ID: 679599
Sample Name: l9Tu5ojqkF
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:39:06
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

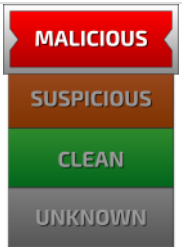
l9Tu5ojqkF

Overview

General Information

Sample Name:	l9Tu5ojqkF
Analysis ID:	679599
MD5:	f1c2cf0a5213d5b..
SHA1:	0dfc8ff630f6da9…
SHA256:	205418de2ec316..
Tags:	32 elf intel mirai
Infos:	

Detection



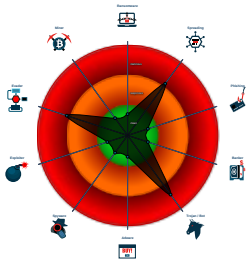
Mirai

Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample deletes itself
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Sample tries to kill multiple process…
- Connects to many ports of the same…
- Yara signature match
- Sample has stripped symbol table
- Enumerates processes within the "p…

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679599
Start date and time: 06/08/202203:39:06	2022-08-06 03:39:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	l9Tu5ojqkF
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.spre.troj.evad.lin@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/l9Tu5ojqkF
PID:	6229
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	gosh that chinese family at the other table sure ate a lot
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- l9Tu5ojqkF (PID: 6229, Parent: 6124, MD5: f1c2cf0a5213d5b79aab8902d0b8c9a2) Arguments: /tmp/l9Tu5ojqkF
  - l9Tu5ojqkF New Fork (PID: 6230, Parent: 6229)
    - l9Tu5ojqkF New Fork (PID: 6231, Parent: 6230)
    - l9Tu5ojqkF New Fork (PID: 6232, Parent: 6230)
    - l9Tu5ojqkF New Fork (PID: 6233, Parent: 6230)
- gvfsd-fuse New Fork (PID: 6253, Parent: 1860)
- fusermount (PID: 6253, Parent: 1860, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- gnome-session-binary New Fork (PID: 6265, Parent: 1477)
- sh (PID: 6265, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
- gsd-wacom (PID: 6265, Parent: 1477, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 6267, Parent: 1477)
- sh (PID: 6267, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
- gsd-keyboard (PID: 6267, Parent: 1477, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 6268, Parent: 1477)
- sh (PID: 6268, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
- gsd-color (PID: 6268, Parent: 1477, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 6269, Parent: 1477)
- sh (PID: 6269, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
- gsd-print-notifications (PID: 6269, Parent: 1477, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
- gnome-session-binary New Fork (PID: 6270, Parent: 1477)
- sh (PID: 6270, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
- gsd-rfkill (PID: 6270, Parent: 1477, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6271, Parent: 1477)
- sh (PID: 6271, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
- gsd-smartcard (PID: 6271, Parent: 1477, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6274, Parent: 1477)
- sh (PID: 6274, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
- gsd-datetime (PID: 6274, Parent: 1477, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6275, Parent: 1477)
- sh (PID: 6275, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
- gsd-screensaver-proxy (PID: 6275, Parent: 1477, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6276, Parent: 1477)
- sh (PID: 6276, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
- gsd-a11y-settings (PID: 6276, Parent: 1477, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6277, Parent: 1477)
- sh (PID: 6277, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
- gsd-sound (PID: 6277, Parent: 1477, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6278, Parent: 1477)
- sh (PID: 6278, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
- gsd-power (PID: 6278, Parent: 1477, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6279, Parent: 1477)
- sh (PID: 6279, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 6279, Parent: 1477, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6281, Parent: 1477)
- sh (PID: 6281, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
- gsd-media-keys (PID: 6281, Parent: 1477, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
l9Tu5ojqkF	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x37f0:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3
l9Tu5ojqkF	Linux_Trojan_Mirai_88de437f	unknown	unknown	• 0x7032:$a: 24 08 8B 4C 24 04 85 D2 74 0D 31 C0 89 F6 C6 04 08 00 40 39 D0
l9Tu5ojqkF	Linux_Trojan_Mirai_cc93863b	unknown	unknown	• 0x8901:$a: C3 57 8B 44 24 0C 8B 4C 24 10 8B 7C 24 08 F3 AA 8B 44 24 08
l9Tu5ojqkF	Linux_Trojan_Mirai_8aa7b5d3	unknown	unknown	• 0x7002:$a: 8B 4C 24 14 8B 74 24 0C 8B 5C 24 10 85 C9 74 0D 31 D2 8A 04 1A 88

