ID: 679229
Sample Name: Gpaw8cp28X
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 12:34:48
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

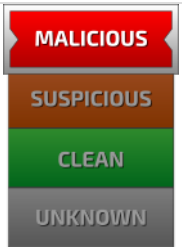
Gpaw8cp28X

Overview

General Information

Sample Name:	Gpaw8cp28X
Analysis ID:	679229
MD5:	06684e4bf9c538..
SHA1:	d883470ae217ce..
SHA256:	2373eac488f891..
Tags:	32 arm elf mirai
Infos:	

Detection



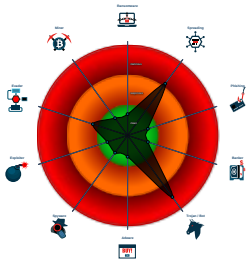
Mirai

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample reads /proc/mounts (often u…
- Connects to many ports of the same…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

All HTTP servers contacted by the sample do not answer. The sample is likely 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.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679229
Start date and time: 05/08/202212:34:48	2022-08-05 12:34:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Gpaw8cp28X
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal72.spre.troj.lin@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/Gpaw8cp28X
PID:	6227
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**
- Gpaw8cp28X (PID: 6227, Parent: 6125, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/Gpaw8cp28X
  - Gpaw8cp28X New Fork (PID: 6230, Parent: 6227)
    - Gpaw8cp28X New Fork (PID: 6232, Parent: 6230)
    - Gpaw8cp28X New Fork (PID: 6233, Parent: 6230)
    - Gpaw8cp28X New Fork (PID: 6236, Parent: 6230)
- gnome-session-binary New Fork (PID: 6261, Parent: 1477)
- sh (PID: 6261, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
- gsd-sharing (PID: 6261, Parent: 1477, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
- gnome-session-binary New Fork (PID: 6263, Parent: 1477)
- sh (PID: 6263, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
- gsd-wacom (PID: 6263, Parent: 1477, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gvfsd-fuse New Fork (PID: 6267, Parent: 1860)
- fusermount (PID: 6267, Parent: 1860, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- 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=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
- gsd-keyboard (PID: 6268, Parent: 1477, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 6273, Parent: 1477)
- sh (PID: 6273, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
- gsd-color (PID: 6273, Parent: 1477, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- 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=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
- gsd-print-notifications (PID: 6276, Parent: 1477, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
- gnome-session-binary New Fork (PID: 6277, Parent: 1477)
- sh (PID: 6277, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
- gsd-rfkill (PID: 6277, Parent: 1477, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6284, Parent: 1477)
- sh (PID: 6284, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
- gsd-smartcard (PID: 6284, Parent: 1477, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6285, Parent: 1477)
- sh (PID: 6285, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
- gsd-datetime (PID: 6285, Parent: 1477, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6286, Parent: 1477)
- sh (PID: 6286, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
- gsd-media-keys (PID: 6286, Parent: 1477, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6287, Parent: 1477)
- sh (PID: 6287, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
- gsd-screensaver-proxy (PID: 6287, Parent: 1477, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6288, Parent: 1477)
- sh (PID: 6288, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
- gsd-a11y-settings (PID: 6288, Parent: 1477, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6289, Parent: 1477)
- sh (PID: 6289, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
- gsd-power (PID: 6289, Parent: 1477, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6290, Parent: 1477)
- sh (PID: 6290, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
- gsd-sound (PID: 6290, Parent: 1477, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6291, Parent: 1477)
- sh (PID: 6291, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 6291, Parent: 1477, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

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

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

Connects to many ports of the same IP (likely port scanning)

System Summary

Sample tries to kill multiple processes (SIGKILL)

