ID: 518983
Sample Name: e9e6i5D2gK
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:54:16
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

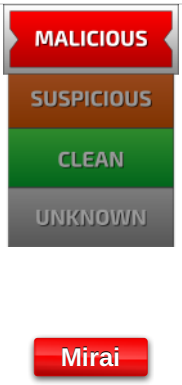
Linux Analysis Report e9e6i5D2gK

Overview

General Information

Sample Name:	e9e6i5D2gK
Analysis ID:	518983
MD5:	8dee5c2c55c632…
SHA1:	a4a8530f05f8c37..
SHA256:	0b1a02f1009fda9..
Tags:	32 elf mips mirai
Infos:	

Detection

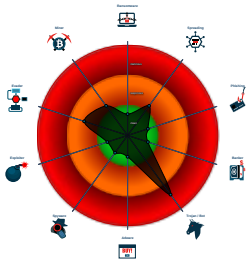


Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Reads system files that contain reco…
- Uses known network protocols on no…
- Sample reads /proc/mounts (often u…
- Reads CPU information from /sys in…
- Yara signature match
- Executes the "grep" command used…
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…

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 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:	518983
Start date:	10.11.2021
Start time:	07:54:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e9e6i5D2gK
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.lin@0/6@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- e9e6i5D2gK (PID: 5240, Parent: 5116, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/e9e6i5D2gK
  - e9e6i5D2gK New Fork (PID: 5242, Parent: 5240)
  - e9e6i5D2gK New Fork (PID: 5243, Parent: 5240)
    - e9e6i5D2gK New Fork (PID: 5246, Parent: 5243)
      - e9e6i5D2gK New Fork (PID: 5284, Parent: 5246)
      - e9e6i5D2gK New Fork (PID: 5316, Parent: 5246)
      - e9e6i5D2gK New Fork (PID: 5723, Parent: 5246)
      - e9e6i5D2gK New Fork (PID: 6244, Parent: 5246)
    - e9e6i5D2gK New Fork (PID: 5247, Parent: 5243)
- gnome-session-binary New Fork (PID: 5292, Parent: 1477)
- sh (PID: 5292, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
- gnome-shell (PID: 5292, Parent: 1477, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
  - gnome-shell New Fork (PID: 5601, Parent: 5292)
  - ibus-daemon (PID: 5601, Parent: 5292, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
    - ibus-daemon New Fork (PID: 5606, Parent: 5601)
    - ibus-memconf (PID: 5606, Parent: 5601, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
    - ibus-daemon New Fork (PID: 5608, Parent: 5601)
      - ibus-daemon New Fork (PID: 5609, Parent: 5608)
      - ibus-x11 (PID: 5609, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
    - ibus-daemon New Fork (PID: 5983, Parent: 5601)
    - ibus-engine-simple (PID: 5983, Parent: 5601, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
- systemd New Fork (PID: 5322, Parent: 1)
- systemd-localed (PID: 5322, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- dbus-daemon New Fork (PID: 5611, Parent: 5610)
- ibus-portal (PID: 5611, Parent: 5610, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
- systemd New Fork (PID: 5641, Parent: 1)
- upowerd (PID: 5641, Parent: 1, MD5: 1253eea2fe5fe4017069664284e326cd) Arguments: /usr/lib/upower/upowerd
- Xorg New Fork (PID: 5719, Parent: 1465)
- sh (PID: 5719, Parent: 1465, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
  - sh New Fork (PID: 5720, Parent: 5719)
  - xkbcomp (PID: 5720, Parent: 5719, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
- systemd New Fork (PID: 5728, Parent: 1)
- accounts-daemon (PID: 5728, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5732, Parent: 5728)
  - language-validate (PID: 5732, Parent: 5728, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5733, Parent: 5732)
    - language-options (PID: 5733, Parent: 5732, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5734, Parent: 5733)
      - sh (PID: 5734, Parent: 5733, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5735, Parent: 5734)
        - locale (PID: 5735, Parent: 5734, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5736, Parent: 5734)
        - grep (PID: 5736, Parent: 5734, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 5737, Parent: 1)
- geoclue (PID: 5737, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- dbus-daemon New Fork (PID: 5955, Parent: 5954)
- gjs (PID: 5955, Parent: 5954, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
- systemd New Fork (PID: 5964, Parent: 1334)
- pulseaudio (PID: 5964, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5999, Parent: 1)
- fprintd (PID: 5999, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
e9e6i5D2gK	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x266b0:$xo1: Dfs`eeh&<'9 • 0x26720:$xo1: Dfs`eeh&<'9 • 0x26790:$xo1: Dfs`eeh&<'9 • 0x26800:$xo1: Dfs`eeh&<'9 • 0x26870:$xo1: Dfs`eeh&<'9
e9e6i5D2gK	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x28655:$x5: .mdebug.abi32 • 0x2587c:$s3: CFOKLKQVPCVMP • 0x25860:$s4: QWRGPTKQMP • 0x2575c:$s5: HWCLVGAJ