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
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x37f0:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_88de437f	unknown	unknown	• 0x7032:$a: 24 08 8B 4C 24 04 85 D2 74 0D 31 C0 89 F6 C6 04 08 00 40 39 D0
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_cc93863b	unknown	unknown	• 0x8901:$a: C3 57 8B 44 24 0C 8B 4C 24 10 8B 7C 24 08 F3 AA 8B 44 24 08
6229.1.0000000008048000.0000000008056000.r-x.sdmp	Linux_Trojan_Mirai_8aa7b5d3	unknown	unknown	• 0x7002:$a: 8B 4C 24 14 8B 74 24 0C 8B 5C 24 10 85 C9 74 0D 31 D2 8A 04 1A 88

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Networking

- Uses known network protocols on non-standard ports
- Connects to many ports of the same IP (likely port scanning)

System Summary

- Malicious sample detected (through community Yara rule)
- Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection

- Sample deletes itself
- Uses known network protocols on non-standard ports

Stealing of Sensitive Information

- Yara detected Mirai

Remote Access Functionality

- Yara detected Mirai

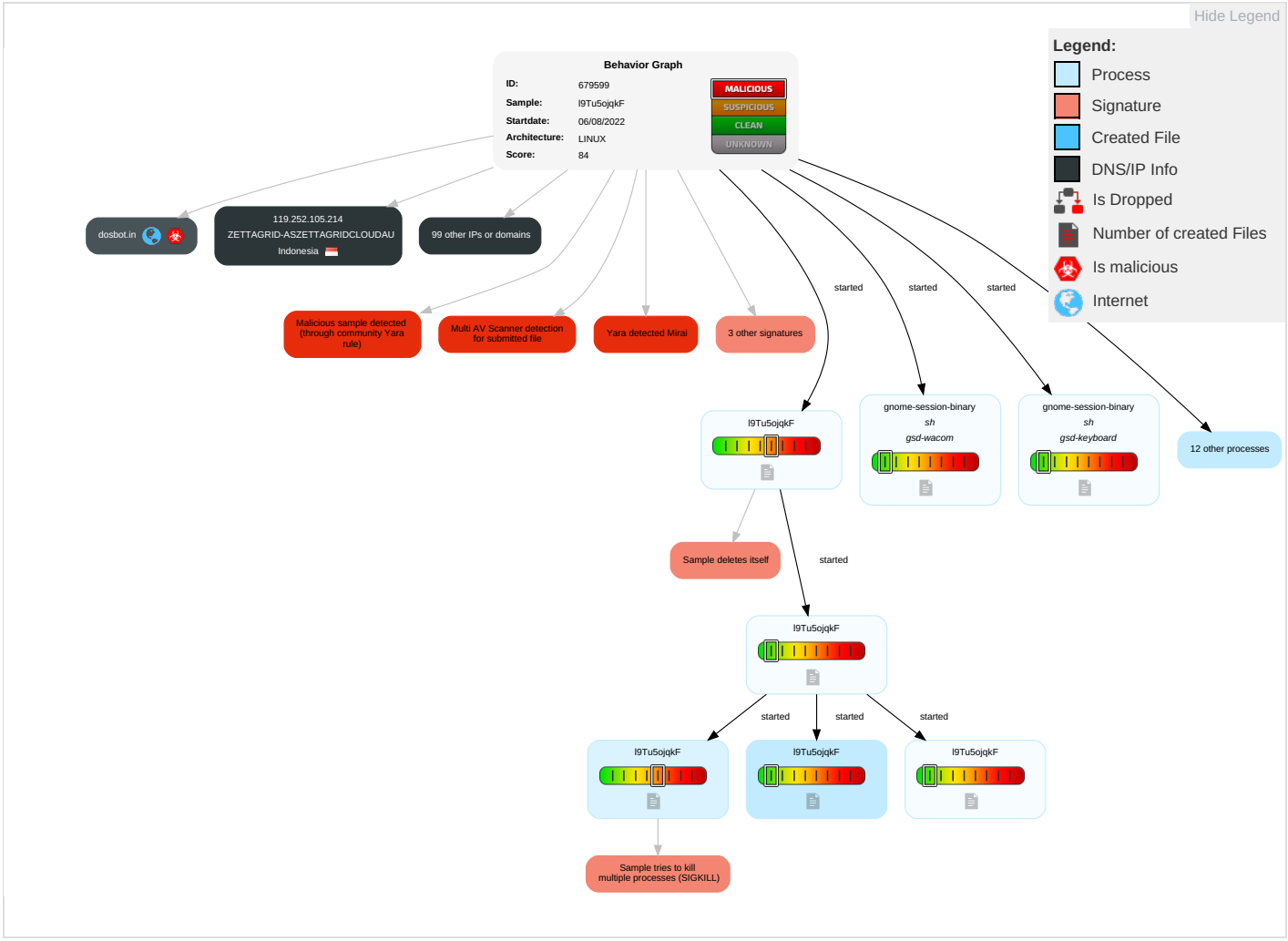
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 File Deletion	1 OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
l9Tu5ojqkF	17%	Virustotal		Browse
l9Tu5ojqkF	35%	ReversingLabs	Linux.Trojan.Mirai	
l9Tu5ojqkF	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

