ID: 553480
Sample Name: SGEgzPdjRk
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:47:53
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

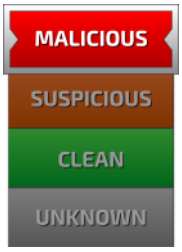
Linux Analysis Report SGEgzPdjRk

Overview

General Information

Sample Name:	SGEgzPdjRk
Analysis ID:	553480
MD5:	bac2f57ce5018c3..
SHA1:	2506edaa267c8b..
SHA256:	bcdcdf35b7e12a8..
Tags:	32 elf mips mirai
Infos:	

Detection

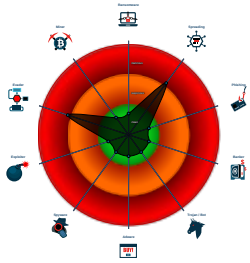


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Sample tries to kill multiple processe…
- 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…
- Sample listens on a socket
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553480
Start date:	15.01.2022
Start time:	00:47:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SGEgzPdjRk
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:	mal56.spre.evad.lin@0/53@0/0

Process Tree

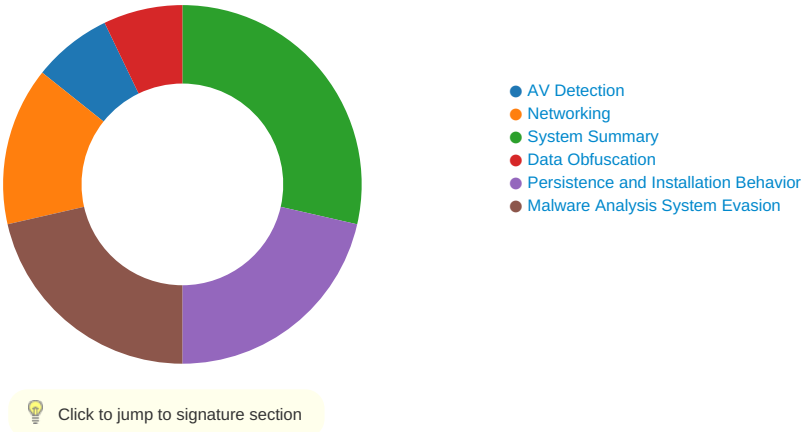
Copyright Joe Security LLC 2022

- **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: 5234, Parent: 5192)
  - sh (PID: 5234, 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: 5235, Parent: 5234)
    - invoke-rc.d (PID: 5235, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5236, Parent: 5235)
      - runlevel (PID: 5236, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5239, Parent: 5235)
      - systemctl (PID: 5239, Parent: 5235, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5242, Parent: 5235)
      - ls (PID: 5242, Parent: 5235, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5243, Parent: 5235)
      - systemctl (PID: 5243, Parent: 5235, 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
- SGEgzPdjRk (PID: 5281, Parent: 5107, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/SGEgzPdjRk
  - SGEgzPdjRk New Fork (PID: 5283, Parent: 5281)
  - SGEgzPdjRk New Fork (PID: 5284, Parent: 5281)
  - SGEgzPdjRk New Fork (PID: 5285, Parent: 5281)
    - SGEgzPdjRk New Fork (PID: 5289, Parent: 5285)
    - SGEgzPdjRk New Fork (PID: 5291, Parent: 5285)
    - SGEgzPdjRk New Fork (PID: 5293, Parent: 5285)
    - SGEgzPdjRk New Fork (PID: 5342, Parent: 5285)
      - SGEgzPdjRk New Fork (PID: 5344, Parent: 5342)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview



AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation:

