Joe Sandbox Cloud BASIC

ID: 518922
Sample Name: Yoshi.x86-20211110-0350
Cookbook: defaultlinuxfilecookbook.jbs
Time: 05:08:25
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

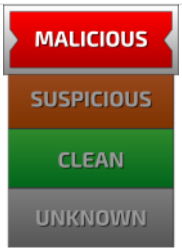
Linux Analysis Report Yoshi.x86-20211110-0350

Overview

General Information

Sample Name:	Yoshi.x86-20211110-0350
Analysis ID:	518922
MD5:	cb3473a526b235..
SHA1:	acb10559e631f61.
SHA256:	c78e289b48b829..
Tags:	Mirai
Infos:	

Detection



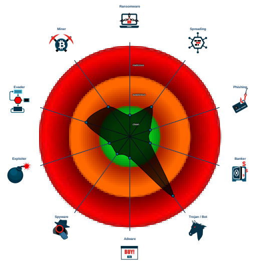
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Reads system files that contain reco…
- Uses known network protocols on no…
- Machine Learning detection for samp…
- Sample reads /proc/mounts (often u…
- Reads CPU information from /sys in…
- Yara signature match
- Executes the "grep" command used…
- Uses the "uname" system call to qu…
- Enumerates processes within the "p

Classification



General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	518922
Start date:	10.11.2021
Start time:	05:08:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Yoshi.x86-20211110-0350
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:	mal80.troj.linX86-20211110-0350@0/7@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- Yoshi.x86-20211110-0350 (PID: 5224, Parent: 5107, MD5: cb3473a526b235ecf6fbbc98dbe82c94) Arguments: /tmp/Yoshi.x86-20211110-0350
    - Yoshi.x86-20211110-0350 New Fork (PID: 5225, Parent: 5224)
    - Yoshi.x86-20211110-0350 New Fork (PID: 5226, Parent: 5224)
        - Yoshi.x86-20211110-0350 New Fork (PID: 5227, Parent: 5226)
            - Yoshi.x86-20211110-0350 New Fork (PID: 5292, Parent: 5227)
            - Yoshi.x86-20211110-0350 New Fork (PID: 5326, Parent: 5227)
            - Yoshi.x86-20211110-0350 New Fork (PID: 5712, Parent: 5227)
        - Yoshi.x86-20211110-0350 New Fork (PID: 5228, Parent: 5226)
- dash New Fork (PID: 5231, Parent: 4331)
- cat (PID: 5231, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.y33HJzJgyl
- dash New Fork (PID: 5232, Parent: 4331)
- head (PID: 5232, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5233, Parent: 4331)
- tr (PID: 5233, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5234, Parent: 4331)
- cut (PID: 5234, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5235, Parent: 4331)
- cat (PID: 5235, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.y33HJzJgyl
- dash New Fork (PID: 5236, Parent: 4331)
- head (PID: 5236, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5237, Parent: 4331)
- tr (PID: 5237, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5238, Parent: 4331)
- cut (PID: 5238, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5239, Parent: 4331)
- rm (PID: 5239, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.y33HJzJgyl /tmp/tmp.Vw6fOLR470 /tmp/tmp.pbb6pGxeaC
- gnome-session-binary New Fork (PID: 5299, Parent: 1477)
- sh (PID: 5299, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
- gnome-shell (PID: 5299, Parent: 1477, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
    - gnome-shell New Fork (PID: 5384, Parent: 5299)
    - ibus-daemon (PID: 5384, Parent: 5299, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
        - ibus-daemon New Fork (PID: 5613, Parent: 5384)
        - ibus-memconf (PID: 5613, Parent: 5384, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
        - ibus-daemon New Fork (PID: 5615, Parent: 5384)
            - ibus-daemon New Fork (PID: 5616, Parent: 5615)
            - ibus-x11 (PID: 5616, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
        - ibus-daemon New Fork (PID: 5987, Parent: 5384)
        - ibus-engine-simple (PID: 5987, Parent: 5384, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
- systemd New Fork (PID: 5334, Parent: 1)
- systemd-localed (PID: 5334, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- dbus-daemon New Fork (PID: 5618, Parent: 5617)
- ibus-portal (PID: 5618, Parent: 5617, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
- systemd New Fork (PID: 5634, Parent: 1)
- upowerd (PID: 5634, Parent: 1, MD5: 1253eea2fe5fe4017069664284e326cd) Arguments: /usr/lib/upower/upowerd
- Xorg New Fork (PID: 5716, Parent: 1465)
- sh (PID: 5716, Parent: 1465, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
    - sh New Fork (PID: 5717, Parent: 5716)
    - xkbcomp (PID: 5717, Parent: 5716, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
- systemd New Fork (PID: 5718, Parent: 1)
- accounts-daemon (PID: 5718, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5722, Parent: 5718)
    - language-validate (PID: 5722, Parent: 5718, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
        - language-validate New Fork (PID: 5723, Parent: 5722)
        - language-options (PID: 5723, Parent: 5722, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
            - language-options New Fork (PID: 5726, Parent: 5723)
            - sh (PID: 5726, Parent: 5723, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
                - sh New Fork (PID: 5727, Parent: 5726)
                - locale (PID: 5727, Parent: 5726, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
                - sh New Fork (PID: 5728, Parent: 5726)
                - grep (PID: 5728, Parent: 5726, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- systemd New Fork (PID: 5731, Parent: 1)
- geoclue (PID: 5731, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- dbus-daemon New Fork (PID: 5958, Parent: 5957)
- gjs (PID: 5958, Parent: 5957, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
- systemd New Fork (PID: 5965, Parent: 1334)
- pulseaudio (PID: 5965, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 6000, Parent: 1)
- fprintd (PID: 6000, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Yoshi.x86-20211110-0350	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x1a774:$xo1: Dfs`eeh&<'9 • 0x1a7e4:$xo1: Dfs`eeh&<'9 • 0x1a854:$xo1: Dfs`eeh&<'9 • 0x1a8c4:$xo1: Dfs`eeh&<'9 • 0x1a934:$xo1: Dfs`eeh&<'9