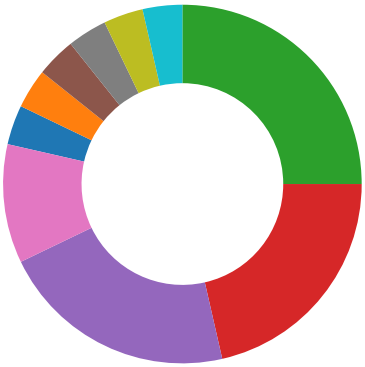
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5316.1.000000006ebd6c56.00000000a9ff7b07.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x266b0:$xo1: Dfs`eeh&<'9 • 0x26720:$xo1: Dfs`eeh&<'9 • 0x26790:$xo1: Dfs`eeh&<'9 • 0x26800:$xo1: Dfs`eeh&<'9 • 0x26870:$xo1: Dfs`eeh&<'9
5723.1.0000000030addc58.00000000eb641aaa.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x328:$xo1: Dfs`eeh&<'9 • 0x39c:$xo1: Dfs`eeh&<'9 • 0x410:$xo1: Dfs`eeh&<'9 • 0x484:$xo1: Dfs`eeh&<'9 • 0x4f8:$xo1: Dfs`eeh&<'9
5240.1.000000006ebd6c56.00000000a9ff7b07.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x266b0:$xo1: Dfs`eeh&<'9 • 0x26720:$xo1: Dfs`eeh&<'9 • 0x26790:$xo1: Dfs`eeh&<'9 • 0x26800:$xo1: Dfs`eeh&<'9 • 0x26870:$xo1: Dfs`eeh&<'9
5242.1.0000000030addc58.00000000eb641aaa.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x328:$xo1: Dfs`eeh&<'9 • 0x39c:$xo1: Dfs`eeh&<'9 • 0x410:$xo1: Dfs`eeh&<'9 • 0x484:$xo1: Dfs`eeh&<'9 • 0x4f8:$xo1: Dfs`eeh&<'9
5284.1.000000006ebd6c56.00000000a9ff7b07.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x266b0:$xo1: Dfs`eeh&<'9 • 0x26720:$xo1: Dfs`eeh&<'9 • 0x26790:$xo1: Dfs`eeh&<'9 • 0x26800:$xo1: Dfs`eeh&<'9 • 0x26870:$xo1: Dfs`eeh&<'9
Click to see the 8 entries				

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

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:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Sample reads /proc/mounts (often used for finding a writable filesystem)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