Sample is packed with UPX

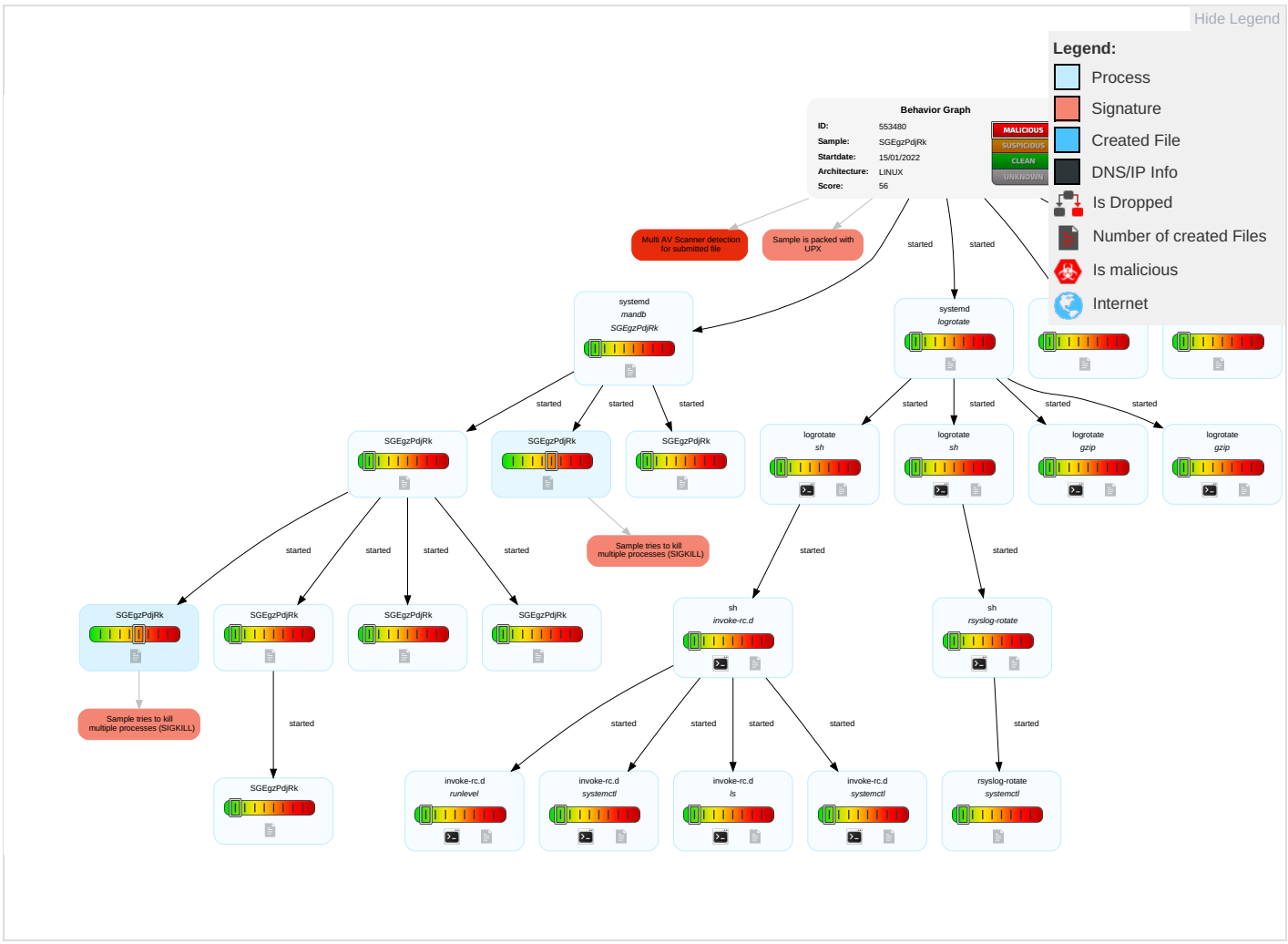
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
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	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Syst Part
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock
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	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Dele Devi Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SGEgzPdjRk	25%	Virustotal		Browse
SGEgzPdjRk	35%	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

No contacted IP infos

Runtime Messages

Command:	/tmp/SGEgzPdjRk
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
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.jXqXSr	
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/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
Preview:	.W.....@..... ....