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

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

Mitre Att&ck Matrix

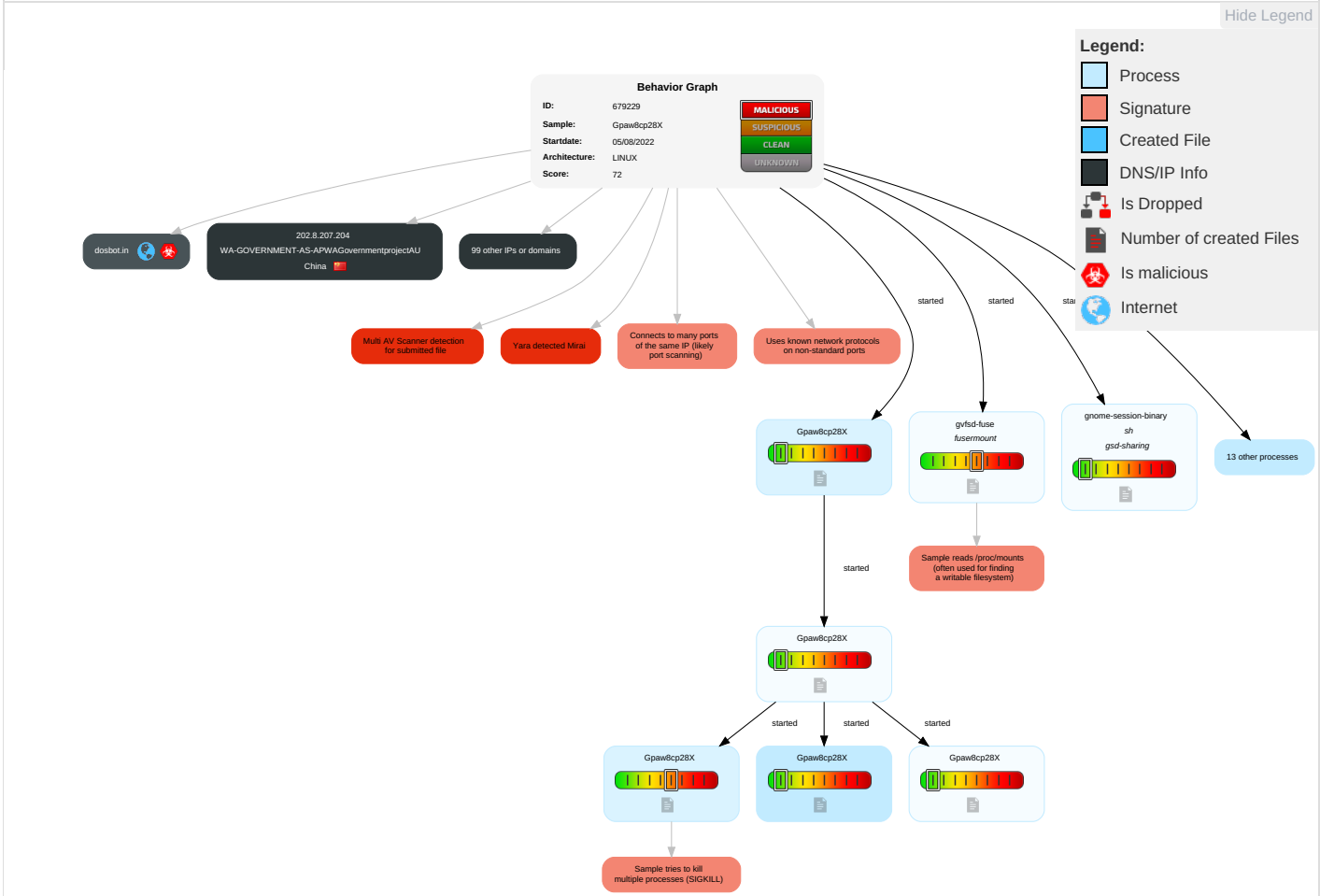
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software 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	1 File and Directory 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
Gpaw8cp28X	24%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

