ID: 553477
Sample Name: phantom.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:34:59
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

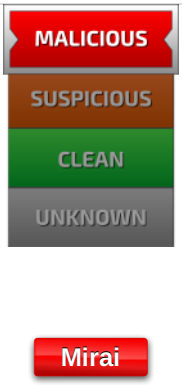
Linux Analysis Report phantom.x86

Overview

General Information

Sample Name:	phantom.x86
Analysis ID:	553477
MD5:	8bb140fe0754eee.
SHA1:	0146917808c967..
SHA256:	217a622a111c0d..
Tags:	Mirai
Infos:	

Detection

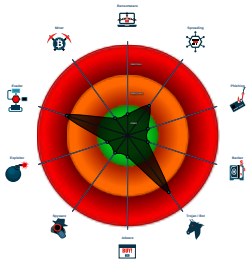


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample contains only a LOAD segm...
- Deletes log files
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Executes commands using a shell c...
- Executes the "systemctl" command...
- Tries to connect to HTTP servers, b...

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553477
Start date:	15.01.2022
Start time:	00:34:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	phantom.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:	mal72.troj.evad.linX86@0/53@0/0
Warnings:	Show All

Process Tree

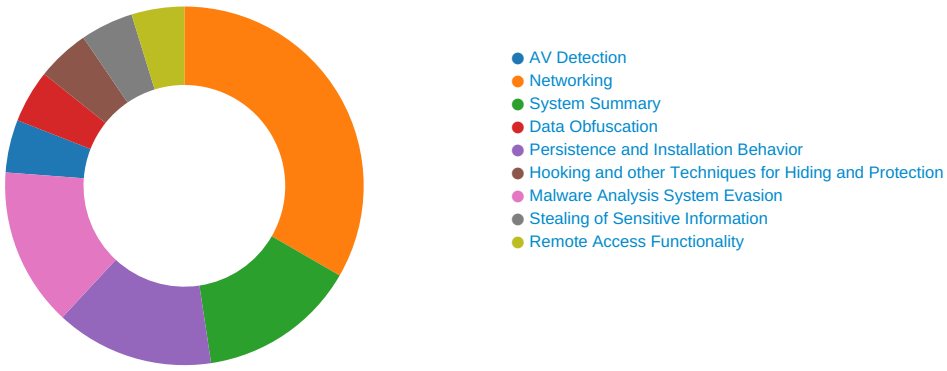
- **system is lnxubuntu20**
- systemd New Fork (PID: 5192, Parent: 1)
- logrotate (PID: 5192, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5233, Parent: 5192)
  - gzip (PID: 5233, Parent: 5192, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5236, Parent: 5192)
  - sh (PID: 5236, Parent: 5192, 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: 5237, Parent: 5236)
    - invoke-rc.d (PID: 5237, Parent: 5236, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5238, Parent: 5237)
      - runlevel (PID: 5238, Parent: 5237, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5239, Parent: 5237)
      - systemctl (PID: 5239, Parent: 5237, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5242, Parent: 5237)
      - ls (PID: 5242, Parent: 5237, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5243, Parent: 5237)
      - systemctl (PID: 5243, Parent: 5237, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 5244, Parent: 5192)
  - gzip (PID: 5244, Parent: 5192, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5245, Parent: 5192)
  - sh (PID: 5245, Parent: 5192, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
    - sh New Fork (PID: 5246, Parent: 5245)
    - rsyslog-rotate (PID: 5246, Parent: 5245, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
      - rsyslog-rotate New Fork (PID: 5247, Parent: 5246)
      - systemctl (PID: 5247, Parent: 5246, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5193, Parent: 1)
- install (PID: 5193, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5232, Parent: 1)
- find (PID: 5232, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5240, Parent: 1)
- mandb (PID: 5240, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- phantom.x86 (PID: 5278, Parent: 5117, MD5: 8bb140fe0754eee2498279f9f1830368) Arguments: /tmp/phantom.x86
  - phantom.x86 New Fork (PID: 5279, Parent: 5278)
    - phantom.x86 New Fork (PID: 5372, Parent: 5279)
    - phantom.x86 New Fork (PID: 5374, Parent: 5279)
      - phantom.x86 New Fork (PID: 5375, Parent: 5374)
        - phantom.x86 New Fork (PID: 5381, Parent: 5375)
        - phantom.x86 New Fork (PID: 5382, Parent: 5375)
      - phantom.x86 New Fork (PID: 5376, Parent: 5374)
      - phantom.x86 New Fork (PID: 5377, Parent: 5374)
  - phantom.x86 New Fork (PID: 5280, Parent: 5278)
  - phantom.x86 New Fork (PID: 5281, Parent: 5278)
    - phantom.x86 New Fork (PID: 5282, Parent: 5281)
      - phantom.x86 New Fork (PID: 5371, Parent: 5282)
      - phantom.x86 New Fork (PID: 5373, Parent: 5282)
    - phantom.x86 New Fork (PID: 5283, Parent: 5281)
    - phantom.x86 New Fork (PID: 5284, Parent: 5281)
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