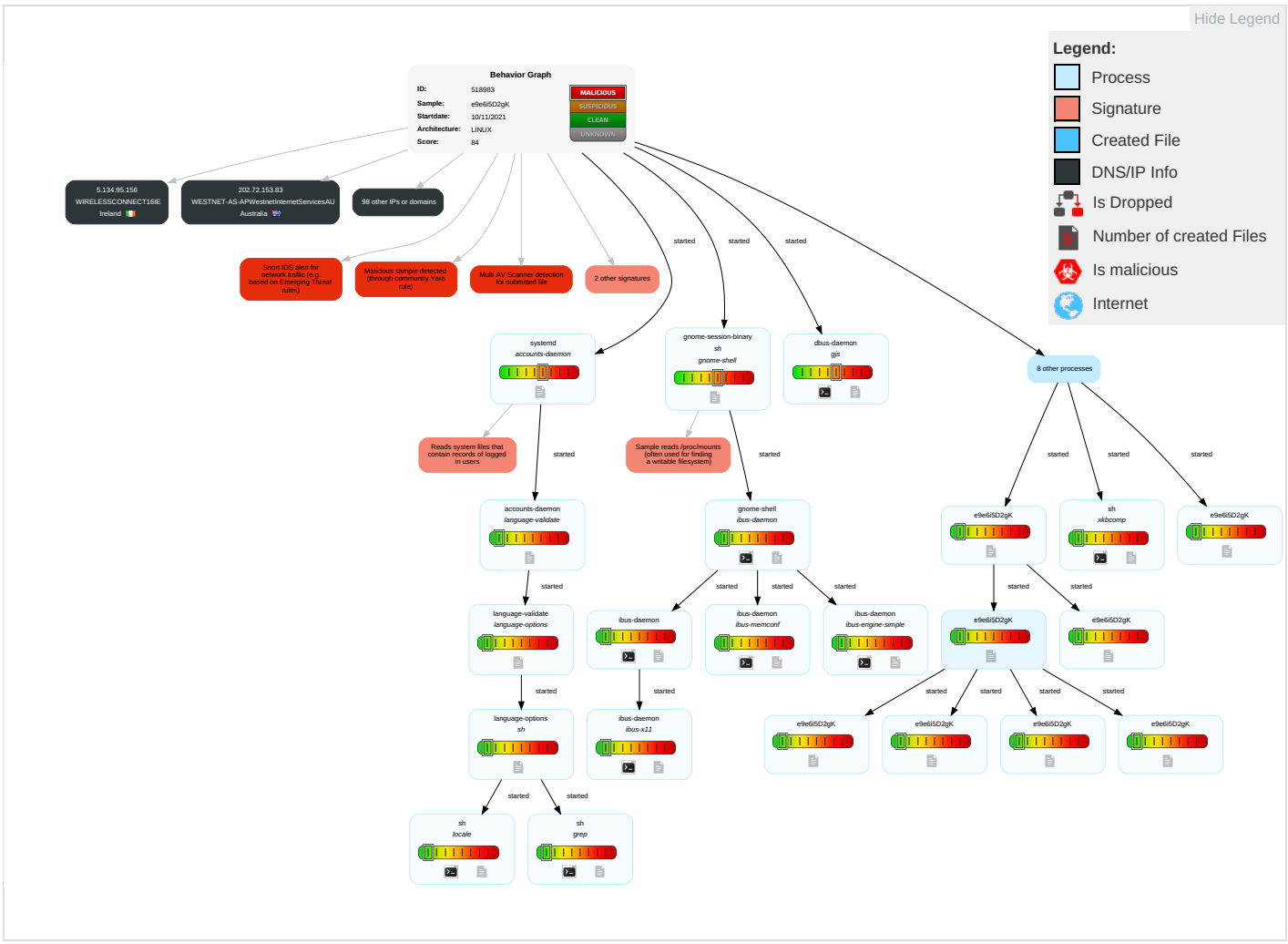
Mitre Att&ck Matrix

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	Scripting 1	Path Interception	Path Interception	File and Directory Permissions Modification 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	Modi Syst Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1	LSASS Memory	System Owner/User 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	Devi Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	File and Directory Discovery 1	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carri Billin Frau