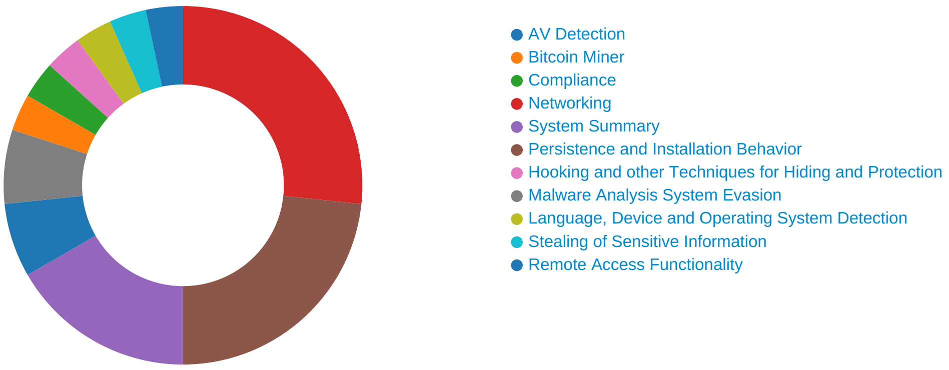
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5712.1.0000000072924dd1.000000004d754636.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x498:$xo1: Dfs`eeh&<'9 • 0x510:$xo1: Dfs`eeh&<'9 • 0x588:$xo1: Dfs`eeh&<'9 • 0x600:$xo1: Dfs`eeh&<'9 • 0x678:$xo1: Dfs`eeh&<'9
5292.1.0000000072924dd1.000000004d754636.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x498:$xo1: Dfs`eeh&<'9 • 0x510:$xo1: Dfs`eeh&<'9 • 0x588:$xo1: Dfs`eeh&<'9 • 0x600:$xo1: Dfs`eeh&<'9 • 0x678:$xo1: Dfs`eeh&<'9
5225.1.0000000072924dd1.000000004d754636.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x498:$xo1: Dfs`eeh&<'9 • 0x510:$xo1: Dfs`eeh&<'9 • 0x588:$xo1: Dfs`eeh&<'9 • 0x600:$xo1: Dfs`eeh&<'9 • 0x678:$xo1: Dfs`eeh&<'9
5326.1.0000000072924dd1.000000004d754636.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x498:$xo1: Dfs`eeh&<'9 • 0x510:$xo1: Dfs`eeh&<'9 • 0x588:$xo1: Dfs`eeh&<'9 • 0x600:$xo1: Dfs`eeh&<'9 • 0x678:$xo1: Dfs`eeh&<'9
5224.1.0000000072924dd1.000000004d754636.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x498:$xo1: Dfs`eeh&<'9 • 0x510:$xo1: Dfs`eeh&<'9 • 0x588:$xo1: Dfs`eeh&<'9 • 0x600:$xo1: Dfs`eeh&<'9 • 0x678:$xo1: Dfs`eeh&<'9
Click to see the 5 entries				

Jbx Signature Overview



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

Persistence and Installation Behavior:

Sample reads /proc/mounts (often used for finding a writable filesystem)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

