

JOeSandbox Cloud BASIC



ID: 562522

Sample Name: z0r0.arm7

Cookbook:

defaultlinuxfilecookbook.jbs

Time: 00:10:19

Date: 29/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Linux Analysis Report z0r0.arm7	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Analysis Advice	5
General Information	5
Runtime Messages	5
Process Tree	6
Yara Overview	6
Initial Sample	6
Memory Dumps	6
Jbx Signature Overview	6
AV Detection	6
Data Obfuscation	6
Mitre Att&ck Matrix	7
Malware Configuration	7
Behavior Graph	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
World Map of Contacted IPs	8
Public IPs	8
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASNs	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
/var/cache/man/5230	9
/var/cache/man/cs/5230	9
/var/cache/man/cs/index.db.ZCcVTE	9
/var/cache/man/da/5230	9
/var/cache/man/da/index.db.oJZlZH	9
/var/cache/man/de/5230	9
/var/cache/man/de/index.db.UOeQpH	9
/var/cache/man/es/5230	9
/var/cache/man/es/index.db.PFMh1F	9
/var/cache/man/fi/5230	9
/var/cache/man/fi/index.db.k0WU0D	9
/var/cache/man/fr.ISO8859-1/5230	9
/var/cache/man/fr.ISO8859-1/index.db.bczf6E	9
/var/cache/man/fr.UTF-8/5230	9
/var/cache/man/fr.UTF-8/index.db.04bzBE	9
/var/cache/man/fr/5230	9
/var/cache/man/fr/index.db.DHaoOH	10
/var/cache/man/hu/5230	10
/var/cache/man/hu/index.db.87moQE	10
/var/cache/man/id/5230	10
/var/cache/man/id/index.db.LIZ3aH	10
/var/cache/man/index.db.MpWjnE	10
/var/cache/man/it/5230	10
/var/cache/man/it/index.db.PvTnTD	10
/var/cache/man/ja/5230	10
/var/cache/man/ja/index.db.rb0OgH	10
/var/cache/man/ko/5230	10
/var/cache/man/ko/index.db.KU3IGH	10
/var/cache/man/nl/5230	10
/var/cache/man/nl/index.db.vCHDAG	10
/var/cache/man/pl/5230	10
/var/cache/man/pl/index.db.pGmGPH	10
/var/cache/man/pt/5230	10
/var/cache/man/pt/index.db.SE4SoH	10
/var/cache/man/pt_BR/5230	10
/var/cache/man/pt_BR/index.db.M7bnKH	10
/var/cache/man/ru/5230	10
/var/cache/man/ru/index.db.LNByAG	10

/var/cache/man/sl/5230	10
/var/cache/man/sl/index.db.FqxkzH	10
/var/cache/man/sr/5230	10
/var/cache/man/sr/index.db.jghL1G	10
/var/cache/man/sv/5230	10
/var/cache/man/sv/index.db.7Z4gNE	10
/var/cache/man/tr/5230	10
/var/cache/man/tr/index.db.vdr98F	10
/var/cache/man/zh_CN/5230	10
/var/cache/man/zh_CN/index.db.FpJ8lG	10
/var/cache/man/zh_TW/5230	11
/var/cache/man/zh_TW/index.db.wczTAG	11
/var/lib/logrotate/status.tmp	11
/var/log/cups/access_log.1.gz	11
/var/log/syslog.1.gz	11
Static File Info	11
General	11
Static ELF Info	11
ELF header	11
Program Segments	11
Network Behavior	12
Network Port Distribution	12
TCP Packets	12
System Behavior	12
Analysis Process: systemd PID: 5184, Parent PID: 1	12
General	12
Analysis Process: logrotate PID: 5184, Parent PID: 1	12
General	12
File Activities	12
File Deleted	12
File Read	12
File Written	12
File Moved	12
Directory Enumerated	12
Owner / Group Modified	12
Permission Modified	12
Analysis Process: logrotate PID: 5226, Parent PID: 5184	12
General	12
Analysis Process: gzip PID: 5226, Parent PID: 5184	13
General	13
File Activities	13
File Read	13
File Written	13
Analysis Process: logrotate PID: 5227, Parent PID: 5184	13
General	13
Analysis Process: sh PID: 5227, Parent PID: 5184	13
General	13
File Activities	13
File Read	13
Analysis Process: sh PID: 5228, Parent PID: 5227	13
General	13
Analysis Process: invoke-rc.d PID: 5228, Parent PID: 5227	13
General	13
File Activities	14
File Read	14
Directory Enumerated	14
Analysis Process: invoke-rc.d PID: 5229, Parent PID: 5228	14
General	14
Analysis Process: runlevel PID: 5229, Parent PID: 5228	14
General	14
File Activities	14
File Read	14
Analysis Process: invoke-rc.d PID: 5231, Parent PID: 5228	14
General	14
Analysis Process: systemctl PID: 5231, Parent PID: 5228	14
General	14
File Activities	14
File Read	14
Analysis Process: invoke-rc.d PID: 5232, Parent PID: 5228	14
General	14
Analysis Process: ls PID: 5232, Parent PID: 5228	15
General	15
File Activities	15
File Read	15
Analysis Process: invoke-rc.d PID: 5234, Parent PID: 5228	15
General	15
Analysis Process: systemctl PID: 5234, Parent PID: 5228	15
General	15
File Activities	15
File Read	15
Analysis Process: logrotate PID: 5235, Parent PID: 5184	15
General	15
Analysis Process: gzip PID: 5235, Parent PID: 5184	15
General	15
File Activities	15
File Read	15
File Written	16
Analysis Process: logrotate PID: 5236, Parent PID: 5184	16
General	16
Analysis Process: sh PID: 5236, Parent PID: 5184	16