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)

Uses known network protocols on non-standard ports

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

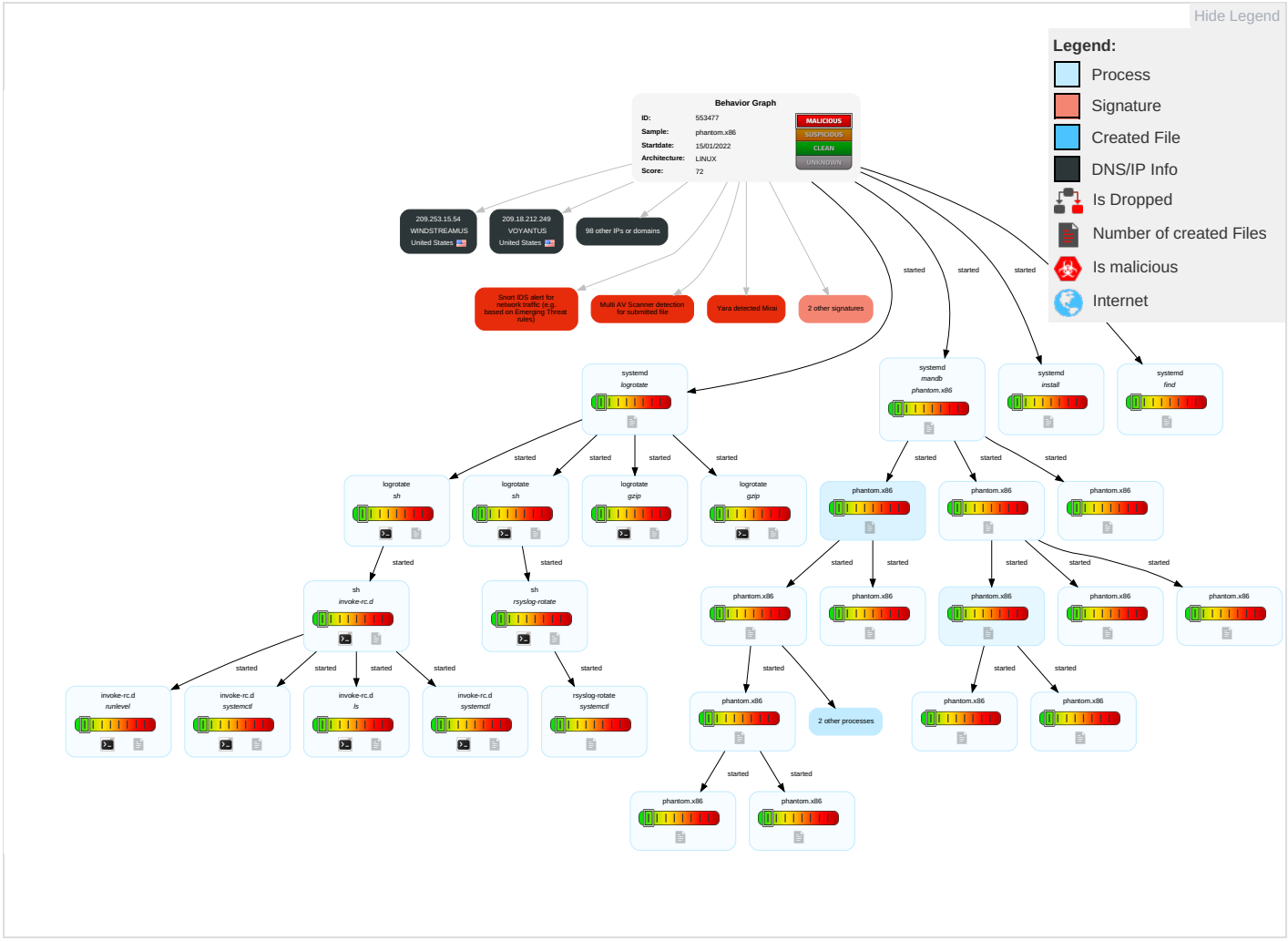
Mitre Att&ck Matrix

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	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	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
phantom.x86	37%	Virustotal		Browse
phantom.x86	51%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.46.153.9	unknown	United States		1252	UNMC-ASUS	false
138.214.135.26	unknown	Canada		59121	AKNWS-NETAsahiKaseiNetworksCorporationJP	false
191.181.205.173	unknown	Brazil		28573	CLAROSABR	false
186.180.66.200	unknown	Colombia		27831	ColombiaMovilCO	false
35.218.99.155	unknown	United States		19527	GOOGLE-2US	false
174.223.172.50	unknown	United States		22394	CELLCOUS	false
92.14.197.230	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
203.183.154.92	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
63.190.130.133	unknown	United States		1239	SPRINTLINKUS	false
155.106.187.197	unknown	United States		7018	ATT-INTERNET4US	false
168.165.75.76	unknown	Mexico		37179	AFRICAINXZA	false
200.133.204.145	unknown	Brazil		1916	AssociacaoRedeNacionaldeEnsinoePesquisaBR	false
247.16.190.72	unknown	Reserved		unknown	unknown	false
44.148.157.125	unknown	United States		62383	LDS-ASBE	false
146.24.28.224	unknown	United States		197938	TRAVIANGAMESDE	false
73.45.72.12	unknown	United States		7922	COMCAST-7922US	false
62.215.147.93	unknown	Kuwait		21050	FAST-TELCOKW	false
111.197.113.115	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
209.253.15.54	unknown	United States		7029	WINDSTREAMUS	false
248.250.22.44	unknown	Reserved		unknown	unknown	false
250.135.211.1	unknown	Reserved		unknown	unknown	false
58.6.174.54	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
130.227.167.221	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
167.100.152.214	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
185.57.37.64	unknown	United Kingdom		202206	MOTIVEGB	false
70.153.237.61	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
181.7.145.113	unknown	Argentina		7303	TelecomArgentinaSAAR	false
185.255.158.224	unknown	Denmark		60111	ASOM-NETDK	false
35.15.136.181	unknown	United States		36375	UMICH-AS-5US	false
155.28.153.184	unknown	United States		1556	DNIC-ASBLK-01550-01601US	false
254.164.185.124	unknown	Reserved		unknown	unknown	false
20.79.32.82	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
190.141.21.40	unknown	Panama		18809	CableOndaPA	false
60.168.40.14	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
27.229.140.235	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
136.255.15.129	unknown	Romania		12302	VODAFONE_ROCharlesdeGaullenr15RO	false
162.79.89.113	unknown	United States		4152	USDA-1US	false
221.64.244.54	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
36.33.212.92	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
80.36.57.53	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
213.161.228.235	unknown	Norway		15765	MIMERNO	false
42.119.44.71	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	false
96.132.29.69	unknown	United States		7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
221.20.125.203	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
241.254.232.178	unknown	Reserved		unknown	unknown	false
210.48.235.19	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