/var/cache/man/da/index.db.138Yms	
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

/var/cache/man/da/index.db.138Yms	
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):	4.16308917006812
Encrypted:	false
SSDEEP:	768:gMGrknsA3KVtOOcmGMrTJDEEf5R1OHhiVDdtq5:/GrkncXD+qmHhGLq
MD5:	EA52C9E6E4422CD44CFB274A7BBC2EF2
SHA1:	9476C1D7DECEA272043517CB0B5F25F59563FD04
SHA-256:	C8706AC2DD72D0337A1242F3C7E88D8880478A2569D8BDE4B3598CDDA30CC17C
SHA-512:	1779F8E486C193BE2D751C94576456D0FEE52EEA81C63043FC5F4672490A9876252F96BF7B1E5ADFA30027293F605311A26F2B98578E5423A59005A441D693D1
Malicious:	false
Reputation:	low
Preview:	.W..... ....

/var/cache/man/de/index.db.sI6NCp	
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:	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
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

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

/var/cache/man/es/index.db.h1ygwq	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3: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.CYTRGq	
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.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

/var/cache/man/fr.ISO8859-1/5240	
Entropy (8bit):	0.9312184489410064
Encrypted:	false
SSDEEP:	12:Ey20yIpyjjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/fr.ISO8859-1/index.db.cYBTBq	
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/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:Ey20yIpyjjjjjjjjjjjjjjjjjjjjjjjXjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjGz7:bhbpFi043WmkN2GmGufUeDDx+yxrq3
MD5:	43ADE2E40B8B5A0DFA0A155FC9A02F7F
SHA1:	3D04BDFFD0E2A8433150C87D334014099336A5C5
SHA-256:	81E48EE4653A5E6F25C33133F24F045EB1EB2CC6724ECE0C5336612AB711273E
SHA-512:	C9C5C436A0E986A39CE3FA1CAF15A92D509F4450744BAE0283204B58CDD6FE9B8EEB8D3E2CAFB4B1ACB46729317FFAEFE86B0DD2D60472CAB30B204CC2003B03
Malicious:	false
Preview:	.W.....@..... ....

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

/var/cache/man/fr.UTF-8/index.db.staMSr	
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):	3.8303353466047136
Encrypted:	false
SSDEEP:	768:A4VX6Bd+dla5HmdT8qHl87BaIPay4uz8HkszHnwNO:A4ROd+dStM83PavzHC
MD5:	A59D183876E7FD34D1B9FC7A7A96BAA9
SHA1:	DC64603903514A89CD73FC1C856DA86D2E7EEE8C
SHA-256:	1FB7E0D49FA373091E02614554FD285AF6F41E7AEBCFD0768E197B08B59A3362
SHA-512:	6C83D65939ABCE4EC648FFCAC4D7EF72B570FDDE04AC6AF9690C991B368A3929662FBD7B953A0E0F544923429CC86A159FCD8FB43E5E58CB63FC03DAD1568 6
Malicious:	false
Preview:	.W..... ....

/var/cache/man/fr/index.db.vp8Oes	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3: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:	E33A8412F52D26BDE55E4D72E0D9D09EB777F4B882F5BB1C4625AB392EE321D6ACD8795001BF50CCDACFAC131A1263B1398F208799F753554C43349136EB8BE C
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/hu/index.db.9RkNQq	
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/hu/index.db.9RkNQq	
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/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.OMLgop	
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/index.db.FfIscr	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	2E442DBA85DEDFDCB07090FDF9DE90D0
SHA1:	02658086E93854D13D82B1F0D80F4B78D26DCA51
SHA-256:	62406BFE7657964E490DE65A0007F7C1D59B62B2B9AD35BA55BA219673378848
SHA-512:	FDBBA0DEF310CF7DBF448CFB6E5C9CDCEFBF6A0CAEB26CA3AFA91A388FBA10A9E77BCC27CA9B0AEA2A7B67F964849E147FB44862C7394C2C7CDCB572C06FCB05
Malicious:	false

/var/cache/man/index.db.FfIscr	
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.VSKzYp	
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/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
Preview:	.W.....P..... ....