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
e9e6i5D2gK	50%	Virustotal		Browse
e9e6i5D2gK	31%	Metadefender		Browse
e9e6i5D2gK	32%	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
69.230.36.246	unknown	United States		7018	ATT-INTERNET4US	false
202.72.153.83	unknown	Australia		9543	WESTNET-AS-APWestnetInternetServicesAU	false
108.168.171.183	unknown	United States		36351	SOFTLAYERUS	false
100.210.122.247	unknown	United States		21928	T-MOBILE-AS21928US	false
145.44.93.199	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
88.136.200.219	unknown	France		8228	CEGETEL-ASFR	false
221.48.215.251	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
177.44.253.129	unknown	Brazil		262441	FundValedoTaquarideEducDesenvolvSocialBR	false
42.152.254.64	unknown	Malaysia		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
75.131.165.180	unknown	United States		20115	CHARTER-20115US	false
217.19.115.49	unknown	Russian Federation		3216	SOVAM-ASRU	false
80.196.122.146	unknown	Denmark		3292	TDCTDCASDK	false
175.170.162.53	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
61.227.159.116	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
220.6.116.125	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
32.143.225.55	unknown	United States		7018	ATT-INTERNET4US	false
57.86.163.59	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
121.177.185.12	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
81.197.146.17	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
211.101.65.176	unknown	China		17964	DXTNETBeijingDian-Xin-TongNetworkTechnologiesCoLtd	false
84.148.41.187	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
66.170.22.8	unknown	United States		4150	SUPRANET-WISUS	false
123.59.155.208	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
111.43.58.28	unknown	China		132525	CMNET-HEILONGJIANG-CNHeiLongJiangMobileCommunicationComp	false
95.123.15.182	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
1.34.21.199	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
187.55.212.231	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
136.225.69.124	unknown	Sweden		158	ERI-ASUS	false
172.125.131.66	unknown	United States		7018	ATT-INTERNET4US	false
66.158.42.213	unknown	United States		6325	ILLINOIS-CENTURYUS	false
78.99.177.209	unknown	Slovakia (SLOVAK Republic)		6855	SK-TELEKOMSK	false
42.158.0.116	unknown	China		23724	CHINANET-IDC-BJ-APIDCChinaTelecommunicationsCorporation	false
47.99.216.219	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
97.255.238.3	unknown	United States		6167	CELLCO-PARTUS	false
59.135.45.170	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
151.113.209.16	unknown	United States		32480	LLUMCUS	false
160.14.239.102	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.107.156.189	unknown	United States		10507	SPCSUS	false
102.41.18.1	unknown	Egypt		8452	TE-ASTE-ASEG	false
202.60.208.210	unknown	India		17887	TCCT-AS-TH-APTCCTechnologyCoLtdTH	false
81.141.43.67	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
122.80.176.49	unknown	China		45069	CNNIC-CTTSDNET-APchinatietongShandongnetCN	false
106.142.62.27	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
65.99.176.84	unknown	Sweden		12552	IPO-EUSE	false
69.246.125.219	unknown	United States		7922	COMCAST-7922US	false
189.108.118.15	unknown	Brazil		10429	TELEFONICABRASILSABR	false
208.141.122.100	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
43.57.106.104	unknown	Japan		4249	LILLY-ASUS	false
140.216.248.67	unknown	United States		22284	AS22284-DOI-OPSUS	false
77.19.124.125	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
165.135.45.215	unknown	United States		25969	SLUUS	false
208.172.77.62	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
24.163.25.235	unknown	United States		11426	TWC-11426-CAROLINASUS	false
209.171.79.45	unknown	Canada		852	ASN852CA	false
164.148.222.130	unknown	South Africa		37130	SITA-ASZA	false
42.54.33.64	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
62.145.208.64	unknown	Netherlands		33915	TNF-ASNL	false
86.78.14.120	unknown	France		15557	LDCOMNETFR	false
154.5.79.172	unknown	Canada		852	ASN852CA	false
124.178.212.173	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
189.200.238.163	unknown	Mexico		13591	MexicoReddeTelecomunicacionesSdeRLdeCVMX	false
59.97.9.183	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
140.216.248.79	unknown	United States		22284	AS22284-DOI-OPSUS	false
47.114.175.33	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
78.167.178.250	unknown	Turkey		9121	TTNETTR	false
92.191.124.48	unknown	France		12479	UNI2-ASES	false
110.7.174.174	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
97.222.195.129	unknown	United States		6167	CELLCO-PARTUS	false
14.151.85.3	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
188.171.41.176	unknown	Spain		12946	TELECABLESpainES	false
178.84.162.7	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
190.74.137.138	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
65.126.38.78	unknown	United States		27235	CVC-INET-33US	false
195.58.81.253	unknown	United Kingdom		3253	SOVINTEL-EF-ASRU	false
60.195.61.224	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
181.221.212.94	unknown	Brazil		28573	CLAROSABR	false
177.240.1.145	unknown	Mexico		13999	MegaCableSAdeCVMX	false
196.145.176.55	unknown	Egypt		36935	Vodafone-EG	false
201.20.214.34	unknown	Brazil		19182	TELEFONICABRASILSABR	false
62.7.14.167	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
37.212.134.4	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.134.95.156	unknown	Ireland		62129	WIRELESSCONNECT16IE	false
146.156.108.122	unknown	United States		197938	TRAVIANGAMESDE	false
201.166.102.57	unknown	Mexico		28554	CablemasTelecomunicacionesSAdeCVMX	false
209.172.239.10	unknown	United States		393289	MERCERU-GA-ASNUS	false
115.217.129.91	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
221.83.91.98	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
125.155.165.128	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
72.6.32.97	unknown	United States		10507	SPCSUS	false
65.237.2.35	unknown	United States		701	UUNETUS	false
126.89.139.234	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
54.57.245.158	unknown	United States		14618	AMAZON-AESUS	false
138.7.41.166	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
174.5.6.12	unknown	Canada		6327	SHAWCA	false
37.212.246.177	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
193.205.119.146	unknown	Italy		137	ASGARRConsortiumGARREU	false
108.54.61.41	unknown	United States		701	UUNETUS	false
89.200.164.210	unknown	Poland		50231	SYRION-ASPL	false
91.220.198.150	unknown	Ukraine		50304	BLIXNO	false
216.254.75.229	unknown	United States		18566	MEGAPATH5-US	false