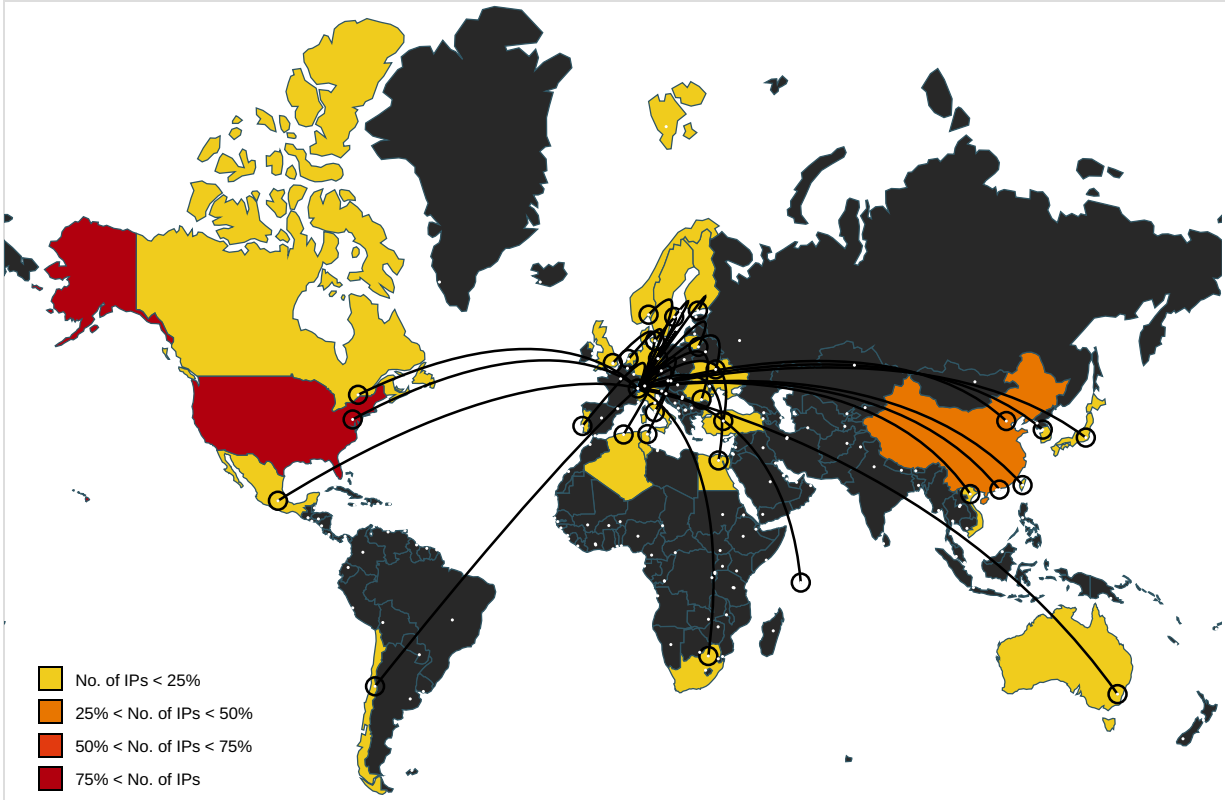
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dosbot.in	107.182.129.240	true	true		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.244.63.176	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
133.82.101.180	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
210.63.26.188	unknown	Taiwan; Republic of China (ROC)		4783	SYSNET-AS1SYSTEXCORPORATIONTW	false
12.76.177.3	unknown	United States		7018	ATT-INTERNET4US	false
13.222.54.118	unknown	United States		16509	AMAZON-02US	false
143.171.203.17	unknown	unknown		16504	GRANITEUS	false
18.236.174.252	unknown	United States		16509	AMAZON-02US	false
182.104.143.167	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
25.198.201.133	unknown	United Kingdom		7922	COMCAST-7922US	false
192.213.135.183	unknown	United States		7127	SCEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.162.164.239	unknown	Denmark		1935	FR-RENATER-LIMOUSINReseauRegionalLimousinEU	false
146.21.111.176	unknown	Sweden		56736	VASTRAGOTALANDSREGIONENSE	false
132.100.154.212	unknown	United States		306	DNIC-ASBLK-00306-00371US	false
204.253.234.226	unknown	United States		701	UUNETUS	false
39.170.106.71	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
197.206.187.55	unknown	Algeria		36947	ALGTEL-ASDZ	false
107.112.85.177	unknown	United States		7018	ATT-INTERNET4US	false
146.225.158.196	unknown	United States		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
48.189.85.175	unknown	United States		2686	ATGS-MMD-ASUS	false
2.237.163.230	unknown	Italy		12874	FASTWEBIT	false
89.214.177.17	unknown	Portugal		42863	MEO-MOVELPT	false
203.247.80.92	unknown	Korea Republic of		10063	KMA-ASKoreaMeteorologicalAdministrationKR	false
133.97.175.104	unknown	Japan		58652	KOCHI-U-NETKochiUniversityJP	false
156.222.254.194	unknown	Egypt		8452	TE-ASTE-ASEG	false
205.45.106.57	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
122.138.197.6	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
76.220.20.215	unknown	United States		7018	ATT-INTERNET4US	false
221.31.66.241	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
113.181.189.131	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
125.226.110.94	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
207.209.111.49	unknown	United States		3300	BTNL	false
121.78.107.93	unknown	Korea Republic of		9286	KINXIDC-AS-KRKINXKR	false
129.125.242.232	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
124.57.94.98	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
97.30.206.110	unknown	United States		22394	CELLCOUS	false
71.52.244.10	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
123.99.85.40	unknown	Korea Republic of		17857	NAKDONGDIGITALBUSANNET-AS-KRTBroadKR	false
118.140.122.229	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
162.47.8.25	unknown	United States		7046	RFC2270-UUNET-CUSTOMERUS	false
94.45.67.208	unknown	Ukraine		47678	SUNLINE-ASUA	false
37.182.218.10	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
210.163.112.160	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
145.218.123.126	unknown	European Union		49362	DSVDK	false
116.97.166.83	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
188.214.21.203	unknown	Romania		20616	GAZDUIRE-ASPierredeCoubertinnr3-5Et2RO	false
222.82.28.66	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
35.75.100.83	unknown	United States		16509	AMAZON-02US	false
187.237.159.132	unknown	Mexico		8151	UninetSAdeCVMX	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
61.31.242.99	unknown	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
