ID: 518915
Sample Name: zD1jpTbFQq
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:52:18
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

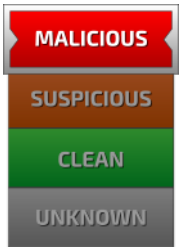
Linux Analysis Report zD1jpTbFQq

Overview

General Information

Sample Name:	zD1jpTbFQq
Analysis ID:	518915
MD5:	e06f0a88a25db59.
SHA1:	ee8da3d3dffde40..
SHA256:	f3f57dc399b0dc7..
Tags:	32 elf mirai powerpc
Infos:	

Detection

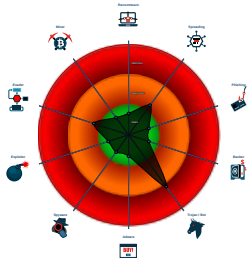


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Yara signature match
- Sample has stripped symbol table
- Reads system information from the ...
- 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:	518915
Start date:	10.11.2021
Start time:	04:52:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zD1jpTbFQq
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:	mal60.troj.lin@0/4@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- zD1jpTbFQq (PID: 5245, Parent: 5119, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/zD1jpTbFQq
  - zD1jpTbFQq New Fork (PID: 5247, Parent: 5245)
  - zD1jpTbFQq New Fork (PID: 5248, Parent: 5245)
    - zD1jpTbFQq New Fork (PID: 5251, Parent: 5248)
    - zD1jpTbFQq New Fork (PID: 5252, Parent: 5248)
    - zD1jpTbFQq New Fork (PID: 5257, Parent: 5248)
    - zD1jpTbFQq New Fork (PID: 5258, Parent: 5248)
    - zD1jpTbFQq New Fork (PID: 5261, Parent: 5248)
      - zD1jpTbFQq New Fork (PID: 5266, Parent: 5261)
    - zD1jpTbFQq New Fork (PID: 5262, Parent: 5248)
- systemd New Fork (PID: 5268, Parent: 1)
- journalctl (PID: 5268, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5280, Parent: 1)
- systemd-journald (PID: 5280, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- xfce4-session New Fork (PID: 5283, Parent: 1900)
- xfsettingsd (PID: 5283, Parent: 1900, MD5: d7ae7090131cf73e021f6c89515f984b) Arguments: xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
  - xfsettingsd New Fork (PID: 5294, Parent: 5283)
- xfce4-session New Fork (PID: 5295, Parent: 1900)
- xfsettingsd (PID: 5295, Parent: 1900, MD5: d7ae7090131cf73e021f6c89515f984b) Arguments: xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
  - xfsettingsd New Fork (PID: 5296, Parent: 5295)
- xfce4-session New Fork (PID: 5297, Parent: 1900)
- xfsettingsd (PID: 5297, Parent: 1900, MD5: d7ae7090131cf73e021f6c89515f984b) Arguments: xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
  - xfsettingsd New Fork (PID: 5302, Parent: 5297)
- xfce4-session New Fork (PID: 5303, Parent: 1900)
- xfsettingsd (PID: 5303, Parent: 1900, MD5: d7ae7090131cf73e021f6c89515f984b) Arguments: xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
  - xfsettingsd New Fork (PID: 5308, Parent: 5303)
- xfce4-session New Fork (PID: 5309, Parent: 1900)
- xfsettingsd (PID: 5309, Parent: 1900, MD5: d7ae7090131cf73e021f6c89515f984b) Arguments: xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
  - xfsettingsd New Fork (PID: 5314, Parent: 5309)
- systemd New Fork (PID: 5317, Parent: 1)
- journalctl (PID: 5317, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- **cleanup**

Yara Overview

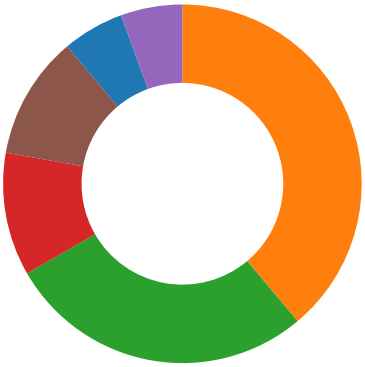
Initial Sample

Source	Rule	Description	Author	Strings
zD1jpTbFQq	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x150e0:$xo1: Dfs`eeh&<'9 • 0x15158:$xo1: Dfs`eeh&<'9 • 0x151cc:$xo1: Dfs`eeh&<'9 • 0x1523c:$xo1: Dfs`eeh&<'9 • 0x15288:$xo1: Dfs`eeh&<'9