Runtime Messages

Command:	/tmp/e9e6i5D2gK
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infection Complete
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.136.200.219	nUDLlJvoP4	Get hash	malicious	Browse	
111.43.58.28	Cloud.x86	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
T-MOBILE-AS21928US	eGH4d5FDoU	Get hash	malicious	Browse	• 100.237.194.109
	hz4vFpTJb8	Get hash	malicious	Browse	• 100.205.236.190
	ecuuS2WNmQ	Get hash	malicious	Browse	• 100.237.194.120
	Yoshi.arm-20211110-0350	Get hash	malicious	Browse	• 100.249.24.191
	pt7DJSPfna	Get hash	malicious	Browse	• 100.165.215.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	x86-20211110-0150	Get hash	malicious	Browse	• 172.40.223.248
	sora.arm	Get hash	malicious	Browse	• 162.167.18.159
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 100.167.216.94
	v9o2vinbUj	Get hash	malicious	Browse	• 162.188.24.4
	QaCRsRGMyb	Get hash	malicious	Browse	• 172.45.144.106
	mips	Get hash	malicious	Browse	• 100.159.221.63
	x86_64	Get hash	malicious	Browse	• 100.136.50.181
	arm	Get hash	malicious	Browse	• 100.209.185.150
	arm6	Get hash	malicious	Browse	• 100.169.104.120
	arm5	Get hash	malicious	Browse	• 172.57.247.170
	qgxgn5fQU1	Get hash	malicious	Browse	• 100.194.13.115
	4DrtSJOLjr	Get hash	malicious	Browse	• 100.221.227.84
	O4aHLhCviL	Get hash	malicious	Browse	• 162.166.121.41
	ZvUGMRqJrx	Get hash	malicious	Browse	• 100.136.32.111
	gFn4iz8ygL	Get hash	malicious	Browse	• 172.38.84.49
ATT-INTERNET4US	Smlp3eBtOI	Get hash	malicious	Browse	• 172.10.171.154
	hz4vFpTJb8	Get hash	malicious	Browse	• 76.234.112.5
	ecuuS2WNmQ	Get hash	malicious	Browse	• 76.230.10.117
	0LuSWzDmJG	Get hash	malicious	Browse	• 12.107.165.35
	cdglTQfNsE	Get hash	malicious	Browse	• 207.242.171.242
	P8xpl5R93m	Get hash	malicious	Browse	• 74.165.58.233
	Yoshi.arm7-20211110-0350	Get hash	malicious	Browse	• 68.250.23.55
	Yoshi.x86-20211110-0350	Get hash	malicious	Browse	• 32.143.225.66
	Yoshi.arm-20211110-0350	Get hash	malicious	Browse	• 13.190.212.110
	pt7DJSPfna	Get hash	malicious	Browse	• 104.52.162.167
	zD1jpTbFQq	Get hash	malicious	Browse	• 208.61.202.33
	fNrSUTMJ8O	Get hash	malicious	Browse	• 107.67.24.167
	2tdWqgPQPc	Get hash	malicious	Browse	• 45.31.65.7
	NMhjdmrpZi	Get hash	malicious	Browse	• 45.21.76.243
	8wdtrqd3z0	Get hash	malicious	Browse	• 161.133.158.108
	arm7	Get hash	malicious	Browse	• 99.179.58.217
	x86-20211110-0150	Get hash	malicious	Browse	• 99.116.100.236
	sora.x86	Get hash	malicious	Browse	• 69.231.146.173
	x86	Get hash	malicious	Browse	• 199.106.35.19
	KKveTTgaAAsecNNaaaa.arm7	Get hash	malicious	Browse	• 166.74.232.253
SOFTLAYERUS	zD1jpTbFQq	Get hash	malicious	Browse	• 169.44.187.157
	KKveTTgaAAsecNNaaaa.arm7	Get hash	malicious	Browse	• 161.156.204.166
	byxEpar5Zm	Get hash	malicious	Browse	• 74.52.194.190
	s4Qw9YZtjr	Get hash	malicious	Browse	• 169.62.101.102
	YG9KkTTAgE	Get hash	malicious	Browse	• 174.133.70.200
	fCca2FJVXG	Get hash	malicious	Browse	• 161.157.130.250
	QLPxrFlfKm	Get hash	malicious	Browse	• 184.172.192.163
	y2NMF6ulOl	Get hash	malicious	Browse	• 37.58.70.148
	8krBRiWrtG	Get hash	malicious	Browse	• 67.228.47.243
	IYcCOLfGT7	Get hash	malicious	Browse	• 70.87.143.51
	lBOsC9VNlS.exe	Get hash	malicious	Browse	• 173.192.101.24
	F0ihkIMDf2	Get hash	malicious	Browse	• 108.229.93.142
	rMwxCtXmuJ	Get hash	malicious	Browse	• 169.50.39.255
	uV1rj8v43F	Get hash	malicious	Browse	• 159.122.175.32
	BBVA TT Swift copy_pdf.exe	Get hash	malicious	Browse	• 141.125.107.247
	BL-NO ASIAN SHIPPINGS DOCUMENTS.exe	Get hash	malicious	Browse	• 172.94.88.26
	NEaRhAVeo9	Get hash	malicious	Browse	• 150.239.179.14
	ApuXjs7iJm	Get hash	malicious	Browse	• 163.102.93.91
	x86-20211103-0152	Get hash	malicious	Browse	• 184.172.25.16
	sora.x86	Get hash	malicious	Browse	• 74.52.52.108
WESTNET-AS-APWestnetInternetServicesAU	eVtKZt4DLL	Get hash	malicious	Browse	• 202.72.165.66
	cNqgk3ITHS	Get hash	malicious	Browse	• 202.72.177.76