218.232.253.32	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
45.200.15.125	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
201.246.248.210	unknown	Chile		7418	TELEFONICACHILESACL	false
160.206.97.255	unknown	Australia		24008	HANSEN-AUHansenTechnologiesDoncasterAU	false
222.172.60.120	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
198.75.152.24	unknown	United States		35350	AS_SCHWARZ_PHARMA_AGAlfred-Nobel-Str10DE	false
196.246.206.187	unknown	South Africa		136384	OPTIX-AS-APOptixPakistanPvtLimitedPK	false
107.242.212.137	unknown	United States		7018	ATT-INTERNET4US	false
70.77.213.149	unknown	Canada		6327	SHAWCA	false
197.43.51.130	unknown	Egypt		8452	TE-ASTE-ASEG	false
144.181.232.194	unknown	Norway		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
102.109.207.12	unknown	Tunisia		37693	TUNISIANATN	false
95.255.100.90	unknown	Italy		3269	ASN-IBSNAZIT	false
25.152.149.205	unknown	United Kingdom		7922	COMCAST-7922US	false
25.19.87.216	unknown	United Kingdom		7922	COMCAST-7922US	false
27.157.84.172	unknown	China		133774	CHINATELECOM-FUJIAN-FUZHOU-IDC1FuzhouCN	false
156.165.92.164	unknown	Egypt		36992	ETISALAT-MISREG	false
84.46.134.233	unknown	Lithuania		15419	LRTC-ASLT	false
169.114.203.114	unknown	United States		37611	AfrihostZA	false
207.63.113.232	unknown	United States		6325	ILLINOIS-CENTURYUS	false
40.253.33.65	unknown	United States		4249	LILLY-ASUS	false
155.148.132.154	unknown	United States		668	DNIC-AS-00668US	false
173.21.73.20	unknown	United States		30036	MEDIACOM-ENTERPRISE-BUSINESSUS	false
80.19.226.209	unknown	Italy		3269	ASN-IBSNAZIT	false
123.242.218.240	unknown	Japan		18092	CSFKyushuTeleCommunicationsCompanyJP	false
211.106.238.201	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
165.212.138.226	unknown	United States		14454	PERIMETER-ESECURITYUS	false
131.151.152.155	unknown	United States		11348	MSTUS	false
143.162.83.130	unknown	United States		8094	PUKNETZA	false
98.31.101.51	unknown	United States		10796	TWC-10796-MIDWESTUS	false
45.86.53.66	unknown	Germany		47787	HASHPOWERPT	false
54.233.71.31	unknown	United States		16509	AMAZON-02US	false
173.133.29.135	unknown	United States		10507	SPCSUS	false
171.196.177.245	unknown	United States		10794	BANKAMERICAUS	false
114.49.23.100	unknown	Japan		37903	EMOBILEYmobileCorporationJP	false
157.196.2.123	unknown	United States		4704	SANNETRakutenMobileIncJP	false
151.178.178.143	unknown	Australia		45025	EDN-ASUA	false
212.213.115.0	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
8.76.213.28	unknown	United States		3356	LEVEL3US	false
168.30.49.104	unknown	United States		3479	PEACHNET-AS1US	false
124.236.254.197	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.231.177.179	unknown	United States		12353	VODAFONE-PTVodafonePortugalPT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
73.136.128.117	unknown	United States		7922	COMCAST-7922US	false
133.207.242.3	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
211.185.174.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
42.57.78.152	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
172.179.36.241	unknown	United States		7018	ATT-INTERNET4US	false
202.8.207.204	unknown	China		136518	WA-GOVERNMENT-AS-APWAGovernmentprojectAU	false
195.227.5.130	unknown	Germany		8469	PIRONETNDH-ASCANCOMPironetAGCoKGDE	false
220.60.94.148	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
182.89.214.58	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.018756052212191
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Gpaw8cp28X
File size:	62728
MD5:	06684e4bf9c538c2a01740b1f88171e7

