-ASN-4CA	false
146.152.201.30	unknown	United States		197938	TRAVIANGAMESDE	false
248.255.162.154	unknown	Reserved		unknown	unknown	false
170.47.41.0	unknown	United States		22178	PA-SENATEUS	false
124.205.52.227	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
179.187.5.184	unknown	Brazil		18881	TELEFONICABRASILSABR	false
223.175.213.136	unknown	Korea Republic of		17853	LGTELECOM-AS-KRLGTELECOMKR	false
75.102.196.108	unknown	United States		20130	DEPAULUS	false
90.104.27.138	unknown	France		3215	FranceTelecom-OrangeFR	false
44.117.91.202	unknown	United States		7377	UCSDUS	false
247.169.112.139	unknown	Reserved		unknown	unknown	false
45.106.164.142	unknown	Egypt		37069	MOBINILEG	false
95.223.227.166	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
113.86.238.36	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
162.96.112.109	unknown	United States		33274	ASN-FAIRVIEWHEALTHSERVICESUS	false
253.127.107.222	unknown	Reserved		unknown	unknown	false
38.211.197.148	unknown	United States		174	COGENT-174US	false
79.253.233.152	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
136.168.31.201	unknown	United States		2152	CSUNET-NWUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.27.241.90	unknown	United States		701	UUNETUS	false
166.175.198.250	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
14.93.4.20	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
186.222.49.245	unknown	Brazil		28573	CLAROSABR	false
173.94.47.24	unknown	United States		11426	TWC-11426-CAROLINASUS	false
96.64.115.226	unknown	United States		7922	COMCAST-7922US	false
24.251.247.192	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
126.218.65.187	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
8.33.44.166	unknown	United States		46802	ASN-BACKCOUNTRYUS	false
124.50.41.36	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
93.78.94.228	unknown	Ukraine		25229	VOLIA-ASUA	false
175.67.185.235	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
146.1.46.239	unknown	United States		3378	MCI-ASNUS	false
164.13.138.176	unknown	Finland		50195	UMSI	false
141.37.182.63	unknown	Germany		553	BELWUEBelWue-KoordinationEU	false
95.118.195.78	unknown	Germany		6805	TDDE-ASN1DE	false
32.212.182.171	unknown	United States		46690	SNET-FCCUS	false
108.172.58.141	unknown	Canada		852	ASN852CA	false
79.83.58.68	unknown	France		15557	LDCOMNETFR	false
182.230.86.39	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
142.23.150.35	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
167.177.246.95	unknown	United States		7800	ALLINA-HEALTH-SYSTEM-INCUS	false

Runtime Messages

Command:	/tmp/SedZv73LJb
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	lzrd cock fest'/proc/'/exe
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
41.23.225.130	ULM7uOGq51	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SEJONGTELECOM-AS-KRSejongTelecomKR	pmXK4A8neD	Get hash	malicious	Browse	• 203.227.200.14
	kwari.arm7	Get hash	malicious	Browse	• 203.227.200.14
	E16TvLJm2w	Get hash	malicious	Browse	• 203.239.73.131
	kDLGx7ivMz	Get hash	malicious	Browse	• 211.239.98.151

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	biKMh38rah	Get hash	malicious	Browse	• 203.231.132.129
	Ntb86B1N1X	Get hash	malicious	Browse	• 210.122.43.183
	MA4UA3e5xe	Get hash	malicious	Browse	• 61.109.204.203
	mips-20211126-2221	Get hash	malicious	Browse	• 211.116.207.254
	KEn71AQ430	Get hash	malicious	Browse	• 203.231.219.228
	y8CYO3E0MF	Get hash	malicious	Browse	• 203.227.200.26
	mLh9jwpikq	Get hash	malicious	Browse	• 203.227.17.76
	4i9Yl7vp8B	Get hash	malicious	Browse	• 203.239.37.45
	sora.arm	Get hash	malicious	Browse	• 61.250.64.14
	9B6EN8PxhH	Get hash	malicious	Browse	• 203.227.200.15
	dark.x86	Get hash	malicious	Browse	• 203.231.219.232
	sora.x86	Get hash	malicious	Browse	• 210.127.68.251
	mipsel	Get hash	malicious	Browse	• 203.239.13.14
	ENYxttDmO1	Get hash	malicious	Browse	• 203.231.219.204
	JjHQ8Q1weT	Get hash	malicious	Browse	• 211.239.243.5
	Xb1sM3W7BK	Get hash	malicious	Browse	• 211.239.173.129
SUNHK-DATA-AS-APSunNetworkHongKongLimited-HongKong	RA8SVd00EW	Get hash	malicious	Browse	• 117.18.11.132
	NNoG9EuSVV	Get hash	malicious	Browse	• 117.19.113.73
	x86	Get hash	malicious	Browse	• 112.213.114.238
	sora.arm7	Get hash	malicious	Browse	• 115.42.62.116
	sora.x86	Get hash	malicious	Browse	• 117.18.11.188
	http___103.170.255.140_pdfword_invc_000930003999000.wbk	Get hash	malicious	Browse	• 210.56.63.51
	7758	Get hash	malicious	Browse	• 103.45.66.145
	hIejwF53zt	Get hash	malicious	Browse	• 112.213.114.222
	Tx60OCR2cN	Get hash	malicious	Browse	• 202.89.8.5
	Tsunami.arm	Get hash	malicious	Browse	• 112.213.114.232
	#Uac80#Ucc30#Uccad.apk	Get hash	malicious	Browse	• 43.243.111.75
	Swift copy.exe	Get hash	malicious	Browse	• 103.231.31.77
	qKjg35J4FG	Get hash	malicious	Browse	• 121.127.227.4
	vdQzjfJR0u	Get hash	malicious	Browse	• 115.42.62.108
	arm7	Get hash	malicious	Browse	• 117.18.11.169
	3DAMhv0DFI	Get hash	malicious	Browse	• 115.42.62.139
	46gV91KJhQ	Get hash	malicious	Browse	• 117.18.11.132
	wk.exe	Get hash	malicious	Browse	• 112.213.121.145
	mA7WUZVyyP	Get hash	malicious	Browse	• 112.213.114.251
	OswYbjULpg.exe	Get hash	malicious	Browse	• 112.213.109.186