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/run/user/127/dconf/user	
Process:	/usr/bin/gnome-shell
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	93B885ADFE0DA089CDF634904FD59F71
SHA1:	5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F
SHA-256:	6E340B9CFFB37A989CA544E6BB780A2C78901D3FB33738768511A30617AFA01D
SHA-512:	B8244D028981D693AF7B456AF8EFA4CAD63D282E19FF14942C246E50D9351D22704A802A71C3580B6370DE4CEB293C324A8423342557D4E5C38438F0E36910EE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

/run/user/127/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:JTRv:dRv
MD5:	001AF7FCE807A04B01A6D4F444BCE851
SHA1:	FB829727ACF9FCE78B2587C8701338FC2B72EF60
SHA-256:	E3DF6FAF134949E7A0D832010616C793673BCAEED43CED709192821F43F7F802
SHA-512:	2B6042C3FB473A2DEABEDD426B92324958562B3F0B57F7E80160AAD67A2D53A0FBD2455EF73BCC21AB5C43D82BEE8AAA95176D28ADE7D617F45629DCEEB40DFD
Malicious:	false
Reputation:	low
Preview:	5964.

/tmp/server-0.xkm	
Process:	/usr/bin/xkbcomp
File Type:	Compiled XKB Keymap: lsb, version 15
Category:	dropped
Size (bytes):	12060
Entropy (8bit):	4.8492493153178975
Encrypted:	false
SSDEEP:	192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ
MD5:	B4E3EB0B8B6B0FC1F46740C573E18D86
SHA1:	7D35426357695EBA77850757E8939A62DCEFF2D1
SHA-256:	7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91
SHA-512:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE01
Malicious:	false
Reputation:	moderate, very likely benign file

/tmp/server-0.xkm	
Preview:	.mkx.....D.....h.....<.....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWNPGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFINDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18