SHA1:	d883470ae217ceb8cb61d7b36befe8e41703226b
SHA256:	2373eac488f89172263c8ea1d996d74d90803c54762cedf5808f05b9d6d341f1
SHA512:	5e209338e20455ea1ea0c9e4697a2b7313fe3ca1df339eecc919c6f9d32d5b10d20e2eac33bf3773114c2fbd354ee0fa65718dcac0d9d3d73ea15cc007d88651
SSDEEP:	768:qnhYWGFe03XhdftXrq4BVoVGYQqFoLFYBQ1PGt557nN/NPIvvJrM54OgR3zD3Gbu:6uWMewrqH572Yq9Gt5JN8i52P3GC1TW
TLSH:	E4532985BC819A13C5D022BBFB5E418C332663B8D2EE3207DD256F11778B91F0EAB615
File Content Preview:	.ELF...a.....(.....4...P.....4. ...(.....8%.....Q.td.....-...L."...H6.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	62288
Section Header Size:	40
Number of Section Headers:	11
Header String Table Index:	10

Sections

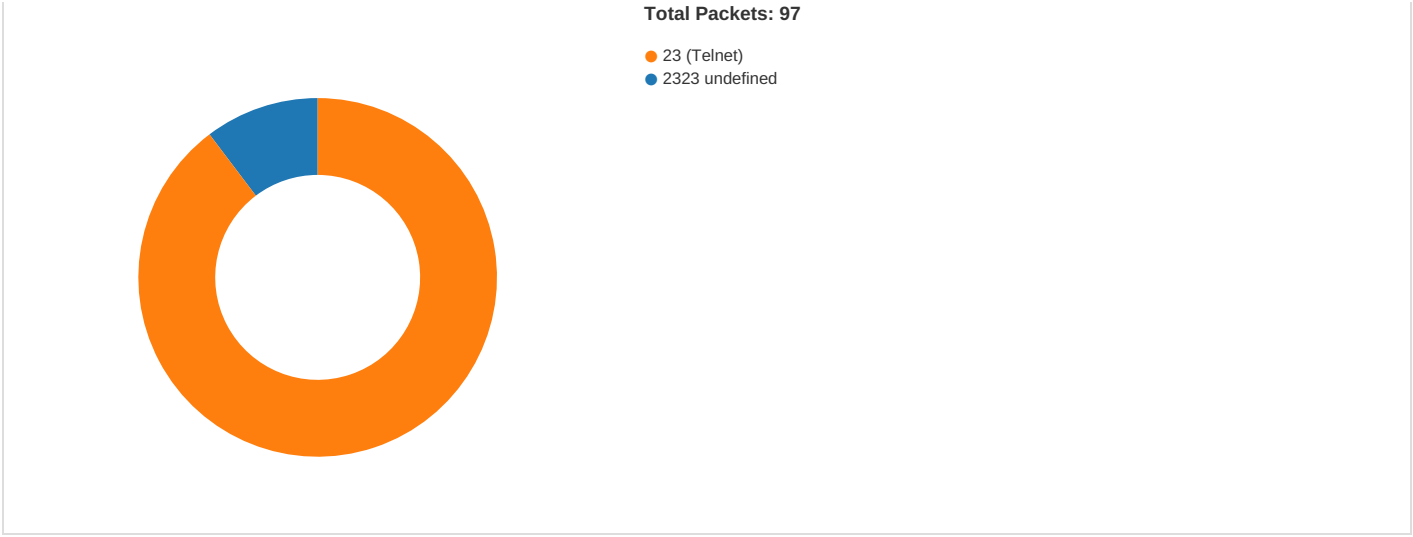
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0xd958	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x15a08	0xda08	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x15a1c	0xda1c	0x1270	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1f000	0xf000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1f008	0xf008	0x8	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x1f010	0xf010	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1f014	0xf014	0x2f8	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1f30c	0xf30c	0x222c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf30c	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	0x8000	0x8000	0xec8c	0xec8c	6.1068	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0xf000	0x1f000	0x1f000	0x30c	0x2538	2.2562	0x6	RW	0x8000		.ctors .dtors .jcr .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 12:35:35.461380959 CEST	192.168.2.23	8.8.8.8	0x72c7	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 5, 2022 12:35:35.483572960 CEST	8.8.8.8	192.168.2.23	0x72c7	No error (0)	dosbot.in		107.182.129.240	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: Gpaw8cp28X PID: **6227**, Parent PID: **6125**

