ID: 562525
Sample Name: z0r0.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:14:18
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

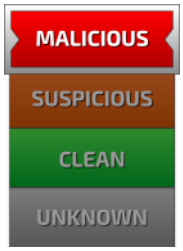
z0r0.arm

Overview

General Information

Sample Name:	z0r0.arm
Analysis ID:	562525
MD5:	de224424cf2826..
SHA1:	df9fdf491ea3735..
SHA256:	42b0ba0c3ccde8..
Tags:	Mirai
Infos:	

Detection

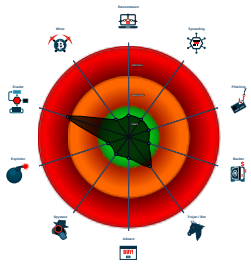


Score:	52
Range:	0 - 100
Whitelisted:	false

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:	562525
Start date:	29.01.2022
Start time:	00:14:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	z0r0.arm
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.linARM@0/53@0/0

Runtime Messages

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

Standard Output:	
Standard Error:	qemu: uncaught target signal 11 (Segmentation fault) - core dumped

Process Tree

- **system is lnxubuntu20**
- systemd New Fork (PID: 5194, Parent: 1)
- logrotate (PID: 5194, Parent: 1, MD5: ff9f6831debb63e53a31ff8057143af6) Arguments: /usr/sbin/logrotate /etc/logrotate.conf
  - logrotate New Fork (PID: 5258, Parent: 5194)
  - gzip (PID: 5258, Parent: 5194, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5259, Parent: 5194)
  - sh (PID: 5259, Parent: 5194, 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: 5260, Parent: 5259)
    - invoke-rc.d (PID: 5260, Parent: 5259, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: invoke-rc.d --quiet cups restart
      - invoke-rc.d New Fork (PID: 5261, Parent: 5260)
      - runlevel (PID: 5261, Parent: 5260, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /sbin/runlevel
      - invoke-rc.d New Fork (PID: 5262, Parent: 5260)
      - systemctl (PID: 5262, Parent: 5260, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-enabled cups.service
      - invoke-rc.d New Fork (PID: 5264, Parent: 5260)
      - ls (PID: 5264, Parent: 5260, MD5: e7793f15c2ff7e747b4bc7079f5cd4f7) Arguments: ls /etc/rc[S2345].d/S[0-9][0-9]cups
      - invoke-rc.d New Fork (PID: 5266, Parent: 5260)
      - systemctl (PID: 5266, Parent: 5260, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl --quiet is-active cups.service
  - logrotate New Fork (PID: 5267, Parent: 5194)
  - gzip (PID: 5267, Parent: 5194, MD5: beef4e1f54ec90564d2acd57c0b0c897) Arguments: /bin/gzip
  - logrotate New Fork (PID: 5268, Parent: 5194)
  - sh (PID: 5268, Parent: 5194, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
    - sh New Fork (PID: 5269, Parent: 5268)
    - rsyslog-rotate (PID: 5269, Parent: 5268, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/lib/rsyslog/rsyslog-rotate
      - rsyslog-rotate New Fork (PID: 5270, Parent: 5269)
      - systemctl (PID: 5270, Parent: 5269, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl kill -s HUP rsyslog.service
- systemd New Fork (PID: 5195, Parent: 1)
- install (PID: 5195, Parent: 1, MD5: 55e2520049dc6a62e8c94732e36cdd54) Arguments: /usr/bin/install -d -o man -g man -m 0755 /var/cache/man
- systemd New Fork (PID: 5257, Parent: 1)
- find (PID: 5257, Parent: 1, MD5: b68ef002f84cc54dd472238ba7df80ab) Arguments: /usr/bin/find /var/cache/man -type f -name *.gz -atime +6 -delete
- systemd New Fork (PID: 5263, Parent: 1)
- mandb (PID: 5263, Parent: 1, MD5: 1dda5ea0027ecf1c2db0f5a3de7e6941) Arguments: /usr/bin/mandb --quiet
- z0r0.arm (PID: 5278, Parent: 5119, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/z0r0.arm
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
z0r0.arm	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x741d:$s2: $Id: UPX • 0x73ce:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
5278.1.00000000d48383b3.00000000797c0c46.r-x.sdmp	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x741d:$s2: $Id: UPX • 0x73ce:$s3: $Info: This file is packed with the UPX executable packer