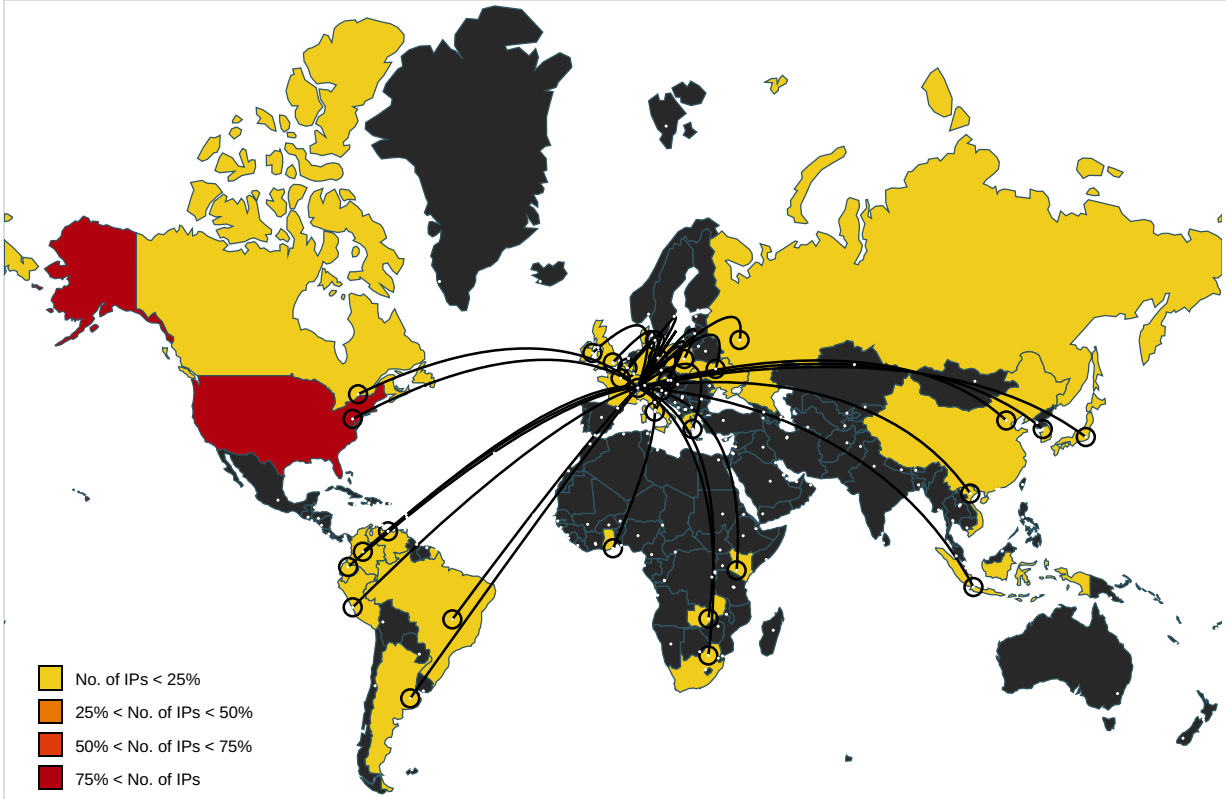
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dosbot.in	204.76.203.200	true	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.41.162.207	unknown	United States		53984	AS-WELLSTARUS	false
45.214.204.94	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
172.59.43.143	unknown	United States		21928	T-MOBILE-AS21928US	false
209.125.69.222	unknown	United States		7029	WINDSTREAMUS	false
85.172.132.72	unknown	Russian Federation		42362	ALANIA-ASBranchformerSevosetinelectrosvyazRU	false
50.36.161.17	unknown	United States		5650	FRONTIER-FRTRUS	false
35.234.44.34	unknown	United States		15169	GOOGLEUS	false
8.118.171.38	unknown	United States		3356	LEVEL3US	false
23.199.141.139	unknown	United States		16625	AKAMAI-ASUS	false
74.178.142.93	unknown	United States		10796	TWC-10796-MIDWESTUS	false
128.255.101.196	unknown	United States		3676	UIOWA-ASUS	false
88.81.208.172	unknown	Russian Federation		28947	INTURAL-ASZAOInTRU	false
207.71.175.212	unknown	United States		26962	IPROTUS	false
27.8.88.225	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
107.137.239.203	unknown	United States		7018	ATT-INTERNET4US	false
130.128.123.168	unknown	United States		6908	DATAHOPDatahop-SixDegreesGB	false
188.4.85.131	unknown	Greece		1241	FORTHNET-GRForthnetEU	false
170.199.89.73	unknown	Canada		7122	MTS-ASNCA	false
200.3.101.67	unknown	Argentina		26594	PampaEnergiaSAAR	false
73.121.196.54	unknown	United States		7922	COMCAST-7922US	false
178.10.156.216	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
90.9.150.175	unknown	France		3215	FranceTelecom-OrangeFR	false
185.65.193.11	unknown	Germany		60294	DE-DGWDeutscheGlasfaserWholesaleInternetDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.190.45.51	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
143.84.43.254	unknown	United States		1541	DNIC-ASBLK-01534-01546US	false
205.195.40.155	unknown	Canada		3356	LEVEL3US	false
12.94.212.208	unknown	United States		7018	ATT-INTERNET4US	false
138.30.225.103	unknown	Japan		600	OARNET-ASUS	false
126.120.51.101	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
113.181.189.136	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
27.218.74.150	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
80.166.215.172	unknown	Denmark		3292	TDCTDCASDK	false
74.178.142.77	unknown	United States		10796	TWC-10796-MIDWESTUS	false
159.165.234.197	unknown	United States		34058	LIFECELL-ASUA	false
205.5.170.254	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