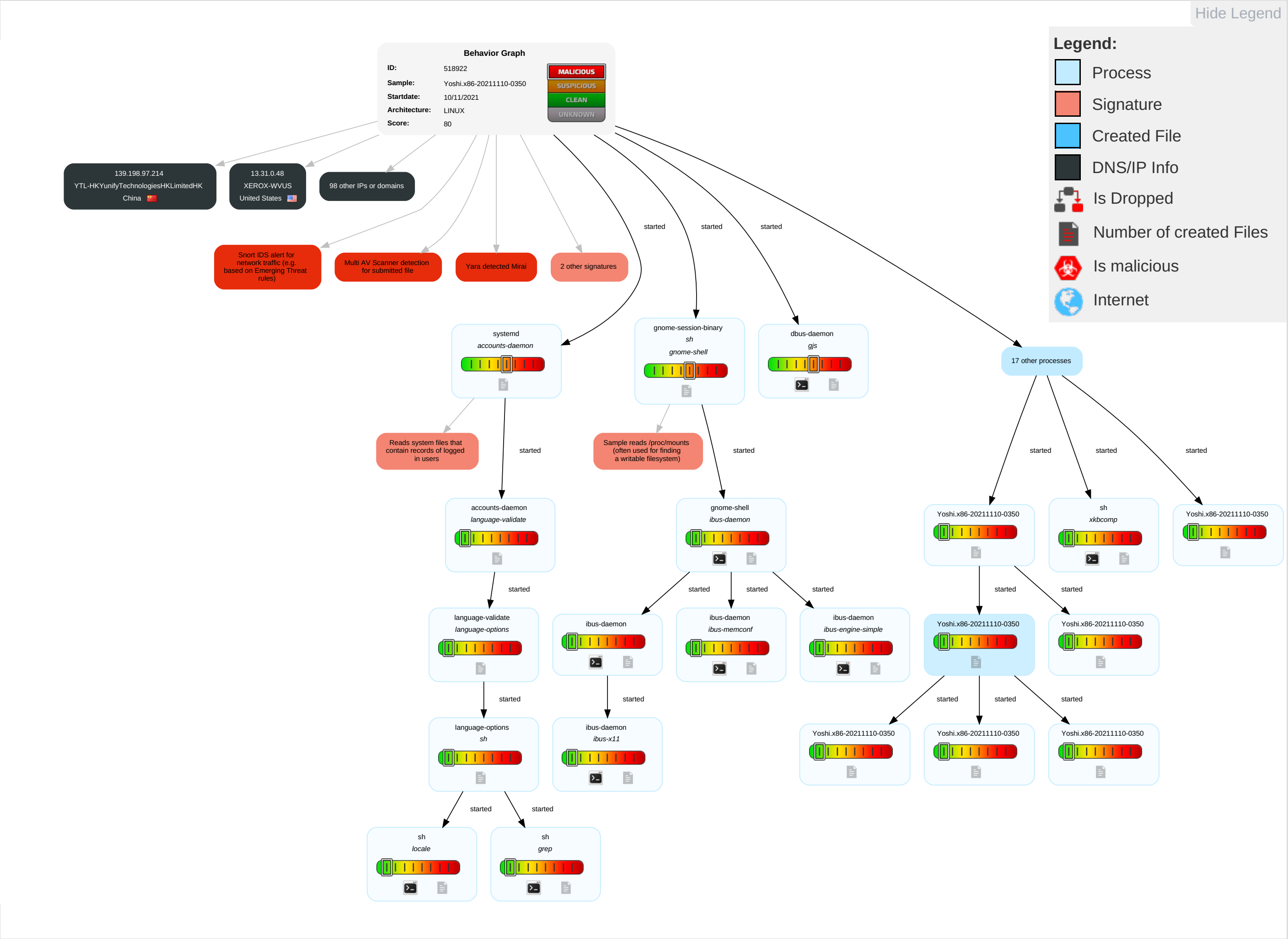
Mitre Att&ck Matrix

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	Scripting 1	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 System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1	LSASS Memory	System Owner/User Discovery 1	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 Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Behavior Graph