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Sample is packed with UPX

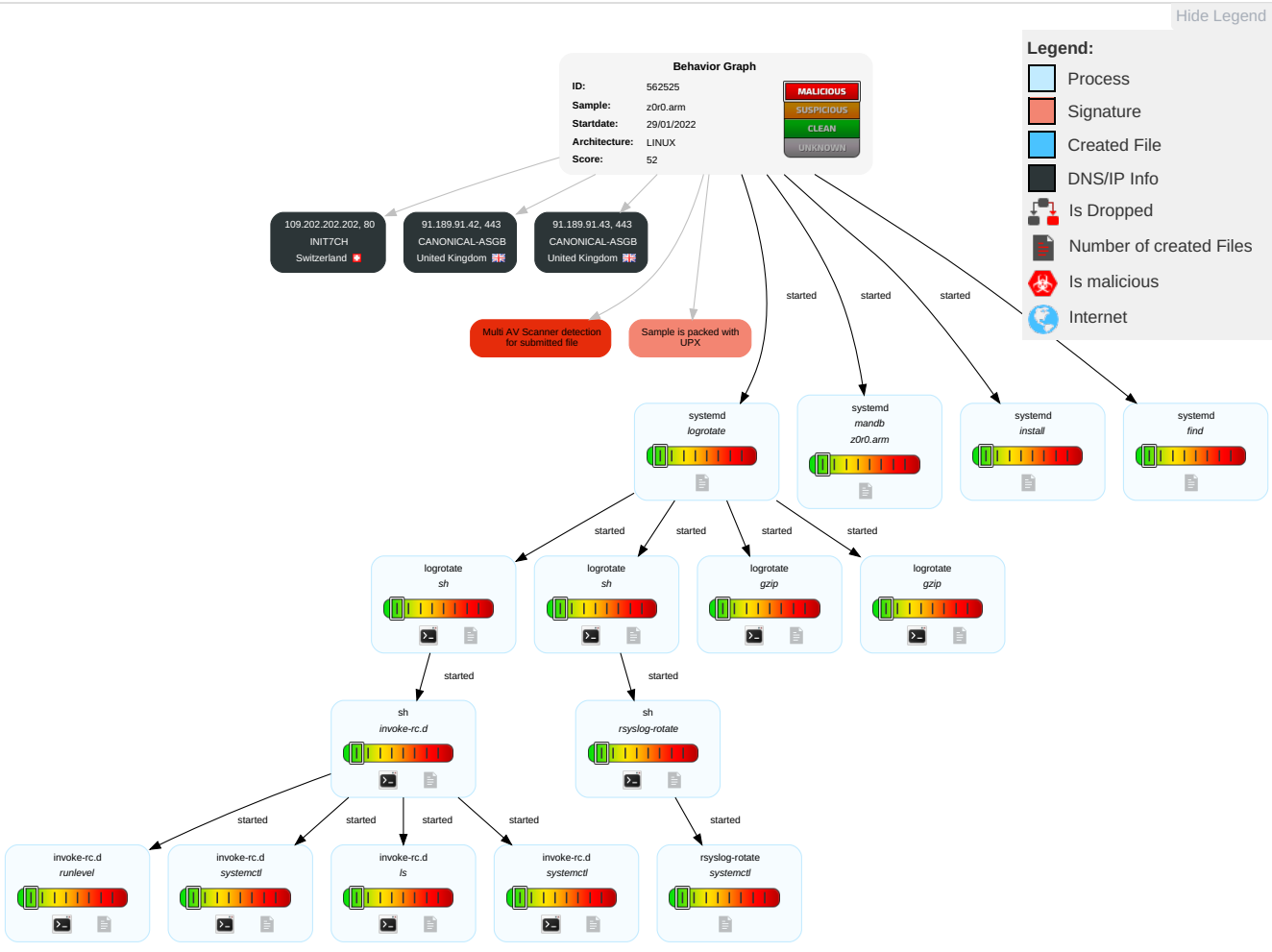
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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.arm	34%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