/var/cache/man/ja/index.db.VfIoao	
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/ja/index.db.Vfloao	
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/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.N9VQls	
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/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
Encrypted:	false
SSDEEP:	192:H8Y5a2oquB2aCYn3lvu3whjXVobdbs7dq1KJGbtf0Hoa:hoquYaCYn3Q8jXqbdbs7dGbKHoa
MD5:	27FED1CA8EB0101C459D9A617C833293
SHA1:	503B2A3E33FE79FF2CD58F831ED33DB358849BEA
SHA-256:	C3033C4F7CF0D6108611EF5A62CA893F98EE6463DDCFF7100D3BAFDEB0036D9E
SHA-512:	7BD630F5E0C5A91C34D2E48D0053923C9F2F5BAA07D21FDA79E60F3AFDF759E594E6639562C1F3EE68DD080D417009DC3AFB7DA534E3B8C29FF7B10438C3FDE
Malicious:	false

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

/var/cache/man/nl/index.db.oe9k9o	
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/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:	CCC8A8CCF4ACA332CAF610155DE9E7C4A12D1C45C98D20766B86098A3D2EF332189F159E3956944CD302DF652FE7A6F0D07CA39CBE7DF4A655D3211452487
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/pl/index.db.1iZcXq	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3:bh
MD5:	F0B902DEA5EF122A0B1F0F496DDC781B
SHA1:	90176D320A9C3601787D53CC346DC743367D53F1
SHA-256:	CFD64D42263C5D323AF423FC09CDB5DDB2F914114B87BAB6566EAB1020F15DE0
SHA-512:	3A5BC0E51D53A12E65441FB98E1201DC434C42DB389CFCA4C96FF65C2413CF9B06B29CC39A48BD3FDC61F4896396813E54B9C2CE404EF35AC33B35377E7188
Malicious:	false
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

/var/cache/man/pt/5240	
Encrypted:	false
SSDEEP:	192:mva8yGn35+0+eo8TAnBW4VppKP8qtRJI:Sa8Rn35+peo8T8V/fqll
MD5:	782FF89B6FA5932F7019AF9CF3F82E43
SHA1:	2ECE8DC134E3A292E2545AA2DCD24114A5FC5749
SHA-256:	01E77D9235C524F2A61EA03953607C13831C391A5B9AB0D9094F9C38F0EEB02E
SHA-512:	2305BEC024CA5D8B43267F5487B02081A0A746B73608E11217D19C91AD857B6A5D8E935194AC4228DA3A5383086E60D593095309E64BAF38841A6E32D7EA7805
Malicious:	false
Preview:	.W.....P..... ....

/var/cache/man/pt/index.db.97DJlr	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3: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.s1P5ap	
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