171.43.3.29	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.212.254.30	unknown	Venezuela		6306	TELEFONICAVENEZOLANACAVE	false
89.16.77.146	unknown	Ireland		35226	RIPPLECOM-ASIE	false
24.50.201.21	unknown	United States		14638	LCPRLUS	false
184.31.203.167	unknown	United States		16625	AKAMAI-ASUS	false
151.86.44.166	unknown	Italy		8217	ASN-ENIIT	false
105.58.216.33	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
76.106.206.56	unknown	United States		7922	COMCAST-7922US	false
64.192.180.152	unknown	United States		33548	UNWIRED-NOCUS	false
73.220.65.71	unknown	United States		7922	COMCAST-7922US	false
141.189.61.166	unknown	United States		17011	PPG-INDUSTRIESUS	false
17.115.203.104	unknown	United States		714	APPLE-ENGINEERINGUS	false
99.67.41.6	unknown	United States		7018	ATT-INTERNET4US	false
154.160.107.230	unknown	Ghana		30986	SCANCOMGH	false
181.251.166.89	unknown	Colombia		26611	COMCELSACO	false
165.33.173.234	unknown	United States		37053	RSAWEB-ASZA	false
44.154.12.68	unknown	United States		62383	LDS-ASBE	false
131.100.166.66	unknown	Brazil		61642	NEXNETTBrasilTelecomBR	false
222.49.214.7	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
92.48.138.37	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
93.103.14.35	unknown	Slovenia		34779	T-2-ASASsetpropagatedbyT-2dooSI	false
83.26.204.58	unknown	Poland		5617	TPNETPL	false
103.29.16.192	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
72.17.245.29	unknown	United States		7029	WINDSTREAMUS	false
61.25.66.236	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
34.19.186.176	unknown	United States		2686	ATGS-MMD-ASUS	false
122.81.86.82	unknown	China		45069	CNNIC-CTTSDNET-APchinatietongShandongnetCN	false
207.198.230.50	unknown	United States		23395	ELIASSPORTSBUREAUUS	false
216.98.234.182	unknown	United States		19092	360NETWORKS-US	false
108.151.82.229	unknown	United States		16509	AMAZON-02US	false
102.141.251.99	unknown	South Africa		327962	PacketSkyZA	false
136.110.180.165	unknown	United States		60311	ONEFMCH	false
2.41.35.65	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
82.33.237.171	unknown	United Kingdom		5089	NTLGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.47.114.84	unknown	United States		3	MIT-GATEWAYSUS	false
184.192.155.45	unknown	United States		10507	SPCSUS	false
5.252.139.146	unknown	Switzerland		49065	SECTRASE	false
80.109.54.101	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
190.116.77.86	unknown	Peru		12252	AmericaMovilPeruSACPE	false
194.82.57.84	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