195.129.27.188	unknown	European Union		702	UUNETUS	false
160.75.166.103	unknown	Turkey		9095	IstanbulTeknikUniversitesiTR	false
193.194.39.59	unknown	Morocco		6713	IAM-ASMA	false
200.176.169.253	unknown	Brazil		22548	NucleodeInfeCoorddoPontoBR-NICBR	false
187.252.127.109	unknown	Mexico		28509	CablemasTelecomunicacionesSAdeCVMX	false
185.11.6.125	unknown	Russian Federation		15493	RUSCOMP-ASRussiancompanyLLCInternetServiceProviderT	false
157.227.65.58	unknown	Australia		4704	SANNETRakutenMobileIncJP	false
76.43.0.141	unknown	United States		18494	CENTURYLINK-LEGACY-EMBARQ-WRBGUS	false
157.139.187.2	unknown	United States		20252	JSIWMCUS	false
80.142.180.154	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
48.11.58.244	unknown	United States		2686	ATGS-MMD-ASUS	false
63.155.197.20	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
253.72.75.120	unknown	Reserved		unknown	unknown	false
116.72.42.120	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	false
151.219.242.134	unknown	unknown		11003	PANDGUS	false
133.118.92.141	unknown	Japan		2522	PPP-EXPJapanNetworkInformationCenterJP	false
169.228.186.243	unknown	United States		7377	UCSDUS	false
179.132.161.105	unknown	Brazil		26599	TELEFONICABRASILSABR	false
76.114.145.159	unknown	United States		7922	COMCAST-7922US	false
255.67.241.130	unknown	Reserved		unknown	unknown	false
117.196.164.125	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
217.60.218.162	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
96.144.25.21	unknown	United States		7922	COMCAST-7922US	false
37.135.6.37	unknown	Spain		12479	UNI2-ASES	false
82.124.221.121	unknown	France		3215	FranceTelecom-OrangeFR	false
19.157.11.236	unknown	United States		3	MIT-GATEWAYSUS	false
57.137.251.6	unknown	Belgium		2686	ATGS-MMD-ASUS	false
223.52.70.237	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
174.103.238.15	unknown	United States		10796	TWC-10796-MIDWESTUS	false
154.90.25.153	unknown	Seychelles		26484	IKGUL-26484US	false
116.87.137.130	unknown	Singapore		55430	STARHUB-NGNBNStarhubLtdSG	false
209.18.212.249	unknown	United States		5006	VOYANTUS	false
210.89.203.17	unknown	Japan		7671	MCNETNTTSmartConnectCorporationJP	false
8.127.239.179	unknown	United States		3356	LEVEL3US	false
43.24.206.124	unknown	Japan		4249	LILLY-ASUS	false
114.142.142.198	unknown	India		4721	JCNJupiterTelecommunicationsCoLtdJP	false
53.49.50.138	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
46.154.181.7	unknown	Turkey		15897	VODAFONETURKEYTR	false
182.89.214.65	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
165.77.232.33	unknown	United States		4725	ODNSoftBankMobileCorpJP	false
37.157.93.73	unknown	Estonia		3249	ESTPAKEE	false
106.31.231.3	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
182.137.131.110	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
208.63.21.65	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
162.149.162.149	unknown	United States		7922	COMCAST-7922US	false
12.134.143.230	unknown	United States		7018	ATT-INTERNET4US	false
75.8.57.219	unknown	United States		7018	ATT-INTERNET4US	false
42.75.76.247	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
83.137.220.4	unknown	Russian Federation		12739	NETLINE_ASRU	false
250.237.36.137	unknown	Reserved		unknown	unknown	false
78.222.94.138	unknown	France		12322	PROXADFR	false
198.39.146.109	unknown	United States		11857	AEGONUSAUS	false
251.237.41.157	unknown	Reserved		unknown	unknown	false
108.176.28.42	unknown	United States		12271	TWC-12271-NYCUS	false