Memory Dumps

Source	Rule	Description	Author	Strings
5251.1.00000000675bcb72.00000000cfa8fb02.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x150e0:$xo1: Dfs`eeh&<'9 • 0x15158:$xo1: Dfs`eeh&<'9 • 0x151cc:$xo1: Dfs`eeh&<'9 • 0x1523c:$xo1: Dfs`eeh&<'9 • 0x15288:$xo1: Dfs`eeh&<'9
5248.1.00000000675bcb72.00000000cfa8fb02.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x150e0:$xo1: Dfs`eeh&<'9 • 0x15158:$xo1: Dfs`eeh&<'9 • 0x151cc:$xo1: Dfs`eeh&<'9 • 0x1523c:$xo1: Dfs`eeh&<'9 • 0x15288:$xo1: Dfs`eeh&<'9
5258.1.00000000675bcb72.00000000cfa8fb02.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x150e0:$xo1: Dfs`eeh&<'9 • 0x15158:$xo1: Dfs`eeh&<'9 • 0x151cc:$xo1: Dfs`eeh&<'9 • 0x1523c:$xo1: Dfs`eeh&<'9 • 0x15288:$xo1: Dfs`eeh&<'9
5258.1.00000000d3035e25.00000000c57598df.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x250c:$xo1: Dfs`eeh&<'9 • 0x2588:$xo1: Dfs`eeh&<'9 • 0x2600:$xo1: Dfs`eeh&<'9 • 0x2674:$xo1: Dfs`eeh&<'9 • 0x26c4:$xo1: Dfs`eeh&<'9
5247.1.00000000d3035e25.00000000c57598df.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x250c:$xo1: Dfs`eeh&<'9 • 0x2588:$xo1: Dfs`eeh&<'9 • 0x2600:$xo1: Dfs`eeh&<'9 • 0x2674:$xo1: Dfs`eeh&<'9 • 0x26c4:$xo1: Dfs`eeh&<'9
Click to see the 10 entries				