General	16
File Activities	16
File Read	16
Analysis Process: sh PID: 5237, Parent PID: 5236	16
General	16
Analysis Process: rsyslog-rotate PID: 5237, Parent PID: 5236	16
General	16
File Activities	16
File Read	16
Analysis Process: rsyslog-rotate PID: 5238, Parent PID: 5237	16
General	16
Analysis Process: systemctl PID: 5238, Parent PID: 5237	16
General	17
File Activities	17
File Read	17
Analysis Process: systemd PID: 5185, Parent PID: 1	17
General	17
Analysis Process: install PID: 5185, Parent PID: 1	17
General	17
File Activities	17
File Read	17
Directory Created	17
Analysis Process: systemd PID: 5197, Parent PID: 1	17
General	17
Analysis Process: find PID: 5197, Parent PID: 1	17
General	17
File Activities	17
File Read	17
Directory Enumerated	17
Analysis Process: systemd PID: 5230, Parent PID: 1	18
General	18
Analysis Process: mandb PID: 5230, Parent PID: 1	18
General	18
File Activities	18
File Deleted	18
File Read	18
File Written	18
File Moved	18
Directory Enumerated	18
Owner / Group Modified	18
Permission Modified	18
Analysis Process: z0r0.arm7 PID: 5270, Parent PID: 5110	18
General	18
File Activities	18
File Read	18

Linux Analysis Report

z0r0.arm7

Overview

General Information

Sample Name:	z0r0.arm7
Analysis ID:	562522
MD5:	c24cfa9352c860...
SHA1:	02af344b5c50b0..
SHA256:	3c8806a64ae3a0..
Tags:	Mirai
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

Multi AV Scanner detection for subm...

Sample is packed with UPX

Sample contains only a LOAD segm...

Yara signature match

Deletes log files

Uses the "uname" system call to qu...

Executes commands using a shell c...

Executes the "systemctl" command...

Tries to connect to HTTP servers, b...

Classification

Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.
Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture.
All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.
Non-zero exit code suggests an error during the execution. Lookup the error code for hints.
Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562522
Start date:	29.01.2022
Start time:	00:10:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	z0r0.arm7
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:	mal52.evad.linARM7@0/53@0/0

Runtime Messages

Command:	/tmp/z0r0.arm7
Exit Code:	139
Exit Code Info:	SIGSEGV (11) Segmentation fault invalid memory reference
Killed:	False