Runtime Messages

Command:	/tmp/phantom.x86
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
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/5240	
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

/var/cache/man/5240	
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/5240	
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.04PZJq	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3: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/5240	
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:	6146001CA7028F58595235F244AE8FC4ECAEA3E95C83276514FC704E91B7596678E74CDE9963D680F2493F9C04AFDEBC4DB5094E2AB7C1A949E9378307AE0116
Malicious:	false
Reputation:	moderate, very likely benign file

/var/cache/man/da/5240	
Preview:	.W.....@..... ....

/var/cache/man/da/index.db.MDFXAr	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3: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/5240	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	4.163076275268073
Encrypted:	false
SSDEEP:	768:gMGrknsA3KVtOOcmGMrTJDEEf5RjOHriVDdtq5:/GrkncXD+qkHrGLq
MD5:	5D16F6B4EF2562C7B8F366BEA94D1522
SHA1:	A405409CEDF9AA15C403747F8C3075FBDBC213C7
SHA-256:	DC365F5FCEA0B3109C57E277B330D451D504BF2079BE732CAD5886D1CC990822
SHA-512:	933FCB662A065859D866DC047AC077AB75D6EE4120FA8B239E270F023010D50FC1D68622CA331680ED86224522954597A86A3F654792518C0FE1208B0F49B4B5
Malicious:	false
Reputation:	low
Preview:	.W..... ....

/var/cache/man/de/index.db.4iy15q	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	55880A8B73FD160B73198E09A21C83DB
SHA1:	5EB780702D2501747AF46F7525EF5C635EC5E64C
SHA-256:	66BD4C98AF40E2E208AC102ACD0F555A6C118E7258D91B833BE1D53EBFFB7BBB
SHA-512:	388924B8CAE80CCA6CA8E5109D0239A963A66CC0454450223EC7FB2A188F6F05E49632E535DC06E49DF6D007B221AA6B3D5F23C80203BCC861FF95EFA10AC1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.W.....@..... ....

/var/cache/man/es/5240	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit

/var/cache/man/es/5240	
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.2o04wp	
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/fi/5240	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.5882948808594274
Encrypted:	false
SSDEEP:	12:Ey20yaajjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjjjjp:bhjz+9Ab
MD5:	09F6ED1A60B8A4203EA97CF5926C6AFF
SHA1:	C28F4E393D55AD057E3C7608741904B796F67076
SHA-256:	56664D61D0BB8BF34CCA28C73CB314CB73EA1C4FAC64D2208B43F63C009FC855
SHA-512:	476EAE37D827C8BB322213799AB52DBE8FA43274DB3447BC5FEDFED64ECCEAF2C11DA375FDA09B37977D03CA1910E22443B22A3EEA875CE6F3BC698F8ADC0 0E2
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fi/index.db.et0KPr	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false

/var/cache/man/fi/index.db.et0KPr	
Preview:	.W.....@..... ....