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

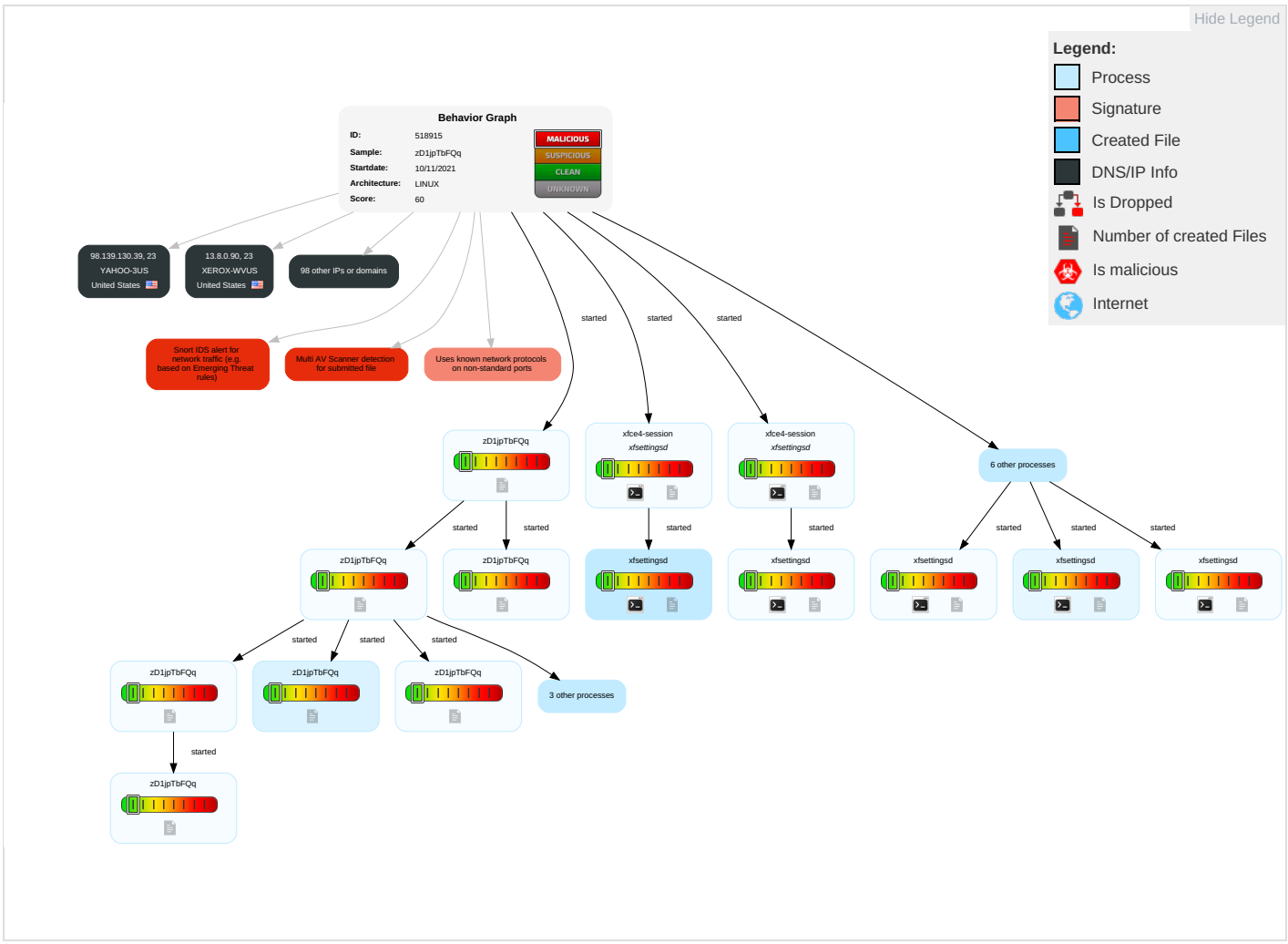
Mitre Att&ck Matrix

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	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	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
zD1jpTbFQq	59%	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
8.141.217.212	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
66.217.147.40	unknown	United States		7029	WINDSTREAMUS	false
83.220.183.211	unknown	Russian Federation		34456	RIALCOM-ASRU	false
110.76.149.26	unknown	Indonesia		38506	PIKANET-AS-IDPTPikaMediaKomunikaID	false
81.90.6.124	unknown	Russian Federation		12739	NETLINE_ASRU	false
111.122.94.155	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
92.53.31.140	unknown	Macedonia		43612	BLIZOOMK	false
191.12.225.240	unknown	Brazil		26599	TELEFONICABRASILSABR	false
152.41.163.251	unknown	United States		22854	CATAWBA-COLLEGEUS	false
2.222.21.147	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
9.63.59.31	unknown	United States		3356	LEVEL3US	false
138.9.239.14	unknown	United States		18663	UOP-ASUS	false
93.72.89.226	unknown	Ukraine		25229	VOLIA-ASUA	false
108.230.125.248	unknown	United States		7018	ATT-INTERNET4US	false
53.112.177.79	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
116.185.245.133	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
146.249.105.69	unknown	France		12765	TOTAL-CONNECTFR	false
207.111.164.255	unknown	United States		7314	TIS-ASNUS	false
182.49.33.62	unknown	China		9371	SAKURA-CSAKURAInternetIncJP	false
96.205.253.20	unknown	United States		7922	COMCAST-7922US	false
79.82.199.182	unknown	France		15557	LDCOMNETFR	false
149.123.58.227	unknown	United States		174	COGENT-174US	false
133.71.76.162	unknown	Japan		131897	EHIME-UNationalUniversityCorporationEhimeUniversityJ	false
116.123.188.38	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
64.11.109.131	unknown	United States		701	UUNETUS	false
108.90.177.118	unknown	United States		7018	ATT-INTERNET4US	false
182.37.86.132	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
172.209.54.248	unknown	United States		18747	IFX18747US	false
204.66.152.22	unknown	United States		1761	TDIR-CAPNETUS	false
208.61.202.33	unknown	United States		7018	ATT-INTERNET4US	false
117.241.195.11	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
124.97.60.6	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
175.160.7.20	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
169.216.205.14	unknown	Korea Republic of		37611	AfrihostZA	false
117.235.136.149	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
150.216.250.169	unknown	United States		10952	ECU-ASUS	false
168.63.110.245	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
188.213.127.160	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
140.224.26.182	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
8.195.218.66	unknown	United States		3356	LEVEL3US	false
148.78.186.253	unknown	United States		16811	SAGENET-GTHUS	false
67.214.45.86	unknown	United States		40336	UNISKY-MIAUS	false
198.20.174.5	unknown	Canada		55286	SERVER-MANIACA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
112.47.206.166	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
181.54.154.55	unknown	Colombia		10620	TelmexColombiaSACO	false
113.185.159.73	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
189.83.123.80	unknown	Brazil		7738	TelemarNorteLesteSABR	false