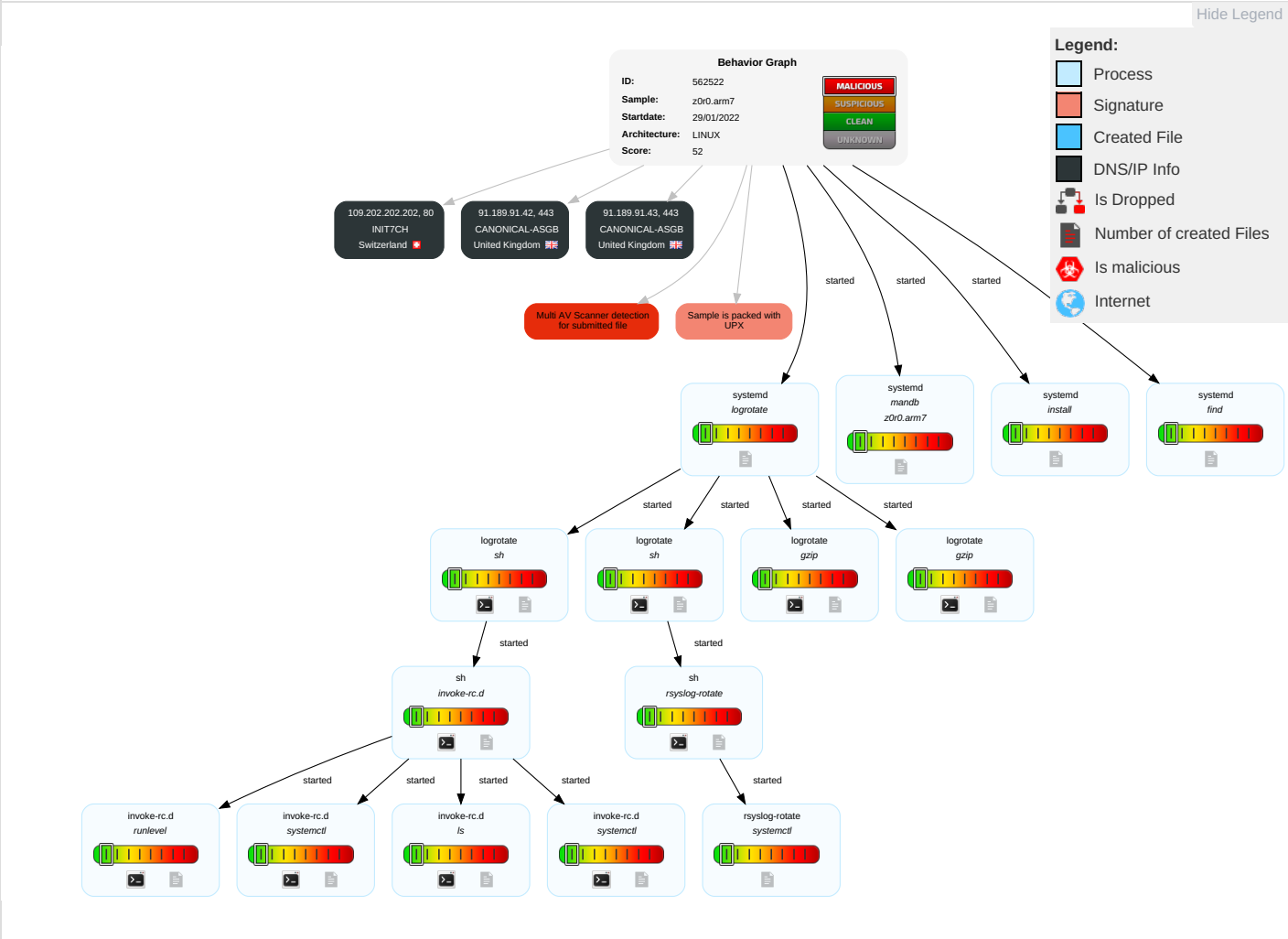
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	1 Systemd Service	1 Systemd Service	1 Scripting	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Indicator Removal on Host	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	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
z0r0.arm7	39%	Virustotal		Browse