/var/cache/man/fr.ISO8859-1/5240	
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:Ey20ylpyjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.ISO8859-1/index.db.dxxXfs	
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/fr.UTF-8/5240	
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:Ey20ylpyjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.UTF-8/index.db.n5c34p	
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/fr.UTF-8/index.db.n5c34p	
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/fr/5240	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	3.8303945862002498
Encrypted:	false
SSDEEP:	768:A4VX6Bd+dla5HmdT8qHl87BaIPay4uz8HksjHnwNO:A4ROd+dStM83PavjHC
MD5:	839C7639B0946E9882FE70633B0A5E8E
SHA1:	AA58A11EBCC8D421E4A054C1782D25C86B026ADB
SHA-256:	FD8D1952430FA9C45320574478B04381F7B287A8E3ADA2EB1F72E9948B0B734B
SHA-512:	AE280AC0F3337B9B1C2FB401DC073E96C5AC634AC7BE3F6FBBF64D0CBF4D9D68B6282DA95C9CF961624D475F03638408CAC3F8C618BC7F8F3CC2DD35B5499DD
Malicious:	false
Preview:	.W..... ....

/var/cache/man/fr/index.db.51Vzdp	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	40960
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/5240	
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:	E33A8412F52D26BDE55E4D72E0D9D09EB777F4B882F5BB1C4625AB392EE321D6ACD8795001BF50CCDACFAC131A1263B1398F208799F753554C43349136EB8BEC
Malicious:	false

/var/cache/man/hu/5240	
Preview:	.W.....@..... ....

/var/cache/man/hu/index.db.EAVros	
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/id/5240	
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
Preview:	.W.....@..... ....

/var/cache/man/id/index.db.gNViRp	
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/index.db.b6qNrs	
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

/var/cache/man/index.db.b6qNrs	
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	2E442DBA85DEDFDCB07090FDF9DE90D0
SHA1:	02658086E93854D13D82B1F0D80F4B78D26DCA51
SHA-256:	62406BFE7657964E490DE65A0007F7C1D59B62B2B9AD35BA55BA219673378848
SHA-512:	FDBBA0DEF310CF7DBF448CFB6E5C9CDCEFBF6A0CAEB26CA3AFA91A388FBA10A9E77BCC27CA9B0AEA2A7B67F964849E147FB44862C7394C2C7CDCB572C06FCB05
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/it/5240	
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.mBfOlp	
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/ja/5240	
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
Malicious:	false

/var/cache/man/ja/5240	
Preview:	.W.....P..... ....

/var/cache/man/ja/index.db.i6ZXop	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/ko/5240	
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:Ey20yYn0jjjjjjjjjjjjjjjjjjjjjjjGjjjjjjjjjjjjjjjjjjjjjmjj7:bhXYznMk31RFe6f
MD5:	FBA25855E1C99D8F87E8AC13E2E2ECB1
SHA1:	D99351AC40D6CC4C9BE54E0E018C44A9A88983D7
SHA-256:	C0E18ED1CEFF427FD4D57D1B79CE1AF7320AC8453BAF8A0349C08267464C4D71
SHA-512:	0969DF6506E083A4995A18518BC3C4472157E7790EEC26C08221B0FC6DE9C7DA0ADB11CF92C56BC35B89BC60447F3D991F935E352552B58FB9BD1D4B2579FBE
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/ko/index.db.oWMJuq	
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/nl/5240	
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

/var/cache/man/nl/5240	
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.aTrbws	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/pl/5240	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.880948418505059
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.wmVpkp	
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/pl/index.db.wmVpkp	
Preview:	.W.....@..... ....

/var/cache/man/pt/5240	
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.JG93tq	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/pt_BR/5240	
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.ujAt8r	
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/pt_BR/index.db.ujAt8r	
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/ru/5240	
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.umdRNo	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	0.3337394253577246
Encrypted:	false
SSDEEP:	12:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	5B66CE03BFE548DEE335E0518E4E0554
SHA1:	65397845DC679AA972454B0FF237A513C0F490CB
SHA-256:	C38BB21B1D92166794DC09807C9A55B67B0A760C684FEEDD0C931F8415DD6D29
SHA-512:	A31C3D23F25607333250443490F0EE295BB702B46A636905FD413E8AEAA8ED23AAB42106868D2938718555C9DEEFB69FB416CAF5228A422F64D6CA8DB438FEE
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sl/5240	
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:Ey20y8jjjjjjjjjjjjjjjjjjjjjGjjjKuV0jjjjjjjjjjjjjjjjjje:bhaVZjx6ot7m13SmZQs
MD5:	67697BEA7C23E4805A82FE9755BB3CAE
SHA1:	14ACAFF0BECBDB116E4C0BC329E59DEF68CF46D1
SHA-256:	553DA7FF76999B7CCC4450498B11E6BD98B3B1E5FF81D82A53568F84B0D270D5
SHA-512:	D966DD6430003E708C6EE10764DC072A1ED0A252E6E1C822CBD28271A2EDD4B1F61C7F9AA7D1D442D6175791A104A365DE25B9C2598500AE705C9250C8BA46 1
Malicious:	false

/var/cache/man/sl/5240	
Preview:	.W.....@..... ....