97.163.77.57	unknown	United States		6167	CELLCO-PARTUS	false
195.216.74.4	unknown	Switzerland		16242	MHSCH	false
190.214.187.34	unknown	Ecuador		28006	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEPEC	false
67.147.254.212	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
199.147.142.240	unknown	United States		4152	USDA-1US	false
167.122.56.51	unknown	United States		19275	INTERVALUS	false
123.131.27.94	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
143.111.250.206	unknown	United States		11773	UTMDACCUS	false
141.230.57.184	unknown	United States		12701	BARCAPLondonGB	false
99.250.224.169	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
120.163.149.157	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
211.119.126.230	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
121.180.7.191	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
195.164.130.154	unknown	Poland		204679	OSEPL	false
118.14.9.168	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
18.237.164.108	unknown	United States		16509	AMAZON-02US	false
35.84.6.3	unknown	United States		237	MERIT-AS-14US	false
96.150.105.243	unknown	United States		7922	COMCAST-7922US	false
213.139.212.68	unknown	Ukraine		208405	SINET-ISP-ASUA	false
52.146.29.9	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.136.249.250	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
193.61.140.181	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
119.252.105.214	unknown	Indonesia		7604	ZETTAGRID-ASZETTAGRIDCLOUDAU	false
162.164.129.230	unknown	United States		21928	T-MOBILE-AS21928US	false
123.215.165.251	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.498860250882768
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	l9Tu5ojqkF
File size:	54556
MD5:	f1c2cf0a5213d5b79aab8902d0b8c9a2
SHA1:	0dfc8ff630f6da90b17477ac261fd74475e0a711
SHA256:	205418de2ec31652223bff945d4ee3e5fe4ce8258346ce755d5d3f8596c2ac47
SHA512:	6dcda86512c630952111dd4cff158b54a116a5fad25454ac3e2fdf9d4fed088335fbd81c9f165258ec3420984a703b111c97c8bfd46532072955da06bf053654
SSDEEP:	1536:pBRuzH5iOE2LhZMvp9MlsqPz+Sj6pP7zjS8:pBgb5iOVZMRQHPKSGVzT
TLSH:	56336BC4A58BD4F5EC1616B124B7B7334B32F43A112DDB87D35DA932BD92A21E24728C
File Content Preview:	.ELF.....d...4...d.....4. ...(.....`...`..@....(.....Q.td.....U..S.....W....h.....[]...$.....U.....= c...t..5.....a.....a.....u.....t....h.P.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	54116
Section Header Size:	40
Number of Section Headers:	11
Header String Table Index:	10