42.168.40.11	unknown	China		4249	LILLY-ASUS	false
96.235.195.59	unknown	United States		701	UUNETUS	false
75.93.164.89	unknown	United States		7029	WINDSTREAMUS	false
222.107.228.174	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
91.156.144.52	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
88.189.112.244	unknown	France		12322	PROXADFR	false
122.141.120.145	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
122.126.239.230	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
31.9.165.6	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
80.42.168.221	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
165.77.0.253	unknown	United States		4725	ODNSoftBankMobileCorpJP	false
17.35.71.6	unknown	United States		714	APPLE-ENGINEERINGUS	false
205.244.82.224	unknown	United States		3364	CSDCO-ASUS	false
109.56.179.18	unknown	Sweden		44034	HI3GSE	false
178.201.249.3	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
13.8.0.90	unknown	United States		26662	XEROX-WVUS	false
203.51.156.22	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
204.120.171.63	unknown	United States		1239	SPRINTLINKUS	false
207.26.25.171	unknown	United States		701	UUNETUS	false
157.114.152.220	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
169.44.187.157	unknown	United States		36351	SOFTLAYERUS	false
9.146.149.27	unknown	United States		3356	LEVEL3US	false
181.80.17.58	unknown	Argentina		7303	TelecomArgentinaSAAR	false
79.67.235.84	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
83.31.103.192	unknown	Poland		5617	TPNETPL	false
155.199.164.196	unknown	United States		786	JANETJiscServicesLimitedGB	false
86.17.103.193	unknown	United Kingdom		5089	NTLGB	false
101.32.36.49	unknown	China		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	false
204.244.141.52	unknown	Canada		5071	WESTEL-1CA	false
83.235.207.5	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
159.156.105.82	unknown	Switzerland		34578	BEDAGCH	false
141.230.254.0	unknown	United States		12701	BARCAPLondonGB	false
73.255.137.215	unknown	United States		7922	COMCAST-7922US	false
164.69.149.27	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
79.245.37.67	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
182.28.200.243	unknown	Indonesia		4795	INDOSATM2-IDINDOSATM2ASNID	false
39.97.83.169	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
101.150.83.142	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
2.35.34.170	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
98.139.130.39	unknown	United States		26101	YAHOO-3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
39.31.92.119	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
60.174.151.99	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
175.142.100.244	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
190.105.172.168	unknown	Haiti		52297	HAICOMHaitiCommunicationsSAHT	false
203.124.232.238	unknown	India		9238	TATA-ASTATAISPIN	false
136.39.108.37	unknown	United States		16591	GOOGLE-FIBERUS	false
164.141.19.164	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
141.220.243.240	unknown	United States		394769	UMF-7-ASUS	false
86.152.155.233	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
92.93.73.81	unknown	France		15557	LDCOMNETFR	false
109.54.4.240	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
152.136.47.106	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
156.194.156.6	unknown	Egypt		8452	TE-ASTE-ASEG	false