ID: 518922

Sample: Yoshi.x86-20211110-0350

Startdate: 10/11/2021

Architecture: LINUX

Score: 80

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Yoshi.x86-20211110-0350	50%	Virustotal		Browse
Yoshi.x86-20211110-0350	48%	ReversingLabs	Linux.Trojan.Mirai	
Yoshi.x86-20211110-0350	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
14.213.58.84	unknown	China	🇨🇳	4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
27.241.214.158	unknown	Taiwan; Republic of China (ROC)	🇹🇼	9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
103.165.24.206	unknown	unknown	?	7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
206.81.117.10	unknown	United States	🇺🇸	8046	NAPANETUS	false
221.235.231.36	unknown	China	🇨🇳	4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
60.205.108.60	unknown	China	🇨🇳	37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
78.200.7.192	unknown	France	🇫🇷	12322	PROXADFR	false
38.218.179.213	unknown	United States	🇺🇸	174	COGENT-174US	false
12.15.101.249	unknown	United States	🇺🇸	32328	ALASCOM-IP-MANAGED-NETWORKUS	false
185.41.19.218	unknown	Norway	🇳🇴	199900	ASN-BEDSYSNO	false
176.237.211.68	unknown	Turkey	🇹🇷	16135	TURKCELL-ASTurkcellASTR	false
77.68.188.231	unknown	Denmark	🇩🇰	43557	ASEMNETDK	false
139.198.97.214	unknown	China	🇨🇳	134366	YTL-HKYunifyTechnologiesHKLimitedHK	false
110.69.124.69	unknown	Korea Republic of	🇰🇷	4766	KIXS-AS-KRKoreaTelecomKR	false
61.93.172.176	unknown	Hong Kong	🇭🇰	9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	false
20.109.196.213	unknown	United States	🇺🇸	8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
160.120.172.228	unknown	Cote D'ivoire	🇨🇮	29571	ORANGE-COTE-IVOIRECI	false
151.22.11.137	unknown	Italy	🇮🇹	1267	ASN-WINDTREIUNETEU	false
77.129.234.62	unknown	France	🇫🇷	15557	LDCOMNETFR	false
152.39.223.145	unknown	United States	🇺🇸	81	NCRENUS	false
24.69.97.22	unknown	Canada	🇨🇦	6327	SHAWCA	false
156.214.15.119	unknown	Egypt	🇪🇬	8452	TE-ASTE-ASEG	false
94.132.45.221	unknown	Portugal	🇵🇹	2860	NOS_COMUNICACOESPT	false
58.250.84.151	unknown	China	🇨🇳	17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
114.59.247.87	unknown	Indonesia	🇮🇩	4795	INDOSATM2-IDINDOSATM2ASNID	false
36.54.36.167	unknown	Japan	🇯🇵	10013	FBDCFreeBitCoLtdJP	false
182.25.78.39	unknown	Indonesia	🇮🇩	4795	INDOSATM2-IDINDOSATM2ASNID	false
86.40.94.173	unknown	Ireland	🇮🇪	5466	EIRCOMInternetHouseIE	false
147.51.110.245	unknown	United States	🇺🇸	1491	DNIC-AS-01491US	false
101.121.5.200	unknown	China	🇨🇳	133612	VODAFONE-AS-APVodafoneAustraliaPtyLtdAU	false
104.90.135.191	unknown	United States	🇺🇸	16625	AKAMAI-ASUS	false
181.204.131.176	unknown	Colombia	🇨🇴	27831	ColombiaMovilCO	false
8.124.12.149	unknown	United States	🇺🇸	3356	LEVEL3US	false
213.192.183.95	unknown	Finland	🇫🇮	719	ELISA-ASHelsinkiFinlandEU	false
70.187.228.16	unknown	United States	🇺🇸	22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
203.144.121.101	unknown	China	🇨🇳	4755	TATACOMM-ASTATACommunicationsformerlyVSNLisLeadingISP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.153.200.75	unknown	Australia	🇦🇺	38790	SPIRIT-TELECOMSpiritTelecomAustraliaPtyLtdAU	false
66.142.171.115	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
80.142.180.164	unknown	Germany	🇩🇪	3320	DTAGInternetserviceprovideroperationsDE	false
173.199.168.228	unknown	United States	🇺🇸	32244	LIQUIDWEBUS	false
205.147.235.48	unknown	United States	🇺🇸	7349	AS-TIERP-7349US	false
182.49.45.63	unknown	China	🇨🇳	9371	SAKURA-CSAKURAInternetIncJP	false
152.45.134.40	unknown	United States	🇺🇸	81	NCRENUS	false
66.44.154.146	unknown	United States	🇺🇸	23465	NUTELECOMUS	false
112.160.188.211	unknown	Korea Republic of	🇰🇷	4766	KIXS-AS-KRKoreaTelecomKR	false
62.86.66.106	unknown	Italy	🇮🇹	3269	ASN-IBSNAZIT	false
102.2.61.4	unknown	unknown	?	36926	CKL1-ASNKE	false
146.208.227.123	unknown	United States	🇺🇸	5619	EVRY-NO	false
98.42.156.209	unknown	United States	🇺🇸	7922	COMCAST-7922US	false
99.180.232.127	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
94.94.36.64	unknown	Italy	🇮🇹	3269	ASN-IBSNAZIT	false
210.85.166.50	unknown	Taiwan; Republic of China (ROC)	🇹🇼	7482	APOL-ASAsiaPacificOn-lineServiceIncTW	false
223.129.191.223	unknown	China	🇨🇳	4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
166.252.202.216	unknown	United States	🇺🇸	22394	CELLCOUS	false
23.72.69.192	unknown	United States	🇺🇸	16625	AKAMAI-ASUS	false
18.28.89.254	unknown	United States	🇺🇸	3	MIT-GATEWAYSUS	false
39.118.64.129	unknown	Korea Republic of	🇰🇷	9318	SKB-ASSKBroadbandCoLtdKR	false
13.31.0.48	unknown	United States	🇺🇸	26662	XEROX-WVUS	false
176.68.84.160	unknown	Sweden	🇸🇪	1257	TELE2EU	false
130.17.184.100	unknown	United States	🇺🇸	2152	CSUNET-NWUS	false
38.250.231.37	unknown	United States	🇺🇸	174	COGENT-174US	false
78.60.212.7	unknown	Lithuania	🇱🇹	8764	TELIA-LIETUVALT	false
8.89.57.170	unknown	United States	🇺🇸	3356	LEVEL3US	false
34.174.118.58	unknown	United States	🇺🇸	2686	ATGS-MMD-ASUS	false
142.98.45.249	unknown	Canada	🇨🇦	5769	VIDEOTRONCA	false
159.155.32.13	unknown	United States	🇺🇸	11757	WHIRLPOOL-ASNUS	false
36.173.104.143	unknown	China	🇨🇳	9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
166.147.21.15	unknown	United States	🇺🇸	6167	CELLCO-PARTUS	false
209.210.62.0	unknown	United States	🇺🇸	396033	BFDX515US	false
122.149.110.158	unknown	Australia	🇦🇺	9443	VOCUS-RETAIL-AUVocusRetailAU	false
188.126.70.104	unknown	Sweden	🇸🇪	42708	PORTLANEwwwportlanecomSE	false
161.191.74.102	unknown	United States	🇺🇸	13474	BancodeGaliciayBuenosAiresAR	false
2.125.47.38	unknown	United Kingdom	🇬🇧	5607	BSKYB-BROADBAND-ASGB	false
97.175.248.212	unknown	United States	🇺🇸	6167	CELLCO-PARTUS	false
60.186.26.114	unknown	China	🇨🇳	4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
73.105.10.72	unknown	United States	🇺🇸	7922	COMCAST-7922US	false
151.105.118.221	unknown	Finland	🇫🇮	1759	TSF-IP-CORETeliaFinlandOyjEU	false
57.44.124.153	unknown	Belgium	🇧🇪	2686	ATGS-MMD-ASUS	false
90.202.191.182	unknown	United Kingdom	🇬🇧	5607	BSKYB-BROADBAND-ASGB	false
163.243.147.68	unknown	United States	🇺🇸	668	DNIC-AS-00668US	false
71.29.203.30	unknown	United States	🇺🇸	7029	WINDSTREAMUS	false
8.232.159.248	unknown	United States	🇺🇸	3356	LEVEL3US	false
218.167.76.218	unknown	Taiwan; Republic of China (ROC)	🇹🇼	3462	HINETDataCommunicationBusinessGroupTW	false
223.93.32.178	unknown	China	🇨🇳	56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.87.28.24	unknown	Netherlands	🇳🇱	1136	KPNKPNNationalEU	false
158.192.236.217	unknown	France	🇫🇷	9159	CreditAgricoleFR	false
181.217.21.237	unknown	Brazil	🇧🇷	21826	CorporacionTelemicCAVE	false
45.106.6.141	unknown	Egypt	🇪🇬	37069	MOBINILEG	false
32.143.225.66	unknown	United States	🇺🇸	7018	ATT-INTERNET4US	false
8.30.115.172	unknown	United States	🇺🇸	23089	HOTWIRE-COMMUNICATIONSUS	false
86.44.199.169	unknown	Ireland	🇮🇪	5466	EIRCOMInternetHouseIE	false
14.241.252.211	unknown	Viet Nam	🇻🇳	45899	VNPT-AS-VNVNPTCorpVN	false
92.211.109.198	unknown	Germany	🇩🇪	3209	VODANETInternationalIP-BackboneofVodafoneDE	false
20.132.107.120	unknown	United States	🇺🇸	206	CSC-IGN-AMERUS	false
187.239.163.155	unknown	Mexico	🇲🇽	8151	UninetSAdeCVMX	false
53.63.240.198	unknown	Germany	🇩🇪	31399	DAIMLER-ASITIGNGlobalNetworkDE	false
200.26.181.233	unknown	Paraguay	🇵🇾	23201	TelecelSAPY	false
190.176.180.80	unknown	Argentina	🇦🇷	22927	TelefonicadeArgentinaAR	false
4.191.205.63	unknown	United States	🇺🇸	3356	LEVEL3US	false
87.186.120.255	unknown	Germany	🇩🇪	3320	DTAGInternetserviceprovideroperationsDE	false