/var/cache/man/sl/index.db.wWPVwo	
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/sr/5240	
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
Preview:	.W.....@..... ....

/var/cache/man/sr/index.db.dPeBKr	
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/sv/5240	
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

/var/cache/man/sv/5240	
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.VTorKr	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/tr/5240	
Process:	/usr/bin/mandb
File Type:	GNU dbm 1.x or ndbm database, little endian, 64-bit
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.7558188637474321
Encrypted:	false
SSDEEP:	96:bhWV1OIM7cn3UZiPU1wywyoEpJmz6W2Mzgg:YDOL4n3fPvywrzgMU
MD5:	5F905B930E7310E72BC3DF5C50F8E579
SHA1:	50B1AD3115F095C743CB26F87ECCE406FAC3523B
SHA-256:	1DB72BA77CA01F25CA9768999825D8F97F5ED4D00E17C9130D6F7CDE34130270
SHA-512:	A6066F4DF4097DB93673CD156BBE5F910C3F64D01E1671E481BC9FBDD720DBD6F8CEF337E20404F7C6AE97B2FA1F5E67088041ACBB6EA85D6758924D5740D0C
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/tr/index.db.1oKdtr	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false

/var/cache/man/tr/index.db.1oKdtr	
Preview:	.W.....@..... ....

/var/cache/man/zh_CN/5240	
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.U2VzYp	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	EE429C7E8B222AFF73C611A8C358B661
SHA1:	DA353E80DCF1195F259CCBC32D39F5923710453F
SHA-256:	BDAAC26D90701E063943763B7CBD9204B6F0007C6F1BCA3C7B4FE3B09CDF6091
SHA-512:	DC651AF7AEB4A64C63986100E416A7DA4782678497B73F1CE42536DE02DB9E4115748881A56B86EC5B12E34C9FDF829BD194BEA7790FDCA7B2F5178A2493080
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/zh_TW/5240	
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:bhAvIZuF4ptmpzf50dhOv8WvxjMMhFmMKxevOfOots+:bhDi4p+ahOhFFKxewj
MD5:	1FC5F2B98E5BC25B10373353D91B86B1
SHA1:	D848DA35B0731328195D59C1E996B95C4952F1F9
SHA-256:	509FAD18B4454CD70D974755F6156D4A5FA9B960AB9FF468D1FC350F0B64F379
SHA-512:	95BC2E289EDE5D9A3F56C9D8AE9DD13D9379BE2ABF8927CDABBE92B9F57A8EB667E9C08E4DFD82BF9F1F57118CE6E495722ADA2668AFF4FA0540F46C0A6D5 138
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/zh_TW/index.db.jmvRhq	
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/zh_TW/index.db.jmvRhq	
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/lib/logrotate/status.tmp	
Process:	/usr/sbin/logrotate
File Type:	ASCII text
Category:	dropped
Size (bytes):	1607
Entropy (8bit):	4.791993862575465
Encrypted:	false
SSDEEP:	48:UrKqJFNFr0J+K5Npq4pNMJNcsXNU3N6NA515xrtNq4wNZNDNU1LN3o9NhqJNCNqQ:krwdm4puxe3Mm7A4wTteJY+nCA5eC9kR
MD5:	CF9182FDFD94B0BCDB7F2553DF1DC551
SHA1:	08222EAF783C4AE9906DBDF385C7B8AAED167046
SHA-256:	B7A197E756497652FEE95B841822FDA8E6E1A9D4B2D9A347E1F4D30BB71C8789
SHA-512:	508AD8171C43CFF82C078921CA20AA87E08D60445011E1549FC2B6736DFA94545A2E4038D13205C0BF977267922A32B563DB8E6FB5A642A2B2215B235CC13012
Malicious:	false
Preview:	logrotate state -- version 2."/var/log/syslog" 2022-1-15-0:35:32."/var/log/dpkg.log" 2022-1-14-23:35:5."/var/log/speech-dispatcher/debug-flite" 2021-8-20-13:0:0."/var/log /unattended-upgrades/unattended-upgrades.log" 2022-1-14-23:35:5."/var/log/unattended-upgrades/unattended-upgrades-shutdown.log" 2021-9-17-9:23:29."/var/log/auth .log" 2022-1-14-23:35:5."/var/log/apt/term.log" 2022-1-14-23:35:5."/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" 2022-1-14-23:35:5."/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" 2022-1-14-23:35:5." /var/log/cups/access_log" 2022-1-15-0:35:32."/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/da

