ID: 321474
Sample Name: i
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 15:40:47
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report i

Overview

General Information

Sample Name:	i
Analysis ID:	321474
MD5:	a73ddd6ec22462..
SHA1:	ac6962542a4b23..
SHA256:	b5cf68c7cb5bb2d..

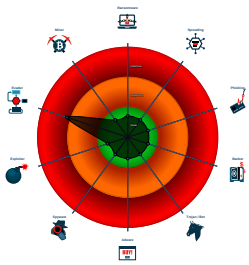
Detection

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Creates hidden files and/or directories
- Executes the "grep" command used…
- Executes the "mkdir" command use…
- Executes the "mktemp" command u…
- Executes the "rm" command used to…
- Executes the "sleep" command use…
- Sample contains only a LOAD segm…
- Uses the "uname" system call to qu…
- Yara signature match

Classification



Startup

- **system is lnxubuntu1**
- dash New Fork (PID: 3193, Parent: 3192)
  - sed (PID: 3193, Parent: 3192, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3194, Parent: 3192)
  - sort (PID: 3194, Parent: 3192, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3195, Parent: 2520)
  - sleep (PID: 3195, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3223, Parent: 3222)
  - sed (PID: 3223, Parent: 3222, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3224, Parent: 3222)
  - sort (PID: 3224, Parent: 3222, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3230, Parent: 2520)
  - sleep (PID: 3230, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3251, Parent: 3250)
  - sed (PID: 3251, Parent: 3250, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3252, Parent: 3250)
  - sort (PID: 3252, Parent: 3250, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3263, Parent: 2520)
  - sleep (PID: 3263, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3279, Parent: 3278)
  - sed (PID: 3279, Parent: 3278, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3280, Parent: 3278)
  - sort (PID: 3280, Parent: 3278, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3281, Parent: 2520)
  - sleep (PID: 3281, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3307, Parent: 3306)
  - sed (PID: 3307, Parent: 3306, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3308, Parent: 3306)
  - sort (PID: 3308, Parent: 3306, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3315, Parent: 2520)
  - sleep (PID: 3315, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3335, Parent: 3334)
  - sed (PID: 3335, Parent: 3334, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3336, Parent: 3334)
  - sort (PID: 3336, Parent: 3334, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3342, Parent: 2520)
  - sleep (PID: 3342, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3363, Parent: 3362)
  - sed (PID: 3363, Parent: 3362, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3364, Parent: 3362)
  - sort (PID: 3364, Parent: 3362, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3374, Parent: 2520)
  - sleep (PID: 3374, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3391, Parent: 3390)
  - sed (PID: 3391, Parent: 3390, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3392, Parent: 3390)
  - sort (PID: 3392, Parent: 3390, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3407, Parent: 2520)
  - sleep (PID: 3407, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1