Runtime Messages

Command:	/tmp/Yoshi.x86-20211110-0350
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infection Complete
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
213.192.183.95	k01aDQAlUL	Get hash	malicious	Browse	
	LyxN1ckWTW	Get hash	malicious	Browse	
101.121.5.200	k01aDQAlUL	Get hash	malicious	Browse	
	xd.x86	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FET-TWFarEastToneTelecommunicationCoLtdTW	pt7DJSPfna	Get hash	malicious	Browse	• 39.15.178.105
	2tdWqgPQPc	Get hash	malicious	Browse	• 61.20.160.150
	arm	Get hash	malicious	Browse	• 27.247.41.108
	Kz2SeJpaxw	Get hash	malicious	Browse	• 27.243.89.17
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 110.26.167.12
	gFn4iz8ygL	Get hash	malicious	Browse	• 110.24.10.63
	YG9KkTTAgE	Get hash	malicious	Browse	• 39.9.66.226
	kkr4DrMz5L	Get hash	malicious	Browse	• 39.8.150.191
	QLPxrFlfKm	Get hash	malicious	Browse	• 110.24.139.143
	DvwfkRaTRo	Get hash	malicious	Browse	• 110.30.97.134
	auzkes	Get hash	malicious	Browse	• 61.20.88.165
	b3astmode.x86	Get hash	malicious	Browse	• 27.242.160.3