/var/log/cups/access_log.1.gz	
Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Fri Jan 14 23:35:05 2022, from Unix
Category:	dropped
Size (bytes):	196
Entropy (8bit):	6.96530059658896
Encrypted:	false
SSDEEP:	3:FtqHMmAqGbnDuUY5y2lCoX23wQ9x8JQtP022yQCMv+bN0fJcWDW3rJ5iNNvOXuz7:X8M3b72lCpvoJQN6Y0RfK3t5bs/z/
MD5:	0B7715182028BFCD7DFFE389C83FD123
SHA1:	8DCE0D2F2260EF4F5A54463FFAEDC9C4A37A0783
SHA-256:	BAE868BDB99D1C4BB9ABD70377BA355E746371AEB12ABF2F7ECE154668CDC7B4
SHA-512:	A08B9004FDCEAB79CC697A43A50F93A7146645576961EE1E5F0DA6C81FCFFF43BF0A088C0EEEB1C8FC6C762DF44C05DE6A20633013A5D8684D315DB7719331 B
Malicious:	false
Preview:	.....a.....0.....jj.@.+.q..6....i...l.....'.E..7..d.....L.....(..= .oM...m[S~....@..T^wQ.....'....l.t.....-.....x~.....3&..e.^.8p!.....x.UZ.V$e.v.h.....8.....v..*...

/var/log/syslog.1.gz	
Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Fri Jan 14 23:35:05 2022, from Unix
Category:	dropped
Size (bytes):	2962
Entropy (8bit):	7.922956020325171
Encrypted:	false
SSDEEP:	48:X8Mf7UUomMM4Vtn/Bvc8HLlsnSbXFFKGUE1XtRRSEUE5mp5tMWdwJB4HhEks:smUUgJVtnnlsnSrFFKGUExR7h5mdpdEX
MD5:	2924AB701C776FB82B82054459D86A61
SHA1:	BA6FA91B3F40B088297A1ADCA92BE3F9064FB4CC
SHA-256:	A772E6582E163B5759FED128D249B1385D147C9E18AF7643D3519CDA8A52F3A5
SHA-512:	CEACEF450D3216EACFBF8315346C65341E26626A48369266555EAE5D61ECE4615EE1D9008CE257360D1E131937916CC3F7FEFCF941ABDBE993B3AE57521AD2 1
Malicious:	false

/var/log/syslog.1.gz	
Preview:	.....a...\is...._...'...-R3.L....g.(.n..x ..X..C..._.....R..~.!..{_ ....Gf8.....)N1..F...)...t.d.P..D.qA...o...o....C-0l..SCwz..C..:..N.P....A.7...r#b..}E..1G..zI....G...+.....,..Iq.Dd.Fe.....P.8 Oh.g$F.+ ..&IJ...|.s..QJ0=.#o%..E.....1&..W.~...j..5..O.4.G8..-.....ScRH>..`.1..y|...H.B..'E&...R...'...d....BS.ND4K..eD`..h.*QLk..`...9M..yo. i.e.1...o.....`.w8.m.p. SBI.E.Mf.L).%.....^.04.....y... r..-_...d...CH.|h.._.....;.....x..t&....j..$o.@.k*5..`./.1cb.....p7..1. .....i.@..4....F.Z.....b..,..`:.$Nx..{.,..*.H..X..+..<....x.%..v.d..)....-*....[.&1.....'.$..... e4...X..Z.H..~....O\.I.....3&.(.,.G...."..0pC.D.{A.K$..8.....nz.{...z.e.fd;.K.@w]..C....M...>."....F.....}.r.....L.Y....nO.x.'.....?Yy....?...8.xs.....[.....~~./.?of.A.V...M...1... .h...q.....Z..`..A...]<..o.8...#k..G 3...e.S6.<k."L).h.d...4..E.s.o...8....0.@{...[..._..L]....9...9...+....,.I....'.<.i.x.!."...1..9...g..7H. .A5|...." .D^$T 6....

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.870193950774575
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	phantom.x86
File size:	24728
MD5:	8bb140fe0754eee2498279f9f1830368
SHA1:	0146917808c967dd97899cd5259de170b67af87b
SHA256:	217a622a111c0d13237c660259617cb1e31943d74a1767a933ddee8ae0b445ac
SHA512:	52a23adbbfd3cade7830976b6e0d64d149593293f7f7ab46f54dd0bc3616f8bf1648ba8ed26382e58ff14886115d1c18ba497d80016fa83ee49790075c57296c
SSDEEP:	768:R/QOC0Yhn6RODyFd4cwNEFCnNBml1YHtfXcs:R/nihnuFnwTNBuktfss
File Content Preview:	.ELF.....g..4.....4. ...(....._...._.....W...W.....Q.td.....tUPX!.....Z.....?d..ELF.....d.....4.,..4. (.....k.-.#.`.....?..P.....d..l