Sections

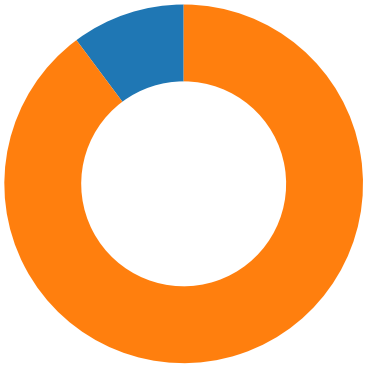
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xbb16	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8053bc6	0xbbc6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8053be0	0xbbe0	0x14fc	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x80560e0	0xd0e0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80560e8	0xd0e8	0x8	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x80560f0	0xd0f0	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8056100	0xd100	0x220	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8056320	0xd320	0x25c0	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xd320	0x43	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	0x8048000	0x8048000	0xd0dc	0xd0dc	6.5406	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xd0e0	0x80560e0	0x80560e0	0x240	0x2800	2.8838	0x6	RW	0x1000		.ctors .dtors .jcr .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 98

- 23 (Telnet)
- 2323 undefined

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 03:39:50.335783958 CEST	192.168.2.23	8.8.8.8	0xea4a	Standard query (0)	dosbot.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 03:39:50.355911970 CEST	8.8.8.8	192.168.2.23	0xea4a	No error (0)	dosbot.in		204.76.203.200	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: l9Tu5ojqkF PID: **6229**, Parent PID: **6124**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/tmp/l9Tu5ojqkF
Arguments:	/tmp/l9Tu5ojqkF
File size:	54556 bytes
MD5 hash:	f1c2cf0a5213d5b79aab8902d0b8c9a2

File Activities

File Deleted

Analysis Process: l9Tu5ojqkF PID: **6230**, Parent PID: **6229**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/tmp/l9Tu5ojqkF
Arguments:	n/a
File size:	54556 bytes
MD5 hash:	f1c2cf0a5213d5b79aab8902d0b8c9a2

Analysis Process: l9Tu5ojqkF PID: **6231**, Parent PID: **6230**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/tmp/l9Tu5ojqkF
Arguments:	n/a
File size:	54556 bytes
MD5 hash:	f1c2cf0a5213d5b79aab8902d0b8c9a2

File Activities

Directory Enumerated

Analysis Process: l9Tu5ojqkF PID: **6232**, Parent PID: **6230**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/tmp/l9Tu5ojqkF
Arguments:	n/a
File size:	54556 bytes
MD5 hash:	f1c2cf0a5213d5b79aab8902d0b8c9a2