/var/cache/man/pt_BR/index.db.s1P5ap	
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.mQhIks	
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:Ey20ypjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj3: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:Ey20y8jjjjjjjjjjjjjjjjjjjjjjjGjjjKuV0jjjjjjjjjjjjjjjjjjje:bhaVZjx6ot7m13SmZQs
MD5:	67697BEA7C23E4805A82FE9755BB3CAE
SHA1:	14ACAFF0BECBDB116E4C0BC329E59DEF68CF46D1
SHA-256:	553DA7FF76999B7CCC4450498B11E6BD98B3B1E5FF81D82A53568F84B0D270D5
SHA-512:	D966DD6430003E708C6EE10764DC072A1ED0A252E6E1C822CBD28271A2EDD4B1F61C7F9AA7D1D442D6175791A104A365DE25B9C2598500AE705C9250C8BA46 1
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/sl/index.db.iZThrs	
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/sl/index.db.iZThrs	
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/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.CCNCvr	
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/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
Encrypted:	false
SSDEEP:	96:bhk/+fz7b9ldxbe2Vn3iwkVJIB0D6c6aZ4+1Wrzbxpl4/tMe1:imrn9lHbe2Vn3iwKhD6cvTAbl4/tMe
MD5:	D97454D6B1F39F39966A809BCA3D9647
SHA1:	276931CED8F34B7651C1BDFC8522FF0560E2C377
SHA-256:	DCB8CE7F4F21595D851100F315C56B717541DB898AEB9ED9C0CCC9FF217A5801
SHA-512:	3E014F3EA8EEE79B87726EDA6291AC2D0BD9B22803EE848F61CA2AAD39D5FB87704410C57C648EE4AF8A1B78EFB0D766524F6DB750208C9BAC346079FD8EE6 9E
Malicious:	false

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

/var/cache/man/sv/index.db.0Hu6Fr	
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/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:	A6066F4DF4097DB93673CD156BBE5F910C3F64D01E1671E481BC9FBDD720DBD6F8CEF337E20404F7C6AE97B2FA1F5E67088041ACBB6EA85D6758924D5740D0 C
Malicious:	false
Preview:	.W.....@..... ....

/var/cache/man/tr/index.db.JHMT2p	
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/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

/var/cache/man/zh_CN/5240	
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.UpDzbs	
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/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.GCJ7Fo	
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

/var/cache/man/zh_TW/index.db.GCJ7Fo	
Preview:	.W.....@..... ....

/var/lib/logrotate/status.tmp	
Process:	/usr/sbin/logrotate
File Type:	ASCII text
Category:	dropped
Size (bytes):	1614
Entropy (8bit):	4.8152687339393045
Encrypted:	false
SSDEEP:	48:UH4qJFNJr0tcK5Npq4pNeJNcsXNU3N6NA555xHtNq4wNZNDNU1LN3o9NFqJNCNqQ:krQLm4pUxe3Mm7A4wTteJY+nCA5eC9kR
MD5:	2B88968D1959AD096CBC02E95B5683DE
SHA1:	7E7D4FD580C10404DAEEDE3FF9EE169C3B46FBDF
SHA-256:	4185B50773A1AA5DCBE45F4EF77FD402B87F50678974C7415CF68A2E578AF036
SHA-512:	8A7077477455E9C94CC172DE55B1F8A42BA8354EE1604B5CE1AE3D9AE8CBE3DF1E484E6F7071B2F913EC2E65A1F7B498908967C0C841B1FDDEC1BB2E418B730
Malicious:	false
Preview:	logrotate state -- version 2."/var/log/syslog" 2022-1-15-0:48:25."/var/log/dpkg.log" 2022-1-14-23:47:59."/var/log/speech-dispatcher/debug-flite" 2021-8-20-13:0:0."/var/log/unattended-upgrades/unattended-upgrades.log" 2022-1-14-23:47:59."/var/log/unattended-upgrades/unattended-upgrades-shutdown.log" 2021-9-17-9:23:29."/var/log/auth.log" 2022-1-14-23:47:59."/var/log/apt/term.log" 2022-1-14-23:47:59."/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" 2022-1-14-23:47:59."/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" 2022-1-14-23:47:59."/var/log/cups/access_log" 2022-1-15-0:48:25."/var/log/ufw.log" 2021-8-20-13:0:0."/var/log/speech-dispatcher/speech-dispatcher.log" 2021-8-20-13:0:0."/var/