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sora.arm7	Get hash	malicious	Browse	• 27.244.207.190
	o6aMoZKsIK	Get hash	malicious	Browse	• 110.26.118.49
	yVbcX1sEtS	Get hash	malicious	Browse	• 39.9.193.234
	u4M7XeqKtD	Get hash	malicious	Browse	• 27.240.206.217
	arm	Get hash	malicious	Browse	• 211.77.233.35
	Antisocial.x86	Get hash	malicious	Browse	• 114.140.203.26
	ivImhRZqGa	Get hash	malicious	Browse	• 27.248.6.232
	eImb49ofup	Get hash	malicious	Browse	• 118.231.23.43
AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	sora.x86	Get hash	malicious	Browse	• 103.175.3.206
	New order #1138.xlsx	Get hash	malicious	Browse	• 103.171.1.113
	wsVomvavHj	Get hash	malicious	Browse	• 103.172.4.110
	PO 0008-22 R1 Bracker.xlsx	Get hash	malicious	Browse	• 103.171.1.113
	Swift_Advice.xlsx	Get hash	malicious	Browse	• 103.171.0.134
	purchase order.xlsx	Get hash	malicious	Browse	• 103.167.85.176
	QLPxrFlfKm	Get hash	malicious	Browse	• 103.176.243.184
	8krBRiWrtG	Get hash	malicious	Browse	• 161.50.51.181
	ORDER 15212.xlsx	Get hash	malicious	Browse	• 103.171.1.113
	F0ihkIMDf2	Get hash	malicious	Browse	• 103.162.154.163
	Payment copy.xlsx	Get hash	malicious	Browse	• 103.167.90.85
	uV1rj8v43F	Get hash	malicious	Browse	• 141.132.42.3
	X8q5ELI79g	Get hash	malicious	Browse	• 103.169.130.71
	Bank_Statement.xlsx	Get hash	malicious	Browse	• 103.167.84.65
	Shipping doccument.xlsx	Get hash	malicious	Browse	• 103.167.90.85
	swift copy.xlsx	Get hash	malicious	Browse	• 103.167.85.176
	Pre-payment Swift Advice.xlsx	Get hash	malicious	Browse	• 103.171.0.134
	TG.xlsx	Get hash	malicious	Browse	• 103.171.1.113
	Purchase order-NX-LI-15-0001.xlsx	Get hash	malicious	Browse	• 103.167.85.176
	GSS-SLF-HK.xlsx	Get hash	malicious	Browse	• 103.167.84.138
CHINANET-BACKBONENo31Jin-rongStreetCN	pt7DJSPfna	Get hash	malicious	Browse	• 180.140.91.40
	zD1jpTbFQq	Get hash	malicious	Browse	• 60.174.151.99
	fNrSUTMJ8O	Get hash	malicious	Browse	• 122.227.69.245
	2tdWqgPQPc	Get hash	malicious	Browse	• 14.213.83.64
	NMhjdmrpZi	Get hash	malicious	Browse	• 121.233.6.222
	8wdtrqd3z0	Get hash	malicious	Browse	• 123.197.21.121
	arm7	Get hash	malicious	Browse	• 183.34.226.62
	x86-20211110-0150	Get hash	malicious	Browse	• 14.26.78.23
	sora.x86	Get hash	malicious	Browse	• 124.236.54.119
	x86	Get hash	malicious	Browse	• 58.66.156.104
	KKveTTgaAAsecNNaaaa.arm7	Get hash	malicious	Browse	• 182.133.95.249
	arm	Get hash	malicious	Browse	• 171.40.189.88
	Heri2RE17I	Get hash	malicious	Browse	• 49.90.222.113
	jew.x86-20211110-0200	Get hash	malicious	Browse	• 1.68.207.218
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 110.154.131.82
	v9o2vinbUj	Get hash	malicious	Browse	• 110.181.221.34
	QSjpGBd7Gv	Get hash	malicious	Browse	• 116.25.221.155
	fbXTgwatuJ	Get hash	malicious	Browse	• 222.182.208.77
	uCkIzRN4ZzUIzCY.exe	Get hash	malicious	Browse	• 27.17.225.141
	mips	Get hash	malicious	Browse	• 27.18.99.15

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/run/user/127/dconf/user	
Process:	/usr/bin/gnome-shell
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	93B885ADFE0DA089CDF634904FD59F71
SHA1:	5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F
SHA-256:	6E340B9CFFB37A989CA544E6BB780A2C78901D3FB33738768511A30617AFA01D
SHA-512:	B8244D028981D693AF7B456AF8EFA4CAD63D282E19FF14942C246E50D9351D22704A802A71C3580B6370DE4CEB293C324A8423342557D4E5C38438F0E36910EE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

/run/user/127/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:JTQv:d6
MD5:	8D73A5B0D3930F77C679E2C7AD58579E
SHA1:	8A1F4C5E74FA63EDD8BF56229FF6FA6EBF71FB92
SHA-256:	4EA5BAD19AACB921164B006E9D65757024AA36EB689BE4DA6C4ADD2C3480AF2A
SHA-512:	6259F9B1EF1250EA9E07E44DD0EB5EC77C43516A79E816AD57E90F44F1BEB2FEA67FFC51D7AAC7D44D9AAD656CB1369C06C932272D3BBB66263D889D7EBC9 00
Malicious:	false
Reputation:	low
Preview:	5965.

/tmp/server-0.xkm	
Process:	/usr/bin/xkbcomp
File Type:	Compiled XKB Keymap: lsb, version 15
Category:	dropped
Size (bytes):	12060
Entropy (8bit):	4.8492493153178975
Encrypted:	false
SSDEEP:	192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ
MD5:	B4E3EB0B8B6B0FC1F46740C573E18D86
SHA1:	7D35426357695EBA77850757E8939A62DCEFF2D1
SHA-256:	7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91
SHA-512:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE0C 1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.mkx.............D......................h.......<.....P.@%.......&......D.......NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta ....Super...Hyper...........evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD 06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB 08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP 3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWN PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181 I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18

/var/cache/motd-news	
Process:	/usr/bin/cut
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.515771857099866
Encrypted:	false
SSDEEP:	3:P2lnI+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn
MD5:	DD514F892B5F93ED615D366E58AC58AF

/var/cache/motd-news

SHA1:	BA75EDB3C2232CC260BC187F604DC8F25AA72C11
SHA-256:	F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF
SHA-512:	9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACCDBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42 2D0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	* Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation.