- dash New Fork (PID: 3419, Parent: 3418)
  - sed (PID: 3419, Parent: 3418, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3420, Parent: 3418)
  - sort (PID: 3420, Parent: 3418, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3432, Parent: 2520)
  - sleep (PID: 3432, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3447, Parent: 3446)
  - sed (PID: 3447, Parent: 3446, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3448, Parent: 3446)
  - sort (PID: 3448, Parent: 3446, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3457, Parent: 2520)
  - sleep (PID: 3457, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
  - i (PID: 3482, Parent: 3133, MD5: a73ddd6ec22462db955439f665cad4e6) Arguments: /usr/bin/qemu-mips /tmp/i
- upstart New Fork (PID: 3495, Parent: 2015)
  - sh (PID: 3495, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3496, Parent: 3495)
    - date (PID: 3496, Parent: 3495, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3497, Parent: 3495)
    - apport-checkreports (PID: 3497, Parent: 3495, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 3522, Parent: 2015)
  - sh (PID: 3522, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3524, Parent: 3522)
    - date (PID: 3524, Parent: 3522, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3532, Parent: 3522)
    - apport-gtk (PID: 3532, Parent: 3522, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- dash New Fork (PID: 3550, Parent: 3549)
  - sed (PID: 3550, Parent: 3549, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3551, Parent: 3549)
  - sort (PID: 3551, Parent: 3549, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3552, Parent: 2520)
  - sleep (PID: 3552, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- upstart New Fork (PID: 3577, Parent: 2015)
  - sh (PID: 3577, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3578, Parent: 3577)
    - date (PID: 3578, Parent: 3577, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3579, Parent: 3577)
    - apport-gtk (PID: 3579, Parent: 3577, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- dash New Fork (PID: 3605, Parent: 3604)
  - sed (PID: 3605, Parent: 3604, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3606, Parent: 3604)
  - sort (PID: 3606, Parent: 3604, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3622, Parent: 2520)
  - sleep (PID: 3622, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3633, Parent: 3632)
  - sed (PID: 3633, Parent: 3632, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3634, Parent: 3632)
  - sort (PID: 3634, Parent: 3632, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3648, Parent: 2520)
  - sleep (PID: 3648, Parent: 2520, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3660, Parent: 2520)
  - sed (PID: 3660, Parent: 2520, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DOMAINS=/ { s/^.*=/search /; p}" /run/systemd/netif/state
- dash New Fork (PID: 3661, Parent: 2520)
  - resolvconf (PID: 3661, Parent: 2520, MD5: unknown) Arguments: /bin/sh /sbin/resolvconf -a networkd
    - resolvconf New Fork (PID: 3674, Parent: 3661)
    - mkdir (PID: 3674, Parent: 3661, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /run/resolvconf/interface
    - resolvconf New Fork (PID: 3677, Parent: 3661)
      - resolvconf New Fork (PID: 3678, Parent: 3677)
      - sed (PID: 3678, Parent: 3677, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/#.*$// -e s/[[:blank:]]\\+$// -e s/^[[:blank:]]\\+// -e "s/[[:blank:]]\\+/ /g" -e "/^nameserver/!b ENDOFCYCLE" -e "s/$/ /" -e "s/\\([:.]\\)0\\+/\\10/g" -e "s/\\([:.]\\)0\\([123456789abcdefABCDEF][[:xdigit:]]*\\)/\\1\\2/g" -e "/::/b ENDOFCYCLE; s/ \\(0[:]\\)\\+/ ::/" -e "/::/b ENDOFCYCLE; s/:\\(0[:]\\)\\+/::/" -e ": ENDOFCYCLE" -
      - resolvconf New Fork (PID: 3679, Parent: 3677)
      - sed (PID: 3679, Parent: 3677, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/[[:blank:]]\\+$// -e /^$/d
- dash New Fork (PID: 3711, Parent: 2079)
  - mkdir (PID: 3711, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/logrotate
- dash New Fork (PID: 3712, Parent: 2079)
  - mkdir (PID: 3712, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/upstart
- dash New Fork (PID: 3713, Parent: 2079)
  - egrep (PID: 3713, Parent: 2079, MD5: ef55d1537377114cc24cdc398fbdd930) Arguments: /bin/sh /bin/egrep [^[:print:]] /home/user/.cache/logrotate/status
  - grep (PID: 3713, Parent: 2079, MD5: fc9b0a0ff848b35b3716768695bf2427) Arguments: grep -E [^[:print:]] /home/user/.cache/logrotate/status
- dash New Fork (PID: 3715, Parent: 2079)
  - mktemp (PID: 3715, Parent: 2079, MD5: 91cf2e2a84f3b49fdecdd8b631902009) Arguments: mktemp
- dash New Fork (PID: 3783, Parent: 2079)
  - cat (PID: 3783, Parent: 2079, MD5: efa10d52f37361f2e3a5d22742f0fcc4) Arguments: cat
- dash New Fork (PID: 3784, Parent: 2079)
  - logrotate (PID: 3784, Parent: 2079, MD5: d0eaf9942936032d217478b93e9cd4b1) Arguments: logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.d54CkEbiVw
    - logrotate New Fork (PID: 3786, Parent: 3784)
    - gzip (PID: 3786, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3802, Parent: 3784)
    - gzip (PID: 3802, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3803, Parent: 3784)
    - gzip (PID: 3803, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3807, Parent: 3784)
    - gzip (PID: 3807, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3837, Parent: 3784)
    - gzip (PID: 3837, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3838, Parent: 3784)
    - gzip (PID: 3838, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3839, Parent: 3784)
    - gzip (PID: 3839, Parent: 3784, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
- dash New Fork (PID: 3840, Parent: 2079)

- dash New Fork (PID: 3840, Parent: 2079)
  - rm (PID: 3840, Parent: 2079, MD5: b79876063d894c449856cca508ecca7f) Arguments: rm -f /tmp/tmp.d54CkEbiVw
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
i	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x206f8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20767:$s2: $Id: UPX • 0x20718:$s3: $Info: This file is packed with the UPX executable packer