File Activities

File Read

Directory Enumerated

Analysis Process: l9Tu5ojqkF PID: **6233**, Parent PID: **6230**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/tmp/l9Tu5ojqkF
Arguments:	n/a
File size:	54556 bytes
MD5 hash:	f1c2cf0a5213d5b79aab8902d0b8c9a2

Analysis Process: gvfsd-fuse PID: **6253**, Parent PID: **1860**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: **6253**, Parent PID: **1860**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

Analysis Process: gnome-session-binary PID: **6265**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6265**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-wacom PID: **6265**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gsd-wacom
Arguments:	/usr/libexec/gsd-wacom
File size:	39520 bytes
MD5 hash:	13778dd1a23a4e94ddc17ac9caa4fcc1

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6267**, Parent PID: **1477**

General

Start time:	03:39:49

Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6267**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-keyboard PID: **6267**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gsd-keyboard
Arguments:	/usr/libexec/gsd-keyboard
File size:	39760 bytes
MD5 hash:	8e288fd17c80bb0a1148b964b2ac2279

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6268**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6268**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-color PID: **6268**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022

Path:	/usr/libexec/gsd-color
Arguments:	/usr/libexec/gsd-color
File size:	92832 bytes
MD5 hash:	ac2861ad93ce047283e8e87cefef9a19

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6269**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6269**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-print-notifications PID: **6269**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6270**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6270**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh

Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-rfkill PID: **6270**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gsd-rfkill
Arguments:	/usr/libexec/gsd-rfkill
File size:	51808 bytes
MD5 hash:	88a16a3c0aba1759358c06215ecfb5cc

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6271**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6271**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-smartcard PID: **6271**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gsd-smartcard
Arguments:	/usr/libexec/gsd-smartcard
File size:	109152 bytes
MD5 hash:	ea1fbd7f62e4cd0331eae2ef754ee605

Analysis Process: gnome-session-binary PID: **6274**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a

File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6274**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-datetime PID: **6274**, Parent PID: **1477**

General

Start time:	03:39:50
Start date:	06/08/2022
Path:	/usr/libexec/gsd-datetime
Arguments:	/usr/libexec/gsd-datetime
File size:	76736 bytes
MD5 hash:	d80d39745740de37d6634d36e344d4bc

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6275**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6275**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-screensaver-proxy PID: **6275**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gsd-screensaver-proxy
Arguments:	/usr/libexec/gsd-screensaver-proxy
File size:	27232 bytes

MD5 hash:	77e309450c87dceee43f1a9e50cc0d02

Analysis Process: gnome-session-binary PID: **6276**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6276**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-a11y-settings PID: **6276**, Parent PID: **1477**

General

Start time:	03:39:50
Start date:	06/08/2022
Path:	/usr/libexec/gsd-a11y-settings
Arguments:	/usr/libexec/gsd-a11y-settings
File size:	23056 bytes
MD5 hash:	18e243d2cf30ecee7ea89d1462725c5c

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6277**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6277**, Parent PID: **1477**

General

Start time:	03:39:49
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-sound PID: **6277**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/usr/libexec/gsd-sound
Arguments:	/usr/libexec/gsd-sound
File size:	31248 bytes
MD5 hash:	4c7d3fb993463337b4a0eb5c80c760ee

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6278**, Parent PID: **1477**

General

Start time:	03:39:50
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6278**, Parent PID: **1477**

General

Start time:	03:39:50
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-power PID: **6278**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/usr/libexec/gsd-power
Arguments:	/usr/libexec/gsd-power
File size:	88672 bytes
MD5 hash:	28b8e1b43c3e7f1db6741ea1ecd978b7

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6279**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6279**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-housekeeping PID: **6279**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6281**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6281**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-media-keys PID: **6281**, Parent PID: **1477**

General

Start time:	03:39:51
Start date:	06/08/2022
Path:	/usr/libexec/gsd-media-keys
Arguments:	/usr/libexec/gsd-media-keys
File size:	232936 bytes
MD5 hash:	a425448c135afb4b8bfd79cc0b6b74da

File Activities

File Read