General

Start time:	12:35:34
Start date:	05/08/2022
Path:	/tmp/Gpaw8cp28X
Arguments:	/tmp/Gpaw8cp28X
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Gpaw8cp28X PID: **6230**, Parent PID: **6227**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/tmp/Gpaw8cp28X
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Gpaw8cp28X PID: **6232**, Parent PID: **6230**

General

Start time:	12:35:35

Start date:	05/08/2022
Path:	/tmp/Gpaw8cp28X
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

Directory Enumerated

Analysis Process: Gpaw8cp28X PID: **6233**, Parent PID: **6230**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/tmp/Gpaw8cp28X
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

Directory Enumerated

Analysis Process: Gpaw8cp28X PID: **6236**, Parent PID: **6230**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/tmp/Gpaw8cp28X
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: gnome-session-binary PID: **6261**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6261**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-sharing PID: **6261**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022

Path:	/usr/libexec/gsd-sharing
Arguments:	/usr/libexec/gsd-sharing
File size:	35424 bytes
MD5 hash:	e29d9025d98590fbb69f89fdbd4438b3

Analysis Process: gnome-session-binary PID: **6263**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6263**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
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: **6263**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gsd-wacom
Arguments:	/usr/libexec/gsd-wacom
File size:	39520 bytes
MD5 hash:	13778dd1a23a4e94ddc17ac9caa4fcc1

Analysis Process: gvfsd-fuse PID: **6267**, Parent PID: **1860**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: **6267**, Parent PID: **1860**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

File Activities

File Read

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

General

Start time:	12:35:35
Start date:	05/08/2022
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:	12:35:35
Start date:	05/08/2022
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: **6268**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gsd-keyboard
Arguments:	/usr/libexec/gsd-keyboard
File size:	39760 bytes
MD5 hash:	8e288fd17c80bb0a1148b964b2ac2279

Analysis Process: gnome-session-binary PID: **6273**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6273**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
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: **6273**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
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: **6276**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
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:	12:35:35
Start date:	05/08/2022
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: **6276**, Parent PID: **1477**

General

Start time:	12:35:35
Start date:	05/08/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

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

General

Start time:	12:35:35
Start date:	05/08/2022
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:	12:35:35
Start date:	05/08/2022
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: 6277, Parent PID: 1477

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gsd-rfkill
Arguments:	/usr/libexec/gsd-rfkill
File size:	51808 bytes
MD5 hash:	88a16a3c0aba1759358c06215ecfb5cc

Analysis Process: gnome-session-binary PID: 6284, Parent PID: 1477

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6284, Parent PID: 1477

General

Start time:	12:35:36
Start date:	05/08/2022
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: 6284, Parent PID: 1477

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gsd-smartcard
Arguments:	/usr/libexec/gsd-smartcard
File size:	109152 bytes
MD5 hash:	ea1fbd7f62e4cd0331eae2ef754ee605

File Activities

File Read

Analysis Process: gnome-session-binary PID: 6285, Parent PID: 1477

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes

MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6285**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6285**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6286**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6286**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6286**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gsd-media-keys
Arguments:	/usr/libexec/gsd-media-keys
File size:	232936 bytes
MD5 hash:	a425448c135afb4b8bfd79cc0b6b74da

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6287**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6287**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6287**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gsd-screensaver-proxy
Arguments:	/usr/libexec/gsd-screensaver-proxy
File size:	27232 bytes
MD5 hash:	77e309450c87dceee43f1a9e50cc0d02

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6288**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6288**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6288**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6289**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6289**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6289**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6290**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a

File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6290**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6290**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6291**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6291**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
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: **6291**, Parent PID: **1477**

General

Start time:	12:35:36
Start date:	05/08/2022
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes

MD5 hash:	b55f3394a84976ddb92a2915e5d76914