Dropped Files

⛔ No Antivirus matches

Domains

⛔ No Antivirus matches

URLs

⛔ No Antivirus matches

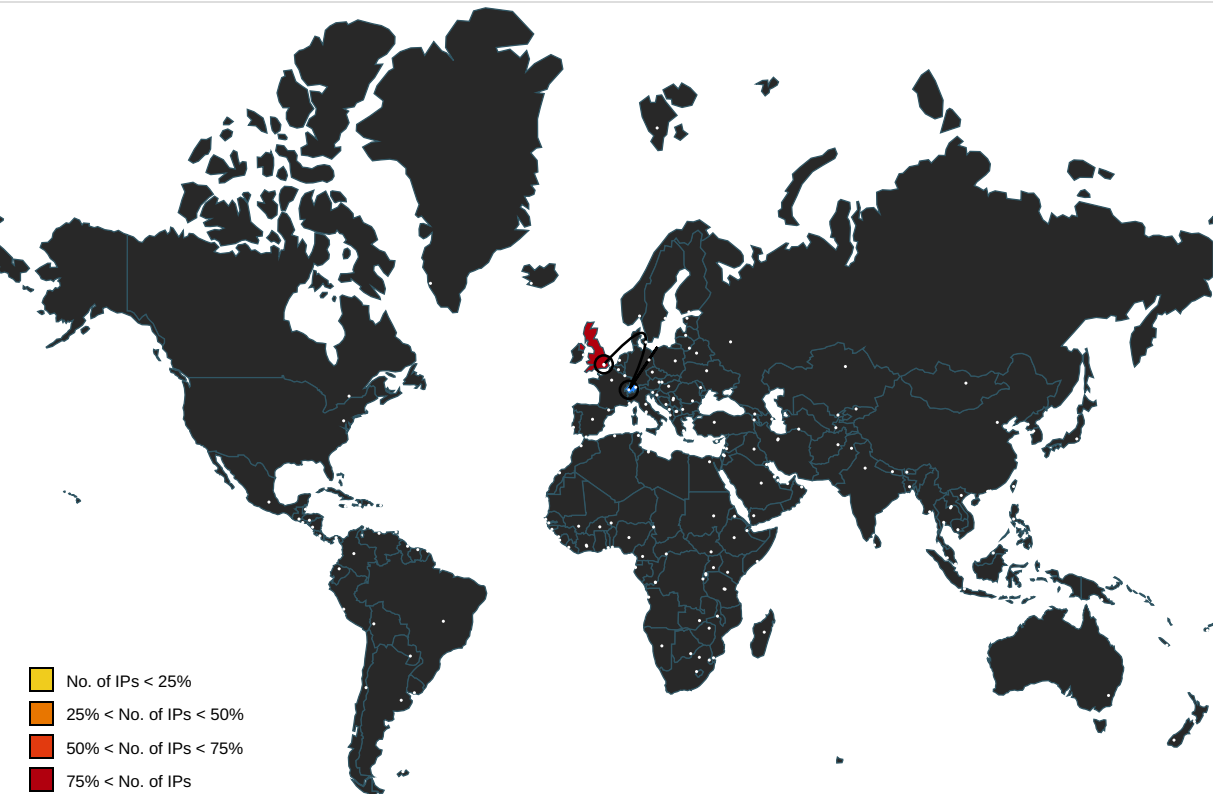
Domains and IPs

Contacted Domains

⛔ No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

/var/cache/man/5230 

/var/cache/man/cs/5230 

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

/var/cache/man/da/5230 

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

/var/cache/man/de/5230 

/var/cache/man/de/index.db.U0eQpH 

/var/cache/man/es/5230 

/var/cache/man/es/index.db.PFMh1F 

/var/cache/man/fi/5230 

/var/cache/man/fi/index.db.k0WUOD 

/var/cache/man/fr.IS08859-1/5230 

/var/cache/man/fr.IS08859-1/index.db.bczf6E 

/var/cache/man/fr.UTF-8/5230 

/var/cache/man/fr.UTF-8/index.db.04bzBE 

/var/cache/man/fr/5230 

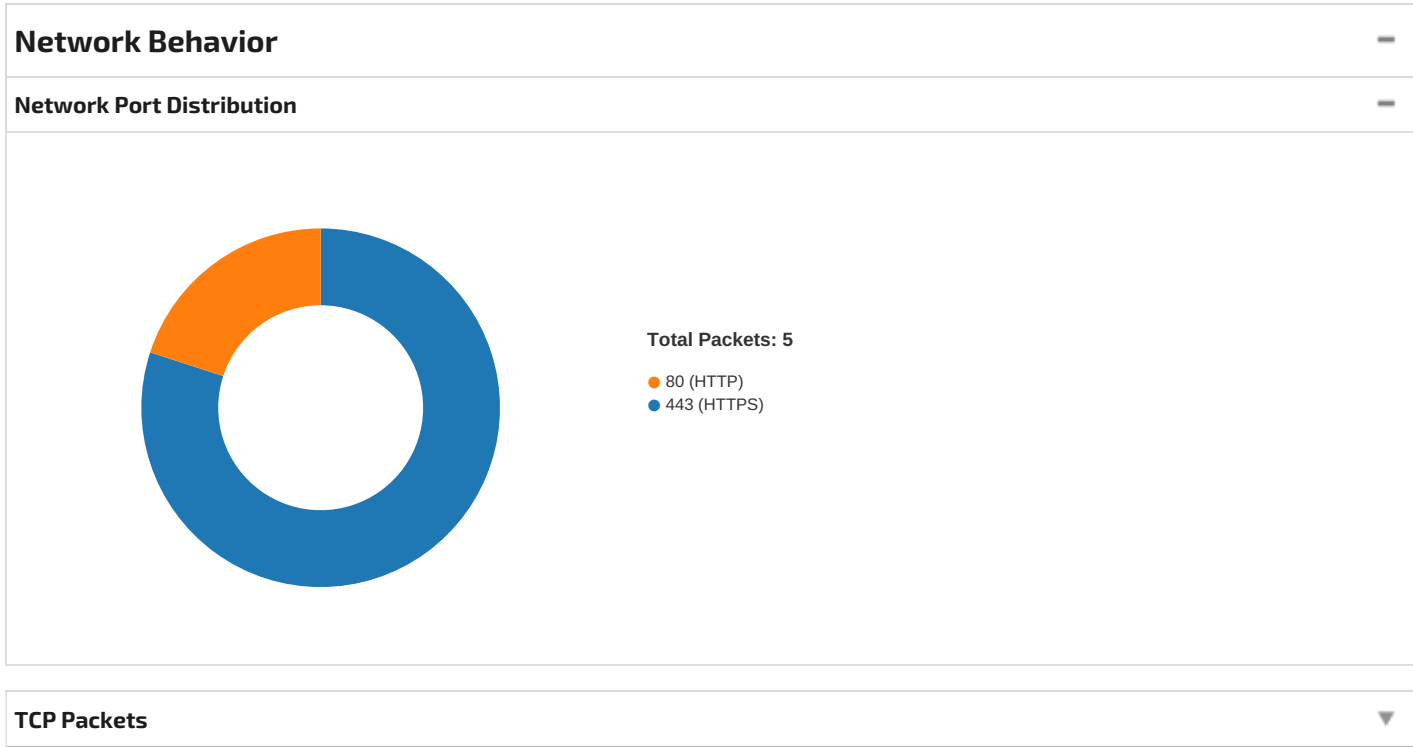
/var/cache/man/fr/index.db.DHa00H	▼
/var/cache/man/hu/5230	▼
/var/cache/man/hu/index.db.87moQE	▼