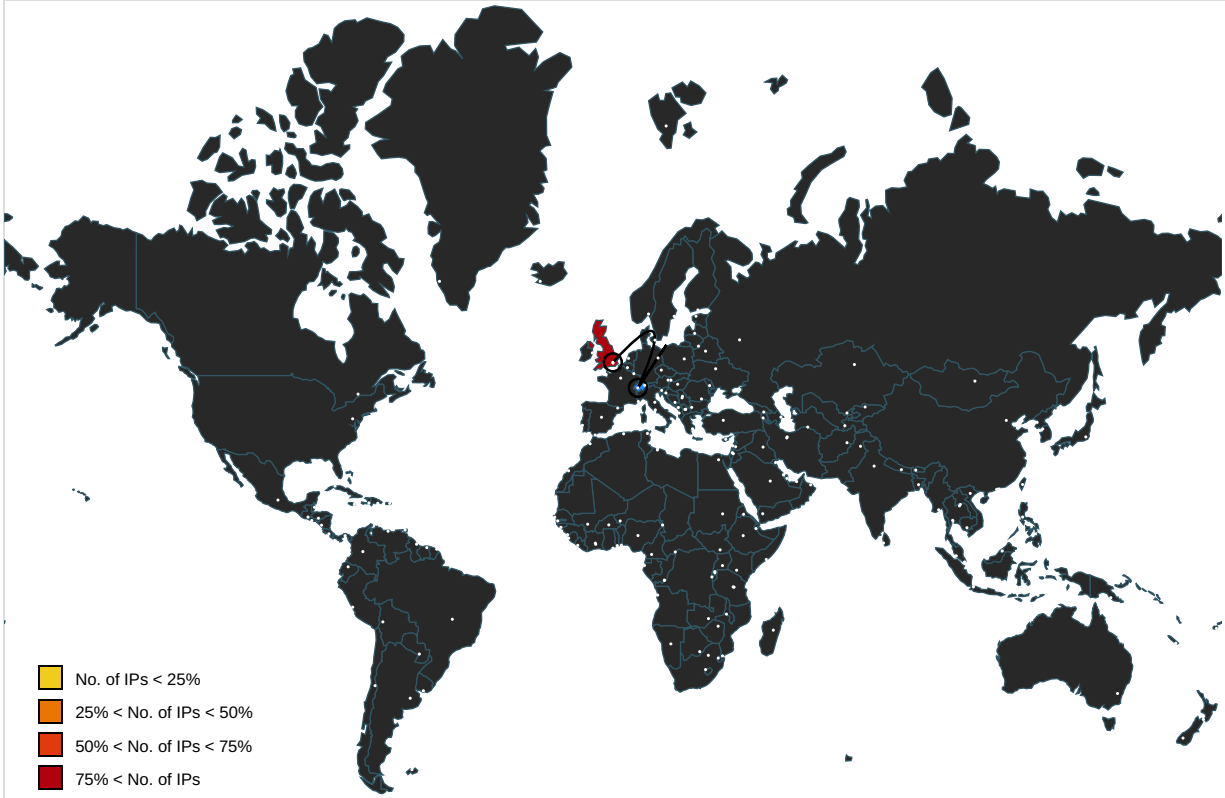
Domains and IPs

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/5263

/var/cache/man/cs/5263

/var/cache/man/cs/index.db.CA1Hw9

/var/cache/man/da/5263

/var/cache/man/da/index.db.zhekg9

/var/cache/man/de/5263

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

/var/cache/man/es/5263

/var/cache/man/es/index.db.a9fyec

/var/cache/man/fi/5263

/var/cache/man/fi/index.db.G8ou08

/var/cache/man/fr.ISO8859-1/5263

/var/cache/man/fr.ISO8859-1/index.db.6Hajwa

/var/cache/man/fr.UTF-8/5263

/var/cache/man/fr.UTF-8/index.db.6IONkc

/var/cache/man/fr/5263

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

/var/cache/man/hu/5263

/var/cache/man/hu/index.db.jLE9Wb

/var/cache/man/id/5263

/var/cache/man/id/index.db.ISobd9

/var/cache/man/index.db.rglO39

/var/cache/man/it/5263

/var/cache/man/it/index.db.e1tcA9

/var/cache/man/ja/5263

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

/var/cache/man/ko/5263

/var/cache/man/ko/index.db.03VMC8

/var/cache/man/nl/5263

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

/var/cache/man/pl/5263

/var/cache/man/pl/index.db.LJNDwc

/var/cache/man/pt/5263

/var/cache/man/pt/index.db.1paJGa

/var/cache/man/pt_BR/5263

/var/cache/man/pt_BR/index.db.MgN2kc

/var/cache/man/ru/5263

/var/cache/man/ru/index.db.cAekB8

/var/cache/man/sl/5263

/var/cache/man/sl/index.db.AOLa0b

/var/cache/man/sr/5263

/var/cache/man/sr/index.db.b8Rqjb

/var/cache/man/sv/5263

/var/cache/man/sv/index.db.xcGBu9

/var/cache/man/tr/5263

/var/cache/man/tr/index.db.Ri204b

/var/cache/man/zh_CN/5263

/var/cache/man/zh_CN/index.db.IBKjA8

/var/cache/man/zh_TW/5263

/var/cache/man/zh_TW/index.db.x40HWb

/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, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.951612466810868
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	z0r0.arm
File size:	31912
MD5:	de224424cf2826cd759b343b63e4564d
SHA1:	df9fdf491ea3735373be2cd3d2a4d4494858bda9
SHA256:	42b0ba0c3ccde84d49d1e3474ff9ef8fbd3210cc79bb7cef5e264596f2c7aca1
SHA512:	f5df1e06a3e6e303365fdc03d8d427b7d82d2b4074cf56bf30731e7b166600b62cda7b32c880d053ddc9309ac00a14060a4d4739e3bad71320dc5abe8603485a
SSDEEP:	768:PNpXVDa1o/nNAGAhhy4cN2ovA2mF2q3UV:PLX01qNAxhhyvvJm0
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....{...{.....&.....Q.td.....K..gUPX!.....#...#.....S.....?.E.h;.}...^.....e..{...(...,G....:.....fG0 E..B3.....O.@.