/var/log/cups/access_log.1.gz	
Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Fri Jan 14 23:47:59 2022, from Unix
Category:	dropped
Size (bytes):	196
Entropy (8bit):	6.871094507575131
Encrypted:	false
SSDEEP:	3:Ft7HMmP0V9jACedtg3Sw3mDJJmypZKVJ1TE2Cx8JQt5eRrax+snecxB5tNGOAhGk:X7ujDedtg3SwGJJdsEgJQjIKecxPDAwk
MD5:	4B1D3531EBAC29505CEDB72A65C68E5A
SHA1:	90EE15AB1E001CBE31E6105665DC14F09B5D3911
SHA-256:	AD4D6ECDCC9E749A5220064A521942D005DACE4BC7E4D28566F053865E2999B1
SHA-512:	4B73D2BCE3B0A65A29BE7BD7C9FB31CCA7D382B145807A8C6A67BC3EDA15A40907620262F1BD955C2546BF4263620CED4C8E31BF7EE4D6606CE594E34C653F96
Malicious:	false
Preview:	.....a.....0.....jj....,.E.....M.....I.....Ug.....w^.F.T0.%+.H.(..= .oM...m[S~.... .J...&..I.4....0...R..>.....'f,+d..e...)T.U..8+.C.[....m .9t.b =F..W.x...}.tZ..*...

/var/log/syslog.1.gz	
Process:	/bin/gzip
File Type:	gzip compressed data, last modified: Fri Jan 14 23:47:59 2022, from Unix
Category:	dropped
Size (bytes):	3080
Entropy (8bit):	7.944039645242147
Encrypted:	false
SSDEEP:	96:CGdnigvESDIv4PYgiiuWLAFaT4Rj1fRYw04RZ:CGdnnvESZ3uWpsJRdZ
MD5:	E9DCC41E7337E3A07F4B1D76965AC401
SHA1:	C7BE3CA16C0877E158C00B4FFDCA350B220838C2
SHA-256:	DB62AFDCEE99648AB383DB102042AB599E9124F8873A3643158E49C8A9513F05
SHA-512:	356C5ADCAA81FB75094C019DF58D682CAAFF423C7D4490A952C8EC552D93C0D0757A17CF35A834DCB9E33C6E05240D64C332705D754613982D7452812C7C2C
Malicious:	false
Preview:	.....a...\is...../N:!...:...f7.:Q....@$$.".. -;../H].E..$..". ..>pyH2dxH....7.4...<.(..<a....Y.Ob.8..s.....MA|...<ft.....+.N..h.x.%..t...(2.....,U....9...W$.e...<Z.4.6.....Y...q...!.a...D$.. .b..)....H@.q...9>.f.p!~..L...[.#p..x/?..j.I...y.v]#....|\&.=.a....Zp..X>.....i.y.Egr.....8O.S .*TXs.....t._.N...I.Nc:A))0@`.t.0.5K.0..&.G.7^....D....7.T.FG..;..6k8....$.E.Mf.O(.JP_K.5.C9.+05``h>]...!.....A...[.B!..`..CH.|`..^.....A..@k..y\LAi.L.t&.....j.....}...4...i.....5....qH.a.a@.....t..b.%.@5..U *....Jc....o..g..GJ.P.....q..it.:..G..p....m.W.....Ee...=..I.!.O...0\P....x....#....U....Vs.,..'`o./.8.h..@..+..7..E.....w....WG....H<..q0Z.4....z.{...z.a.zhZ.Ml_.m.U.b.....vL..!..\.G..\x....e..>6..(..Q?|.T...'.....?.|.t.....w..?.sB....7.........c....).....Z1.?#6._g..8...%.....3.....8g).A...]<..n.8...%j..G S.d.eh..w...BL)+."....h...e.....Q..)!`....)...E.[.vtU....9...Y.....,+.4.."..My.....C.E*0.#4es4'.OsLg..B..j....D@..Y....1.t.