Runtime Messages

Command:	/tmp/zD1jpTbFQq
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	xXxSlicexXxxVEGA.
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	NMhjdmrpZi	Get hash	malicious	Browse	• 139.244.36.194
	arm7	Get hash	malicious	Browse	• 139.245.51.216
	x86-20211110-0150	Get hash	malicious	Browse	• 121.198.26.158
	sora.x86	Get hash	malicious	Browse	• 8.168.189.30
	KKveTTgaAAsecNNaaaa.arm7	Get hash	malicious	Browse	• 47.99.128.220
	arm	Get hash	malicious	Browse	• 47.99.216.211
	Heri2RE17I	Get hash	malicious	Browse	• 47.105.100.82
	vbc.exe	Get hash	malicious	Browse	• 101.132.116.91
	mips	Get hash	malicious	Browse	• 39.106.158.24
	hsnAV1agq8.exe	Get hash	malicious	Browse	• 121.89.207.1
	yfOb3wBmub.exe	Get hash	malicious	Browse	• 121.89.207.1
	qgxgn5fQU1	Get hash	malicious	Browse	• 59.110.169.4
	BS0Dxmu2go	Get hash	malicious	Browse	• 8.157.73.157
	GB0O1NUtmJ	Get hash	malicious	Browse	• 47.113.198.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dYgJ72oG4f	Get hash	malicious	Browse	• 47.105.136.170
	O4aHLhCviL	Get hash	malicious	Browse	• 47.114.175.36
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 8.139.27.141
	jyTZMJKPD2	Get hash	malicious	Browse	• 47.96.183.126
	SQFoFeC1jQ	Get hash	malicious	Browse	• 139.247.66.94
	byxEpar5Zm	Get hash	malicious	Browse	• 8.175.9.72
WINDSTREAMUS	fNrSUTMJ8O	Get hash	malicious	Browse	• 74.8.108.56
	arm7	Get hash	malicious	Browse	• 63.255.73.32
	x86-20211110-0150	Get hash	malicious	Browse	• 72.242.215.100
	sora.x86	Get hash	malicious	Browse	• 173.184.64.70
	sora.arm7	Get hash	malicious	Browse	• 75.92.93.242
	sora.arm	Get hash	malicious	Browse	• 98.16.221.213
	fZ9Y8XVXDH	Get hash	malicious	Browse	• 68.143.234.231
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 166.102.36.218
	QSjpGBd7Gv	Get hash	malicious	Browse	• 205.187.13 6.105
	x86_64	Get hash	malicious	Browse	• 74.9.152.70
	arm	Get hash	malicious	Browse	• 98.17.135.18
	arm6	Get hash	malicious	Browse	• 173.184.23 0.178
	4DrtSJOLjr	Get hash	malicious	Browse	• 40.134.73.47
	Kz2SeJpaxw	Get hash	malicious	Browse	• 74.8.121.17
	fMGehkjmPv	Get hash	malicious	Browse	• 209.253.40.34
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 165.247.11.247
	OoeA4dABtV	Get hash	malicious	Browse	• 207.223.23 6.218
	YG9KkTTAgE	Get hash	malicious	Browse	• 69.95.185.164
	kkr4DrMz5L	Get hash	malicious	Browse	• 66.184.133.224
	fCca2FJVXG	Get hash	malicious	Browse	• 216.73.137.189

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/run/systemd/journal/streams/.#9:74252mAQxYs	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.511422543934028
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm5SVjhWGYnS1c+sjsv:SbFuFyLVIg1BG+f+M0FhBQSiTji4s
MD5:	7B73F82546FE8A5EDCC9143DFD3D9623
SHA1:	99F973F289FE56E370C1AB2CB51035C0EDCCC9B9
SHA-256:	9F76085AEE2C9244A13B4C38F719358084169367A993970B2D0E12E89F1BED79
SHA-512:	D14BF70B3D0D09CD24F152BFC33A5FEC396D86AB0CBFA397AB32281C057B6CC3A068CFC8B8EC73CFC3AEB547AB968D49E6BE6734A42E3F0382F7977ECF2059E
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=3be6002e7fd64011ac6b184d7bd2f262.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/run/systemd/journal/streams/.#9:742562yIbVs	
Process:	/lib/systemd/systemd-journald
File Type:	ASCII text
Category:	dropped