Signature Overview

- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

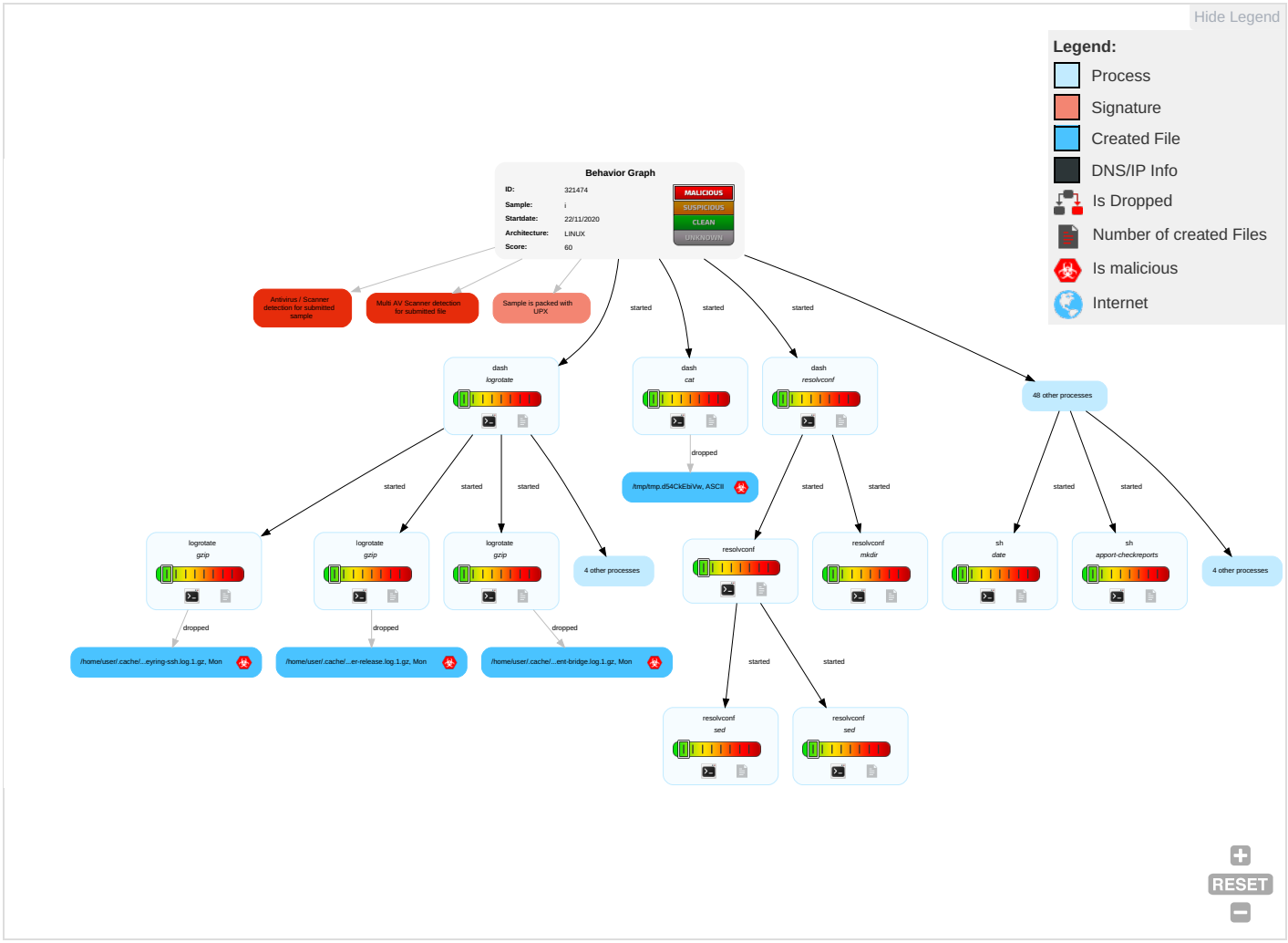
Data Obfuscation:

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Hidden Files and Directories 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syste Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 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)	File Deletion 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

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
i	62%	Virustotal		Browse
i	18%	Metadefender		Browse
i	59%	ReversingLabs	Linux.Trojan.Mirai	
i	100%	Avira	LINUX/Mirai.ccjqy	

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321474
Start date:	22.11.2020
Start time:	15:40:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	i
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Detection:	MAL
Classification:	mal60.evad.lin@0/11@0/0

Runtime Messages

Command:	/tmp/i
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 5 (Trace/breakpoint trap) - core dumped