Static File Info

General	
File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.8741042811561925
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	SGEgzPdjRk
File size:	26184
MD5:	bac2f57ce5018c375edb702622eec6b9
SHA1:	2506edaa267c8bbb17dbe039f24e928fd8c386bc
SHA256:	bcdcdf35b7e12a89a6f5a44877bbc82cb53a23b863722f5a705aa8bbcea9f940
SHA512:	f4619179ceabd6c0e919a75f40ef6cf46489211265ad03caba99e94414a33a28b88a130e7198c1d9ade1daac1831a720e2933b37abab4a59b1fc1ede3031c4e3
SSDEEP:	768:DU3QyUyNoYr3MgzqAEAM01bwTJgGlzDpbuR1JP:g3QfYT9OErbiVJux
File Content Preview:	.ELF.....Q....4.....4. ...(.....e...e.....p.E.p.E.p.....UPX!.d.....U.....?.E.h4...@b..) ..]....E..X...~.N{CS...P.X~Y..m...}..1.@)O..{+s....\..%q.c..s.n...@...,..N.....

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x1051d8
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
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	0x100000	0x100000	0x651c	0x651c	4.1715	0x5	R E	0x10000		
LOAD	0x1870	0x451870	0x451870	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: systemd PID: 5192 Parent PID: 1

General

Start time:	00:48:25
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:	00:48:25
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:	00:48:25
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:	00:48:25
Start date:	15/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes

Copyright Joe Security LLC 2022

MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5234 Parent PID: 5192

General

Start time:	00:48:25
Start date:	15/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5234 Parent PID: 5192

General

Start time:	00:48:25
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: 5235 Parent PID: 5234

General

Start time:	00:48:25
Start date:	15/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5235 Parent PID: 5234

General

Start time:	00:48:25
Start date:	15/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes

Copyright Joe Security LLC 2022

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: invoke-rc.d PID: 5236 Parent PID: 5235

General

Start time:	00:48:26
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: 5236 Parent PID: 5235

General

Start time:	00:48:26
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: 5235

General

Start time:	00:48:27
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: 5235

General

Start time:	00:48:27
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: 5235

General

Start time:	00:48:27
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: 5235

General

Start time:	00:48:27
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: 5235

General

Start time:	00:48:27
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: 5235

General

Start time:	00:48:27
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:	00:48:28
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:	00:48:28
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:	00:48:28
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:	00:48:28
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

Copyright Joe Security LLC 2022

File Read

Analysis Process: sh PID: 5246 Parent PID: 5245

General

Start time:	00:48:28
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:	00:48:28
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:	00:48:29
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:	00:48:29
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:	00:48:25
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:	00:48:25
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:	00:48:25
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:	00:48:25
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

Copyright Joe Security LLC 2022

Analysis Process: systemd PID: 5240 Parent PID: 1

General

Start time:	00:48:27
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:	00:48:27
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: SGEgzPdjRk PID: 5281 Parent PID: 5107

General

Start time:	00:48:37
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	/tmp/SGEgzPdjRk
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: SGEgzPdjRk PID: 5283 Parent PID: 5281

General

Start time:	00:48:37
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: SGEgzPdjRk PID: 5284 Parent PID: 5281

General

Start time:	00:48:37
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SGEgzPdjRk PID: 5285 Parent PID: 5281

General

Start time:	00:48:37
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SGEgzPdjRk PID: 5289 Parent PID: 5285

General

Start time:	00:48:38
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Copyright Joe Security LLC 2022

Analysis Process: SGEgzPdjRk PID: 5291 Parent PID: 5285

General

Start time:	00:48:38
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SGEgzPdjRk PID: 5293 Parent PID: 5285

General

Start time:	00:48:38
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SGEgzPdjRk PID: 5342 Parent PID: 5285

General

Start time:	00:50:11
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SGEgzPdjRk PID: 5344 Parent PID: 5342

General

Start time:	00:50:11
Start date:	15/01/2022
Path:	/tmp/SGEgzPdjRk
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Copyright Joe Security LLC 2022