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5250/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6

/proc/5250/oom_score_adj	
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):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:CAv:CK
MD5:	251228B89D027A84AC9239BB479F7FD1
SHA1:	CF25590A562FE1FA7E766ADEC3DD6581D12A9398
SHA-256:	784FD8846009847E8493CED7F73AB7AD790719F4E036C26C9F7EA83A5C1C6AE1
SHA-512:	8F5BF028A28757B7EBC33786D695ADA2FF547FCC226A3804BD9B20B41052607867EC9486DDC2498FA15C34EE8C5F4E405D46D5F43FCB291F9DA34B9991BE8E2E
Malicious:	false
Reputation:	low
Preview:	5250.

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.907735920089907
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	SedZv73LJb
File size:	31960
MD5:	bdc02fe5c4e820cc750d4b5b7280f2cd
SHA1:	d49ff96bbfbd990ffdb4727a809b97eb05bf1c2a
SHA256:	a06645dcacd00b2ffa5db96729241c355e012fa87a2ef16d595a4bac7a7dcd10
SHA512:	5761b1230316be14335fb19f0d441377a16b28e4a809d7e9cd08da48d99c3e4ad14cd135cac186094c20cb245faa8d41d950540941e0686b70bb68cd39990bb
SSDEEP:	384:X3fpCLrsjHIX69URc+hmnulY1qHprFKt6zhS45vDajssVwfyhBTla39RWGVCz0Ng:nfpWcehzJFYKgULAssKfyhB5a3LWt
File Content Preview:	.ELF.....xh..4.....4. ...(.....{...{.....[...[E..[E.....4UPX!`.....Y...Y.....U.....?.E.h;....#.....b.L.1*)....Nw3.42..J.dn....>7.G._=...F.....*b..3_..v~..4NBA9*.i&..Q..@e.....

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)

ELF header

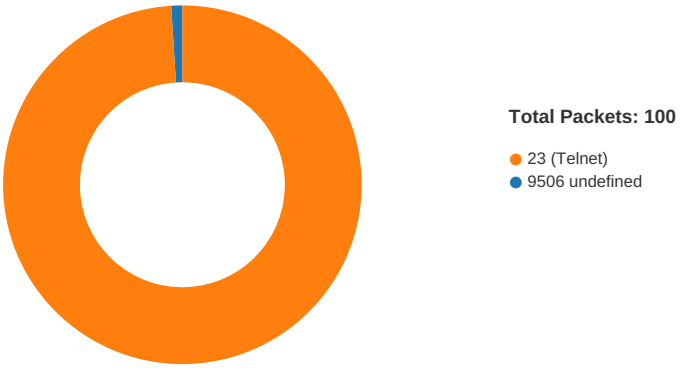
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x106878
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x7bb5	0x7bb5	4.1579	0x5	R E	0x10000		
LOAD	0x5bd8	0x455bd8	0x455bd8	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: SedZv73LJb PID: 5216 Parent PID: 5108

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	/tmp/SedZv73LJb
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: SedZv73LJb PID: 5218 Parent PID: 5216

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: SedZv73LJb PID: 5220 Parent PID: 5216

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SedZv73LJb PID: 5221 Parent PID: 5216

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SedZv73LJb PID: 5224 Parent PID: 5221

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: SedZv73LJb PID: 5226 Parent PID: 5221

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: SedZv73LJb PID: 5229 Parent PID: 5221

General

Start time:	17:05:02
Start date:	09/12/2021
Path:	/tmp/SedZv73LJb
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: systemd PID: 5249 Parent PID: 1

General

Start time:	17:05:10
Start date:	09/12/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5249 Parent PID: 1

General

Start time:	17:05:10
Start date:	09/12/2021
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: 5250 Parent PID: 1

General

Start time:	17:05:10
Start date:	09/12/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5250 Parent PID: 1

General

Start time:	17:05:10
Start date:	09/12/2021
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: dash PID: 5258 Parent PID: 4331

General

Start time:	17:05:25
Start date:	09/12/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5258 Parent PID: 4331

General

Start time:	17:05:25
Start date:	09/12/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.FfRdbVixpI /tmp/tmp.30Eql1npMD /tmp/tmp.8ub6rio7wF
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read