/var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0

Process:	/usr/bin/ibus-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.169155049816653
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWvDmkH19v:q5sU3LWfLUDmQymqSFbfomShzfv
MD5:	FDFF86CAB0545210FFDEE660084DDB68
SHA1:	D66961AA2419CDB5115570E8E864DD3F6D64431E
SHA-256:	AE0577109D945E0FF7BD133F98B9E99EF12E6928625E91C6A380075FC193B957
SHA-512:	9D91A776BDC93600F601D24CDE9DA95D4B960E4ECF185F56E6F0F5B64FF32DD59ED6BEAE3276CBAEF84292403F0E35AB0F7F320A4320F1032D1DB0CCAD285 C5
Malicious:	false
Reputation:	low
Preview:	# This file is created by ibus-daemon, please do not modify it..# This file allows processes on the machine to find the.# ibus session bus with the below address..# If the IBUS_ADDRESS environment variable is set, it will.# be used rather than this file..IBUS_ADDRESS=unix:abstract=/var/lib/gdm3/.cache/ibus/dbus-xtmG7FJV,guid=40b8aa05c6554356f0709f8f618b544e.IBUS_DAEMON_PID=5384.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink

Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE 9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source

Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE 9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.464702529748402
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	Yoshi.x86-20211110-0350
File size:	111376
MD5:	cb3473a526b235ecf6fbbc98dbe82c94
SHA1:	acb10559e631f61d25fa9a3a2220e4d6c26982d3
SHA256:	c78e289b48b8290926103ded72ca2dcdc17ba5f6cf5b2d8178b0526ab6248c94
SHA512:	867f2d3835039902fa163e5c41b6d69b6f32fa8a9b3a8a3092f9143db8a3c17fb021014ccf2cf7edc8d8125f5bc899765c9e244de6b34c1f3a1e7cf7a1074f3b
SSDEEP:	3072:hV4ifcpWpQS4fdtFZLluZbGsEzeYi7vDWzbCYld9n:vXQCH4fPF9gZ1EqxDWqI
File Content Preview:	.ELF...................d...4...........4. ...(..................................... ....0...0..@...@...........Q.td...........................U..S....... w....h....3...[]...$.............U......=@1...t..5....$0.....$0......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:	110976
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	0x19256	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8061306	0x19306	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8061320	0x19320	0x1c80	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8063000	0x1b000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8063008	0x1b008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8063020	0x1b020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8063140	0x1b140	0xd00	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x1b140	0x3e	0x0	0x0		0	0	1

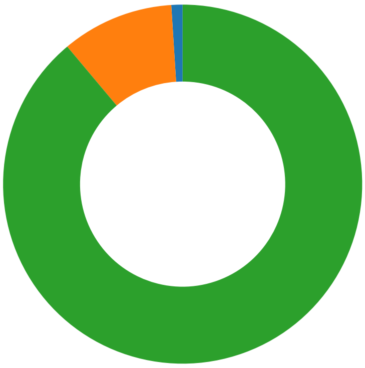
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x1afa0	0x1afa0	3.8740	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x1b000	0x8063000	0x8063000	0x140	0xe40	2.6353	0x6	RW	0x1000		.ctors .dtors .data .bss

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 99

- ● 23 (Telnet)
- ● 2323 undefined
- ● 2616 undefined

TCP Packets

System Behavior

Analysis Process: Yoshi.x86-20211110-0350 PID: 5224 Parent PID: 5107

General

Start time:	05:09:09
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	/tmp/Yoshi.x86-20211110-0350
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: Yoshi.x86-20211110-0350 PID: 5225 Parent PID: 5224

General

Start time:	05:09:09
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: Yoshi.x86-20211110-0350 PID: 5226 Parent PID: 5224

General

Start time:	05:09:09
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: Yoshi.x86-20211110-0350 PID: 5227 Parent PID: 5226

General

Start time:	05:09:09
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

File Activities

File Read

Directory Enumerated

Analysis Process: Yoshi.x86-20211110-0350 PID: 5292 Parent PID: 5227

General

Start time:	05:10:14
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: Yoshi.x86-20211110-0350 PID: 5326 Parent PID: 5227

General

Start time:	05:10:30
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: Yoshi.x86-20211110-0350 PID: 5712 Parent PID: 5227

General

Start time:	05:10:42
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350

Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: Yoshi.x86-20211110-0350 PID: 5228 Parent PID: 5226

General

Start time:	05:09:09
Start date:	10/11/2021
Path:	/tmp/Yoshi.x86-20211110-0350
Arguments:	n/a
File size:	111376 bytes
MD5 hash:	cb3473a526b235ecf6fbbc98dbe82c94

Analysis Process: dash PID: 5231 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5231 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.y33HJzJgyl
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5232 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5232 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5233 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5233 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
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: 5234 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5234 Parent PID: 4331

General

Start time:	05:09:14
Start date:	10/11/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5235 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5235 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.y33HJzJgyl
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5236 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5236 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/head

Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5237 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5237 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
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: 5238 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5238 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
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: 5239 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5239 Parent PID: 4331

General

Start time:	05:09:15
Start date:	10/11/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.y33HJzJgyl /tmp/tmp.Vw6fOLR470 /tmp/tmp.pbb6pGxeaC
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: gnome-session-binary PID: 5299 Parent PID: 1477