/run/systemd/journal/streams/.#9:742562yIbVs	
Size (bytes):	223
Entropy (8bit):	5.529631514219359
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmph4FVHhB1EvAglsjq:SbFuFyLVIg1BG+f+M4FxFEYTji4s
MD5:	D0304411F03172DC7BA1ABD4BBEBB26A
SHA1:	73E6F823ECEA5598A2A70DE05DDACF2C4A261D1E
SHA-256:	2203E7DAA0296132BF000098FAFD3E54A2457E22FF17CFDF53F59569C1BE7212
SHA-512:	AF63A99CF14F446F8469197319418BCCBEC8B9CA36BEF21FF5BB37C8B22BD4E971823CB64D5F1623B1EA90D2ABB6FCCE0074E2756557715D2245A59BC8B87B8
Malicious:	false
Reputation:	low
Preview:	# This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=c50063e8c75c4227a1bfba9c431fd9aa.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service.

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/system.journal	
Process:	/lib/systemd/systemd-journald
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	1.448047321524811
Encrypted:	false
SSDEEP:	3:F31HlbMg7fl9Mg7F:F3Vflv
MD5:	C88D104844C9FA10D75CAF83B9078AEC
SHA1:	920D12F6638F08118DB5515FAF9F0EFEACFBD4F3
SHA-256:	FD2E34DE60BD081DF453CD95C7F4808AFC65A1B4AB121531295814495B3B11D9
SHA-512:	D41405C6B2CEAD157B5DE96CE60C3136AB3D3CEA7B716E51AA115FA3ED7790A4174A2D2CB9F028992E00573D6384E9DF0022AA3F10A4915B7B74C5ECE59629B
Malicious:	false
Reputation:	low
Preview:	LPKSHHRH.....=-%.CK....".y.b.....=-%.CK....".y.b.....

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/user-1000.journal	
Process:	/lib/systemd/systemd-journald
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	1.4595260194504922
Encrypted:	false
SSDEEP:	3:F31HlvXKufXK6lt:F3fdLX
MD5:	9D0990C6C6734BFC3EBBA0B56A3D86B6
SHA1:	4E82380513A3E807E04C73EB2AA4C0314B70FDD0
SHA-256:	180F3932C2F975835DFB4B7BC25F1C6617CA0D4692706BC556E601C1054475E9
SHA-512:	52B6A383CA0F115D25162DECCC200C354E4AE54B42AB0131596D284EB883F4446A0922139FAEAC588AD61F1D8FE0B79B1BBBF81E44F726416C3A08223FF5481
Malicious:	false
Reputation:	low
Preview:	LPKSHHRH.....5.2..]AM.v.%\. .....5.2..]AM.v.%\. .....

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.361116795039536
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	zD1jpTbFQq
File size:	93144
MD5:	e06f0a88a25db599d47dadb03907ef00
SHA1:	ee8da3d3dffde40ef93700991aa5d472d760fda5
SHA256:	f3f57dc399b0dc7bbe3a019afb7d7402c40274deea75b2cc605ff13e94229c71

General

SHA512:	49d3b63ad117a26995b8eb12c2c742ab396499b1f388e5 5e67da7c42ab2de79ea54321743640b09d270d8167c66a 26db26ba180a7f067987b13e6279a0b4b280
SSDEEP:	1536:U6PIx2j6HUvZjqEQTq3F+cCRIP3n6wFObVnI98M Ksd+:ZP6yZKqV536DnIyMr+
File Content Preview:	.ELF.....4..i.....4. ...(.....f...f..... .....f...f...f.....(X.....dt.Q.....!..|.....$H...H .G!...$8!. \|...N.. .!..\|.....?.....jP..../...@..\?.....f$.+../...A.. $8...})....f$N..

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x100001f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	92664
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