/var/cache/man/id/5230	▼
/var/cache/man/id/index.db.LI23aH	▼
/var/cache/man/index.db.MpWjnE	▼
/var/cache/man/it/5230	▼
/var/cache/man/it/index.db.PvTnTD	▼
/var/cache/man/ja/5230	▼
/var/cache/man/ja/index.db.rb00gH	▼
/var/cache/man/ko/5230	▼
/var/cache/man/ko/index.db.KU3IGH	▼
/var/cache/man/nl/5230	▼
/var/cache/man/nl/index.db.vCHDAG	▼
/var/cache/man/pl/5230	▼
/var/cache/man/pl/index.db.pGmGPH	▼
/var/cache/man/pt/5230	▼
/var/cache/man/pt/index.db.SE4SoH	▼
/var/cache/man/pt_BR/5230	▼
/var/cache/man/pt_BR/index.db.M7bnKH	▼
/var/cache/man/ru/5230	▼
/var/cache/man/ru/index.db.LNByAG	▼
/var/cache/man/sl/5230	▼
/var/cache/man/sl/index.db.FqkzH	▼
/var/cache/man/sr/5230	▼
/var/cache/man/sr/index.db.jghL1G	▼
/var/cache/man/sv/5230	▼
/var/cache/man/sv/index.db.7Z4gNE	▼
/var/cache/man/tr/5230	▼
/var/cache/man/tr/index.db.vdr98F	▼
/var/cache/man/zh_CN/5230	▼
/var/cache/man/zh_CN/index.db.FpJ8lG	▼