/var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0	
Process:	/usr/bin/ibus-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.120221325120518
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWeKMQA+TThI:q5sU3LWfLUDmQymqSFbfomSMWTW1f/
MD5:	EF9D47DB809E4A72602AE05FF9154952
SHA1:	999217CDBDDBD6D7DFFE58C1A1F603E6EC76E0DB
SHA-256:	4E6609F5DBB529CD3F02071B7DA51184F9E5003EB312AFB64442FEAA8DDED4A6
SHA-512:	FADD76CF2CE8CE283872B1B7DE65DC76F26E7B53F8D857378918D5F72D55EBCD7347AE8249C46FD6BE7AE1A08143788FD9CEAC27DE722C21CA683033D30A450
Malicious:	false
Reputation:	low
Preview:	# This file is created by ibus-daemon, please do not modify it..# This file allows processes on the machine to find the.# ibus session bus with the below address..# If the IBUS_ADDRESS environment variable is set, it will.# be used rather than this file..IBUS_ADDRESS=unix:abstract=/var/lib/gdm3/.cache/ibus/dbus-ImJPr8Do,guid=43ab00510e7c1d3ad6b31d2d618b7b28.IBUS_DAEMON_PID=5601.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.415455824329945
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	e9e6i5D2gK
File size:	165996
MD5:	8dee5c2c55c632ccbe516521e2e18dc2
SHA1:	a4a8530f05f8c37ab7854cd82bd6179828dc5b50
SHA256:	0b1a02f1009fda9597fe19726b1c7d83310dbdbab7d9193490e27dfbb515b9c3
SHA512:	35c234d0726874c248212f169707935a27824903ded627826b20a0ad8cee85d675217add0810f13b911918fc6016cd5f115de4f3f7cb02caec0eb4baf139ca84
SSDEEP:	3072:EreZxuDQVJEeDn4nyLEvAVEsaRTSVj5/aSgPfJN22wH:1ZxGQVGOEvAVEsaRTSVj5/aSg3e2wH
File Content Preview:	.ELF.....@.`...4...d....4. ...(.....@...@....t...t.....F...F.....dt.Q.....<...'....I'.....<...'.....I.. ....'9... .....<...'.....!.....'9U

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	165476
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

Sections

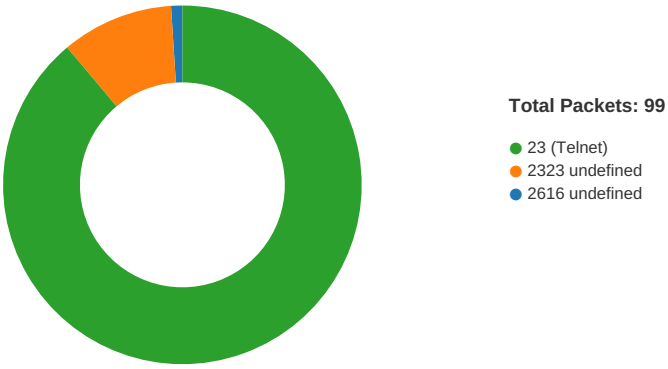
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x254d0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x4255f0	0x255f0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x425650	0x25650	0x1e30	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x468000	0x28000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x468008	0x28008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x468020	0x28020	0x258	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x468280	0x28280	0x38c	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x46860c	0x2860c	0x20	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x468630	0x2860c	0x9a8	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x666	0x2860c	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x2860c	0x57	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	0x27480	0x27480	3.5070	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x28000	0x468000	0x468000	0x60c	0xfd8	2.7591	0x6	RW	0x10000		.ctors .dtors .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: e9e6i5D2gK PID: 5240 Parent PID: 5116

General

Start time:	07:54:57
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	/tmp/e9e6i5D2gK
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: e9e6i5D2gK PID: 5242 Parent PID: 5240

General

Start time:	07:54:57
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a

File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: e9e6i5D2gK PID: 5243 Parent PID: 5240

General

Start time:	07:54:57
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: e9e6i5D2gK PID: 5246 Parent PID: 5243

General

Start time:	07:54:57
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: e9e6i5D2gK PID: 5284 Parent PID: 5246

General

Start time:	07:56:01
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: e9e6i5D2gK PID: 5316 Parent PID: 5246

General

Start time:	07:56:17
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: e9e6i5D2gK PID: 5723 Parent PID: 5246

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: e9e6i5D2gK PID: 6244 Parent PID: 5246

General

Start time:	07:57:00
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: e9e6i5D2gK PID: 5247 Parent PID: 5243

General

Start time:	07:54:57
Start date:	10/11/2021
Path:	/tmp/e9e6i5D2gK
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: gnome-session-binary PID: 5292 Parent PID: 1477