Static ELF Info

ELF header

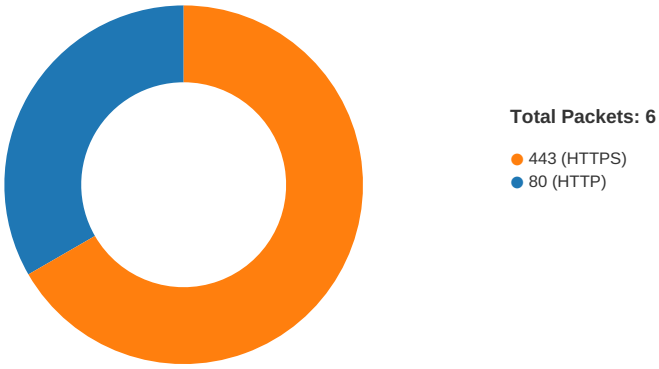
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0xe9e4
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	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	0x7bac	0x7bac	4.0395	0x5	R E	0x8000		
LOAD	0x0	0x10000	0x10000	0x0	0x12694	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: systemd PID: 5194, Parent PID: 1

General

Start time:	00:14:58
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: logrotate PID: 5194, Parent PID: 1

General

Start time:	00:14:58
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: 5258, Parent PID: 5194

General

Start time:	00:14:58
Start date:	29/01/2022

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

Analysis Process: gzip PID: **5258**, Parent PID: **5194**

General

Start time:	00:14:58
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: **5259**, Parent PID: **5194**

General

Start time:	00:14:58
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: **5259**, Parent PID: **5194**

General

Start time:	00:14:58
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: **5260**, Parent PID: **5259**

General

Start time:	00:14:58
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: invoke-rc.d PID: **5260**, Parent PID: **5259**

General

Start time:	00:14:58
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: **5261**, Parent PID: **5260**

General

Start time:	00:14:58
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: **5261**, Parent PID: **5260**

General

Start time:	00:14:58
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: **5262**, Parent PID: **5260**

General

Start time:	00:14:58
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: **5262**, Parent PID: **5260**

General

Start time:	00:14:58
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: **5264**, Parent PID: **5260**

General

Start time:	00:14:59
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: **5264**, Parent PID: **5260**

General

Start time:	00:14:59
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: **5266**, Parent PID: **5260**

General

Start time:	00:15:00
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: **5266**, Parent PID: **5260**

General

Start time:	00:15:00
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: **5267**, Parent PID: **5194**

General

Start time:	00:15:00
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: gzip PID: **5267**, Parent PID: **5194**

General

Start time:	00:15:00
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: **5268**, Parent PID: **5194**

General

Start time:	00:15:00
Start date:	29/01/2022
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	84056 bytes
MD5 hash:	ff9f6831debb63e53a31ff8057143af6

Analysis Process: sh PID: **5268**, Parent PID: **5194**

General

Start time:	00:15:00
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: **5269**, Parent PID: **5268**

General

Start time:	00:15:00
Start date:	29/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rsyslog-rotate PID: **5269**, Parent PID: **5268**

General

Start time:	00:15:00
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: **5270**, Parent PID: **5269**

General

Start time:	00:15:00
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: **5270**, Parent PID: **5269**

General

Start time:	00:15:00
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: **5195**, Parent PID: **1**

General

Start time:	00:14:58
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: install PID: **5195**, Parent PID: **1**

General

Start time:	00:14:58
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: **5257**, Parent PID: **1**

General

Start time:	00:14:58
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: find PID: **5257**, Parent PID: **1**

General

Start time:	00:14:58
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: **5263**, Parent PID: **1**

General

Start time:	00:14:58
Start date:	29/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: mandb PID: **5263**, Parent PID: **1**

General

Start time:	00:14:58
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.arm PID: **5278**, Parent PID: **5119**

General

Start time:	00:15:03
Start date:	29/01/2022
Path:	/tmp/z0r0.arm
Arguments:	/tmp/z0r0.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

- **File Read**