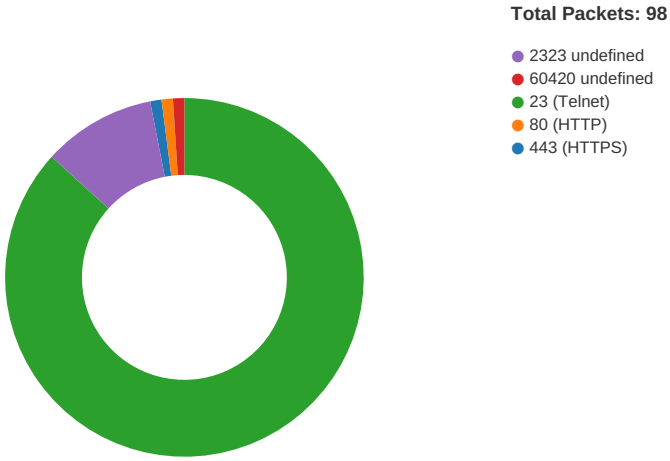
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0x14778	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x10014830	0x14830	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x10014850	0x14850	0x1db8	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x1002660c	0x1660c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x10026614	0x16614	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x10026620	0x16620	0x31c	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1002693c	0x1693c	0x70	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x100269ac	0x169ac	0xa4	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x10026a50	0x169ac	0x2414	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x169ac	0x4b	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	0x10000000	0x10000000	0x16608	0x16608	4.3134	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1660c	0x1002660c	0x1002660c	0x3a0	0x2858	1.8826	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: zD1jpTbFQq PID: 5245 Parent PID: 5119

General

Start time:	04:53:00
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	/tmp/zD1jpTbFQq
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: zD1jpTbFQq PID: 5247 Parent PID: 5245

General

Start time:	04:53:01
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: zD1jpTbFQq PID: 5248 Parent PID: 5245

General

Start time:	04:53:01
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq

Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: zD1jpTbFQq PID: 5251 Parent PID: 5248

General

Start time:	04:53:01
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: zD1jpTbFQq PID: 5252 Parent PID: 5248

General

Start time:	04:53:01
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: zD1jpTbFQq PID: 5257 Parent PID: 5248

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: zD1jpTbFQq PID: 5258 Parent PID: 5248

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq

Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: zD1jpTbFQq PID: 5261 Parent PID: 5248

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: zD1jpTbFQq PID: 5266 Parent PID: 5261

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: zD1jpTbFQq PID: 5262 Parent PID: 5248

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/tmp/zD1jpTbFQq
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: systemd PID: 5268 Parent PID: 1

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5268 Parent PID: 1

General

Start time:	04:53:05
Start date:	10/11/2021
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 5280 Parent PID: 1

General

Start time:	04:53:06
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5280 Parent PID: 1

General

Start time:	04:53:06
Start date:	10/11/2021
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Analysis Process: xfce4-session PID: 5283 Parent PID: 1900

General

Start time:	04:53:07
Start date:	10/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfsettingsd PID: 5283 Parent PID: 1900

General

Start time:	04:53:07
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfsettingsd PID: 5294 Parent PID: 5283

General

Start time:	04:53:09
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	n/a
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-session PID: 5295 Parent PID: 1900

General

Start time:	04:53:09
Start date:	10/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfsettingsd PID: 5295 Parent PID: 1900

General

Start time:	04:53:10
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfsettingsd PID: 5296 Parent PID: 5295

General

Start time:	04:53:11
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	n/a
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfce4-session PID: 5297 Parent PID: 1900

General

Start time:	04:53:11
Start date:	10/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfsettingsd PID: 5297 Parent PID: 1900

General

Start time:	04:53:11
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfsettingsd PID: 5302 Parent PID: 5297

General

Start time:	04:53:13
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	n/a
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfce4-session PID: 5303 Parent PID: 1900

General

Start time:	04:53:13
Start date:	10/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfsettingsd PID: 5303 Parent PID: 1900

General

Start time:	04:53:14
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfsettingsd PID: 5308 Parent PID: 5303

General

Start time:	04:53:15
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	n/a
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfce4-session PID: 5309 Parent PID: 1900

General

Start time:	04:53:15
Start date:	10/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfsettingsd PID: 5309 Parent PID: 1900

General

Start time:	04:53:16
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	xfsettingsd --display :1.0 --sm-client-id 2eab19738-df3b-455c-ba97-1de80472a7b4
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: xfsettingsd PID: 5314 Parent PID: 5309

General

Start time:	04:53:18
Start date:	10/11/2021
Path:	/usr/bin/xfsettingsd
Arguments:	n/a
File size:	322136 bytes
MD5 hash:	d7ae7090131cf73e021f6c89515f984b

File Activities

File Read

Analysis Process: systemd PID: 5317 Parent PID: 1

General

Start time:	04:53:19
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5317 Parent PID: 1

General

Start time:	04:53:19
Start date:	10/11/2021
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read