General

Start time:	07:56:11
Start date:	10/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5292 Parent PID: 1477

General

Start time:	07:56:11
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gnome-shell PID: 5292 Parent PID: 1477

General

Start time:	07:56:11
Start date:	10/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	/usr/bin/gnome-shell
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-shell PID: 5601 Parent PID: 5292

General

Start time:	07:56:23
Start date:	10/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5601 Parent PID: 5292

General

Start time:	07:56:23
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	ibus-daemon --panel disable --xim
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5606 Parent PID: 5601

General

Start time:	07:56:24
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5606 Parent PID: 5601

General

Start time:	07:56:24
Start date:	10/11/2021
Path:	/usr/libexec/ibus-memconf
Arguments:	/usr/libexec/ibus-memconf
File size:	22904 bytes
MD5 hash:	523e939905910d06598e66385761a822

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5608 Parent PID: 5601

General

Start time:	07:56:24
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5609 Parent PID: 5608

General

Start time:	07:56:24
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5609 Parent PID: 1

General

Start time:	07:56:24
Start date:	10/11/2021
Path:	/usr/libexec/ibus-x11
Arguments:	/usr/libexec/ibus-x11 --kill-daemon
File size:	100352 bytes
MD5 hash:	2aa1e54666191243814c2733d6992dbd

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5983 Parent PID: 5601

General

Start time:	07:56:45
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-engine-simple PID: 5983 Parent PID: 5601

General

Start time:	07:56:45
Start date:	10/11/2021
Path:	/usr/libexec/ibus-engine-simple

Arguments:	/usr/libexec/ibus-engine-simple
File size:	14712 bytes
MD5 hash:	0238866d5e8802a0ce1b1b9af8cb1376

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5322 Parent PID: 1

General

Start time:	07:56:23
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5322 Parent PID: 1

General

Start time:	07:56:23
Start date:	10/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

File Activities

File Read

Analysis Process: dbus-daemon PID: 5611 Parent PID: 5610

General

Start time:	07:56:24
Start date:	10/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: ibus-portal PID: 5611 Parent PID: 5610

General

Start time:	07:56:24

Start date:	10/11/2021
Path:	/usr/libexec/ibus-portal
Arguments:	/usr/libexec/ibus-portal
File size:	92536 bytes
MD5 hash:	562ad55bd9a4d54bd7b76746b01e37d3

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5641 Parent PID: 1

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: upowerd PID: 5641 Parent PID: 1

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/usr/lib/upower/upowerd
Arguments:	/usr/lib/upower/upowerd
File size:	260328 bytes
MD5 hash:	1253eea2fe5fe4017069664284e326cd

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: Xorg PID: 5719 Parent PID: 1465

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5719 Parent PID: 1465

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5720 Parent PID: 5719

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5720 Parent PID: 5719

General

Start time:	07:56:28
Start date:	10/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: systemd PID: 5728 Parent PID: 1

General

Start time:	07:56:31
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5728 Parent PID: 1

General

Start time:	07:56:31
Start date:	10/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 5732 Parent PID: 5728

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 5732 Parent PID: 5728

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: language-validate PID: 5733 Parent PID: 5732

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5733 Parent PID: 5732

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 5734 Parent PID: 5733

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5734 Parent PID: 5733

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5735 Parent PID: 5734

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5735 Parent PID: 5734

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5736 Parent PID: 5734

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5736 Parent PID: 5734

General

Start time:	07:56:32
Start date:	10/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5737 Parent PID: 1

General

Start time:	07:56:36
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5737 Parent PID: 1

General

Start time:	07:56:36
Start date:	10/11/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5955 Parent PID: 5954

General

Start time:	07:56:37
Start date:	10/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: gjs PID: 5955 Parent PID: 5954

General

Start time:	07:56:37
Start date:	10/11/2021
Path:	/usr/bin/gjs
Arguments:	/usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
File size:	23128 bytes
MD5 hash:	5f3eceb792bb65c22f23d1efb4fde3ad

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5964 Parent PID: 1334

General

Start time:	07:56:39
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5964 Parent PID: 1334

General

Start time:	07:56:39
Start date:	10/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5999 Parent PID: 1

General

Start time:	07:56:52
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 5999 Parent PID: 1

General

Start time:	07:56:52
Start date:	10/11/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84

File Activities

File Read

Directory Enumerated