Static ELF Info

ELF header

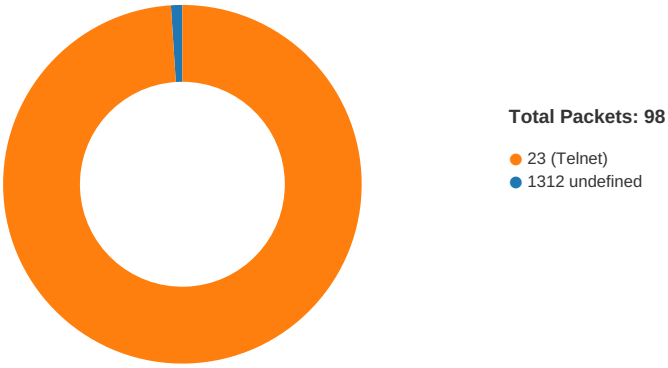
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xc067a0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program 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	0xc01000	0xc01000	0x5f9b	0x5f9b	4.5630	0x5	R E	0x1000		
LOAD	0x700	0x8055700	0x8055700	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: systemd PID: 5192 Parent PID: 1

General

Start time:	00:35:31
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5192 Parent PID: 1

General

Start time:	00:35:31
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: 5233 Parent PID: 5192

General

Start time:	00:35:32
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5233 Parent PID: 5192

General

Start time:	00:35:32
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: 5236 Parent PID: 5192

General

Start time:	00:35:32
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5236 Parent PID: 5192

General

Start time:	00:35:32
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: 5237 Parent PID: 5236

General

Start time:	00:35:32
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5237 Parent PID: 5236

General

Start time:	00:35:32
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: 5238 Parent PID: 5237

General

Start time:	00:35:32
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: 5238 Parent PID: 5237

General

Start time:	00:35:32
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: 5239 Parent PID: 5237

General

Start time:	00:35:32
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: 5239 Parent PID: 5237

General

Start time:	00:35:32
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: 5242 Parent PID: 5237

General

Start time:	00:35:34
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: 5242 Parent PID: 5237

General

Start time:	00:35:34
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: 5243 Parent PID: 5237

General

Start time:	00:35:34
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: 5243 Parent PID: 5237

General

Start time:	00:35:34
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: 5244 Parent PID: 5192

General

Start time:	00:35:34
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5244 Parent PID: 5192

General

Start time:	00:35:34
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: 5245 Parent PID: 5192

General

Start time:	00:35:34
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5245 Parent PID: 5192

General

Start time:	00:35:34
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: 5246 Parent PID: 5245

General

Start time:	00:35:34
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: 5246 Parent PID: 5245

General

Start time:	00:35:34
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: 5247 Parent PID: 5246

General

Start time:	00:35:34
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: 5247 Parent PID: 5246

General

Start time:	00:35:34
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: 5193 Parent PID: 1

General

Start time:	00:35:31
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: 5193 Parent PID: 1

General

Start time:	00:35:31
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: 5232 Parent PID: 1

General

Start time:	00:35:31
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: 5232 Parent PID: 1

General

Start time:	00:35:31
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: 5240 Parent PID: 1

General

Start time:	00:35:32
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: 5240 Parent PID: 1

General

Start time:	00:35:32
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

Analysis Process: phantom.x86 PID: 5278 Parent PID: 5117

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	/tmp/phantom.x86
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5279 Parent PID: 5278

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

File Activities

File Read

Directory Enumerated

Analysis Process: phantom.x86 PID: 5372 Parent PID: 5279

General

Start time:	00:38:32
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5374 Parent PID: 5279

General

Start time:	00:38:32

Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5375 Parent PID: 5374

General

Start time:	00:38:32
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5381 Parent PID: 5375

General

Start time:	00:38:37
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5382 Parent PID: 5375

General

Start time:	00:38:37
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5376 Parent PID: 5374

General

Start time:	00:38:32
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5377 Parent PID: 5374

General

Start time:	00:38:32
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5280 Parent PID: 5278

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5281 Parent PID: 5278

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5282 Parent PID: 5281

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

File Activities

File Read

Directory Enumerated

Analysis Process: phantom.x86 PID: 5371 Parent PID: 5282

General

Start time:	00:38:32
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes

MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5373 Parent PID: 5282

General

Start time:	00:38:32
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5283 Parent PID: 5281

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368

Analysis Process: phantom.x86 PID: 5284 Parent PID: 5281

General

Start time:	00:35:43
Start date:	15/01/2022
Path:	/tmp/phantom.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	8bb140fe0754eee2498279f9f1830368