/var/cache/man/zh_TW/5230	▼
/var/cache/man/zh_TW/index.db.wczTAG	▼
/var/lib/logrotate/status.tmp	▼
/var/log/cups/access_log.1.gz	▼
/var/log/syslog.1.gz	▼

Static File Info		—
General		—
File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped	
Entropy (8bit):	7.980725087298671	
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%	
File name:	z0r0.arm7	
File size:	56064	
MD5:	c24cfa9352c860fa1ff5bca19dbcd304	
SHA1:	02af344b5c50b045f20f211c08552605d36583ce	
SHA256:	3c8806a64ae3a0b25d9c3ba374f2830fb3a033435277bfa9a30be9adcb36b35e	
SHA512:	69ea7869b2b7c4d9ba9465da69ea3bcd2dee445285dab4a46fb21fd6859dd7134d0133f32a18574ffe1b14c3cbc345e2b12a2e72a191134931a8c060f09406c3	
SSDEEP:	1536:O1jtGtb9eCvfB5iJn5NWONxAHm6qogbS12:O1k59d7iIJ3YibSo	
File Content Preview:	.ELF.....(....L...4.....4. ..(.....O...O.....L&.....Q.td.....x?.UPX!.....A...A....j.....?E.h;...#..\$.o...-...Au...0.*>..2/... ...L@.....;L.N..	

Static ELF Info		—
ELF header		
Class:	ELF32	
Data:	2's complement, little endian	
Version:	1 (current)	
Machine:	ARM	
Version Number:	0x1	
Type:	EXEC (Executable file)	
OS/ABI:	UNIX - Linux	
ABI Version:	0	
Entry Point Address:	0x10c4c	
Flags:	0x4000002	
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	0x8000	0x8000	0x9e4f	0x9e4f	4.0287	0x5	R E	0x8000			
LOAD	0x0	0x18000	0x18000	0x0	0x1264c	0.0000	0x6	RW	0x8000			
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4			



System Behavior

Analysis Process: systemd PID: 5184, Parent PID: 1	
General	
Start time:	00:10:52
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5184, Parent PID: 1	
General	
Start time:	00:10:52
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	/usr/sbin/logrotate /etc/logrotate.conf
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

File Activities	
File Deleted	
File Read	
File Written	
File Moved	
Directory Enumerated	
Owner / Group Modified	
Permission Modified	

Analysis Process: logrotate PID: 5226, Parent PID: 5184	
General	
Start time:	00:10:53
Start date:	29/01/2022

Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5226, Parent PID: 5184

General

Start time:	00:10:53
Start date:	29/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities

File Read

File Written

Analysis Process: logrotate PID: 5227, Parent PID: 5184

General

Start time:	00:10:53
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5227, Parent PID: 5184

General

Start time:	00:10:53
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	sh -c "\n\t\tinvoke-rc.d --quiet cups restart > /dev/null\n" logrotate _script "/var/log/cups/*log "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5228, Parent PID: 5227

General

Start time:	00:10:53
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: 5228, Parent PID: 5227

General

Start time:	00:10:53
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	invoke-rc.d --quiet cups restart
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c
-----------	----------------------------------

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: invoke-rc.d	PID: 5229, Parent PID: 5228	—
General		—
Start time:	00:10:53	
Start date:	29/01/2022	
Path:	/usr/sbin/invoke-rc.d	
Arguments:	n/a	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: runlevel	PID: 5229, Parent PID: 5228	—
General		—
Start time:	00:10:53	
Start date:	29/01/2022	
Path:	/sbin/runlevel	
Arguments:	/sbin/runlevel	
File size:	996584 bytes	
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b	

File Activities	—
File Read	▼

Analysis Process: invoke-rc.d	PID: 5231, Parent PID: 5228	—
General		—
Start time:	00:10:53	
Start date:	29/01/2022	
Path:	/usr/sbin/invoke-rc.d	
Arguments:	n/a	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: systemctl	PID: 5231, Parent PID: 5228	—
General		—
Start time:	00:10:53	
Start date:	29/01/2022	
Path:	/usr/bin/systemctl	
Arguments:	systemctl --quiet is-enabled cups.service	
File size:	996584 bytes	
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b	