General

Start time:	05:10:24
Start date:	10/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5299 Parent PID: 1477

General

Start time:	05:10:24
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gnome-shell PID: 5299 Parent PID: 1477

General

Start time:	05:10:24
Start date:	10/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	/usr/bin/gnome-shell
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-shell PID: 5384 Parent PID: 5299

General

Start time:	05:10:36
Start date:	10/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5384 Parent PID: 5299

General

Start time:	05:10:37
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	ibus-daemon --panel disable --xim
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5613 Parent PID: 5384

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5613 Parent PID: 5384

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/libexec/ibus-memconf
Arguments:	/usr/libexec/ibus-memconf
File size:	22904 bytes
MD5 hash:	523e939905910d06598e66385761a822

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5615 Parent PID: 5384

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5616 Parent PID: 5615

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5616 Parent PID: 1

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/libexec/ibus-x11
Arguments:	/usr/libexec/ibus-x11 --kill-daemon
File size:	100352 bytes
MD5 hash:	2aa1e54666191243814c2733d6992dbd

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5987 Parent PID: 5384

General

Start time:	05:10:59
Start date:	10/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-engine-simple PID: 5987 Parent PID: 5384

General

Start time:	05:10:59
Start date:	10/11/2021

Path:	/usr/libexec/ibus-engine-simple
Arguments:	/usr/libexec/ibus-engine-simple
File size:	14712 bytes
MD5 hash:	0238866d5e8802a0ce1b1b9af8cb1376

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5334 Parent PID: 1

General

Start time:	05:10:37
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5334 Parent PID: 1

General

Start time:	05:10:37
Start date:	10/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

File Activities

File Read

Analysis Process: dbus-daemon PID: 5618 Parent PID: 5617

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: ibus-portal PID: 5618 Parent PID: 5617

General

Start time:	05:10:38
Start date:	10/11/2021
Path:	/usr/libexec/ibus-portal
Arguments:	/usr/libexec/ibus-portal
File size:	92536 bytes
MD5 hash:	562ad55bd9a4d54bd7b76746b01e37d3

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 5634 Parent PID: 1

General

Start time:	05:10:41
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: upowerd PID: 5634 Parent PID: 1

General

Start time:	05:10:41
Start date:	10/11/2021
Path:	/usr/lib/upower/upowerd
Arguments:	/usr/lib/upower/upowerd
File size:	260328 bytes
MD5 hash:	1253eea2fe5fe4017069664284e326cd

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: Xorg PID: 5716 Parent PID: 1465

General

Start time:	05:10:42
Start date:	10/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5716 Parent PID: 1465

General

Start time:	05:10:42
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5717 Parent PID: 5716

General

Start time:	05:10:42
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5717 Parent PID: 5716

General

Start time:	05:10:42
Start date:	10/11/2021
Path:	/usr/bin/xkbcomp
Arguments:	/usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
File size:	217184 bytes
MD5 hash:	c5f953aec4c00d2a1cc27acb75d62c9b

File Activities

File Deleted

File Read

File Written

Analysis Process: systemd PID: 5718 Parent PID: 1

General

Start time:	05:10:44
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a

File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5718 Parent PID: 1

General

Start time:	05:10:44
Start date:	10/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	/usr/lib/accountsservice/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

File Read

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 5722 Parent PID: 5718

General

Start time:	05:10:45
Start date:	10/11/2021
Path:	/usr/lib/accountsservice/accounts-daemon
Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 5722 Parent PID: 5718

General

Start time:	05:10:45
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	/usr/share/language-tools/language-validate en_US.UTF-8
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: language-validate PID: 5723 Parent PID: 5722

General

Start time:	05:10:45
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5723 Parent PID: 5722

General

Start time:	05:10:45
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	/usr/share/language-tools/language-options
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 5726 Parent PID: 5723

General

Start time:	05:10:46
Start date:	10/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5726 Parent PID: 5723

General

Start time:	05:10:46
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "locale -a | grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5727 Parent PID: 5726

General

Start time:	05:10:46
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5727 Parent PID: 5726

General

Start time:	05:10:46
Start date:	10/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5728 Parent PID: 5726

General

Start time:	05:10:46
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5728 Parent PID: 5726

General

Start time:	05:10:46
Start date:	10/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: systemd PID: 5731 Parent PID: 1

General

Start time:	05:10:51
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5731 Parent PID: 1

General

Start time:	05:10:51
Start date:	10/11/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5958 Parent PID: 5957

General

Start time:	05:10:51
Start date:	10/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: gjs PID: 5958 Parent PID: 5957

General

Start time:	05:10:51
Start date:	10/11/2021
Path:	/usr/bin/gjs
Arguments:	/usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
File size:	23128 bytes
MD5 hash:	5f3eceb792bb65c22f23d1efb4fde3ad

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5965 Parent PID: 1334

General

Start time:	05:10:52
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5965 Parent PID: 1334

General

Start time:	05:10:52
Start date:	10/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 6000 Parent PID: 1

General

Start time:	05:11:04
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6000 Parent PID: 1

General

Start time:	05:11:04
Start date:	10/11/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84

File Activities

File Read

Directory Enumerated