File Activities	—
File Read	▼

Analysis Process: invoke-rc.d	PID: 5232, Parent PID: 5228	—
General		—
Start time:	00:10:55	
Start date:	29/01/2022	
Path:	/usr/sbin/invoke-rc.d	
Arguments:	n/a	
File size:	129816 bytes	

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c
-----------	----------------------------------

Analysis Process: ls PID: 5232, Parent PID: 5228	
General	
Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/bin/ls
Arguments:	ls /etc/rc[S2345].d/S[0-9][0-9]cups
File size:	142144 bytes
MD5 hash:	e7793f15c2ff7e747b4bc7079f5cd4f7

File Activities	
File Read	

Analysis Process: invoke-rc.d PID: 5234, Parent PID: 5228	
General	
Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/sbin/invoke-rc.d
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5234, Parent PID: 5228	
General	
Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/bin/systemctl
Arguments:	systemctl --quiet is-active cups.service
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities	
File Read	

Analysis Process: logrotate PID: 5235, Parent PID: 5184	
General	
Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: 5235, Parent PID: 5184	
General	
Start time:	00:10:55
Start date:	29/01/2022
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	97496 bytes
MD5 hash:	beef4e1f54ec90564d2acd57c0b0c897

File Activities	
File Read	

File Written

Analysis Process: logrotate PID: 5236, Parent PID: 5184

General

Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: 5236, Parent PID: 5184

General

Start time:	00:10:55
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5237, Parent PID: 5236

General

Start time:	00:10:55
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: 5237, Parent PID: 5236

General

Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	/usr/lib/rsyslog/rsyslog-rotate
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: rsyslog-rotate PID: 5238, Parent PID: 5237

General

Start time:	00:10:55
Start date:	29/01/2022
Path:	/usr/lib/rsyslog/rsyslog-rotate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemctl PID: 5238, Parent PID: 5237

General		—
Start time:	00:10:55	
Start date:	29/01/2022	
Path:	/usr/bin/systemctl	
Arguments:	systemctl kill -s HUP rsyslog.service	
File size:	996584 bytes	
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b	

File Activities		—
File Read		▼

Analysis Process: systemd PID: 5185, Parent PID: 1		—
General		—
Start time:	00:10:52	
Start date:	29/01/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: install PID: 5185, Parent PID: 1		—
General		—
Start time:	00:10:52	
Start date:	29/01/2022	
Path:	/usr/bin/install	
Arguments:	/usr/bin/install -d -o man -g man -m 0755 /var/cache/man	
File size:	158112 bytes	
MD5 hash:	55e2520049dc6a62e8c94732e36cdd54	

File Activities		—
File Read		▼
Directory Created		▼

Analysis Process: systemd PID: 5197, Parent PID: 1		—
General		—
Start time:	00:10:52	
Start date:	29/01/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: find PID: 5197, Parent PID: 1		—
General		—
Start time:	00:10:52	
Start date:	29/01/2022	
Path:	/usr/bin/find	
Arguments:	/usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete	
File size:	320160 bytes	
MD5 hash:	b68ef002f84cc54dd472238ba7df80ab	

File Activities		—
File Read		▼
Directory Enumerated		▼

Analysis Process: systemd PID: 5230, Parent PID: 1		—
General		—
Start time:	00:10:53	
Start date:	29/01/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: mandb PID: 5230, Parent PID: 1		—
General		—
Start time:	00:10:53	
Start date:	29/01/2022	
Path:	/usr/bin/mandb	
Arguments:	/usr/bin/mandb --quiet	
File size:	142432 bytes	
MD5 hash:	1dda5ea0027ecf1c2db0f5a3de7e6941	

File Activities		—
File Deleted		▼
File Read		▼
File Written		▼
File Moved		▼
Directory Enumerated		▼
Owner / Group Modified		▼
Permission Modified		▼

Analysis Process: z0r0.arm7 PID: 5270, Parent PID: 5110		—
General		—
Start time:	00:11:09	
Start date:	29/01/2022	
Path:	/tmp/z0r0.arm7	
Arguments:	/tmp/z0r0.arm7	
File size:	4956856 bytes	
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1	

File Activities		—
File Read		▼