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/home/user/.cache/logrotate/status.tmp	
Process:	/usr/sbin/logrotate
File Type:	ASCII text
Category:	dropped
Size (bytes):	1458
Entropy (8bit):	4.866479323539009
Encrypted:	false
SSDEEP:	24:fOeWfnS8MHLIJWfnrIILWfnw7WfnDvRT/MHXIbTMHtW8MF8iQl/wWfnRvTMHz:2elNHLcsgnnHXdHtWbFLLswHz
MD5:	E834FBD4E7133101B91BBDB86D92EE4B
SHA1:	D6CEF16CF3986DB469A43503794A814B88F0C229
SHA-256:	4D667654CF6955FAB1290616C5C3F34F78656C1499F0509CC4B5882CC724E69A
SHA-512:	E71388A03A6C243C03160ABCEEDD74487FC2AB58CA75FA9C92145045BD6D10BA6FEA9FE50D22B3C80B271C905156D5C4814050E05A133C98B7E9944A98F3034
Malicious:	false
Reputation:	low
Preview:	logrotate state -- version 2."/home/user/.cache/upstart/indicator-application.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/indicator-sound.log" 2018-5-7-10:33:19."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr_share_apport_apport-gtk.1000.crash.log" 2020-11-22-16:0:0."/home/user/.cache/upstart/indicator-session.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/dbus.log" 2020-11-22-16:41:34."/home/user/.cache/upstart/gnome-keyring-ssh.log" 2020-11-22-16:41:34."/home/user/.cache/upstart/indicator-bluetooth.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/indicator-datetime.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/startxfce4.log" 2020-11-22-16:41:34."/home/user/.cache/upstart/update-notifier-release.log" 2020-11-22-16:41:34."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr_share_apport_apport.0.crash.log" 2020-11-22-16:0:0."/home/user/.cache/upstart/ssh-agent.log" 2020-11-22-16:41:34."/home/user/.cache/upstart/update-notifier-crash-_var_crash

/home/user/.cache/upstart/dbus.log.1.gz	
Process:	/bin/gzip
File Type:	Sun Nov 22 14:40:52 2020, from Unix
Category:	dropped
Size (bytes):	267
Entropy (8bit):	7.176604663951017
Encrypted:	false
SSDEEP:	6:XpsYlQuom0gW0F46ASWpC8t0BEP80ryEbjL+swraiuWRGI:X+/nLT0F48WUTBEEAJPyROi0l
MD5:	F7D434449209A580CCAB65800AF42CDE
SHA1:	A2C05B5D8859F4CD2FC942FC83A4151356243483
SHA-256:	B00A4566CCFEFE6A062B9B3D7CE3A734F5F16B60E2F7630501DD7722FA7B728C
SHA-512:	B2BCD5596D8A1EBF70D1AF064156590709E4E6F363E21E72DE9C5104E1A1A7EF72F0C78044A19F02BC45E5201675449E7A95CF4ADB7BB0B183A7AFA74974B48
Malicious:	false
Reputation:	low
Preview:	....tx._.....N.0...H.Co.E*w.E.8.MbL....EMc.;...3....._~..?....i....=./(...,.....9[....p,.....!..p..ANb.e..0....(.y...K...N..<.x..i."+.j=.tfpl..=Ee...."....|`..zb*..KKQ.|Yz..nK!....."'T..f=G=.....s.#.N...eOD....s...u....h@..+...j...P.....A.S.....

/home/user/.cache/upstart/gnome-keyring-ssh.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	99
Entropy (8bit):	6.129257882662173
Encrypted:	false
SSDEEP:	3:FtPaGuofByOJ9+JbgcpuvfIMGddoffEwZW/l:XPa25NrQbgYuoMBfMsGl
MD5:	2B8D9549C00943FB9FFC73FD80E6AC1A
SHA1:	E6348E8BB25396F0542E7E74AE30AF03F48E237E
SHA-256:	606AE477FACBE88A7BF8C1718AE0259E50487BB5F98B80F0E2895DD799BBE858
SHA-512:	C2CA8D2DFC0B0E28FDB3E94EF2BE74D7D663E9943EE55D03F9F8C8E1425AC4C0C07391020DEE0931EC9967185BDD75BDA438BC413DDBC6AB18D2EF28388C D59
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	....._..... ....;t...!.@....-.....+B..X.%.J.>..`..jA....:-i.8...i7..f..+....@jB.X.y.OK..Y...

/home/user/.cache/upstart/gpg-agent.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:26 2020, from Unix
Category:	dropped
Size (bytes):	109
Entropy (8bit):	6.285347714840308
Encrypted:	false
SSDEEP:	3:Ft+KspyDBmKyr7JtqZioTFBkdMl/:X+KspyDB94JtYPk+
MD5:	13A3054AF030A536BDA784F022481B4C
SHA1:	062CEC7C61E642887CE10970A7353066C4283DFD
SHA-256:	0D9475D2511F0A2C555242326C2D4EB69E4456726BDDB84913B95EC59F8FDCF6
SHA-512:	EB0A9DDC9D084934F42DF3AC9FE92CE534A841B38F6008774F29788EEFEC4FD22BFE12570B30558A351755347E92742C867B3B65E0616294146C390FB60A3388
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....._....0....=l...E.C....p&.....fX.L..Wt...)*.*...e.X.....).Fj+.,."E..5f.....X.K..w.....

/home/user/.cache/upstart/ssh-agent.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	60
Entropy (8bit):	5.121567004295788
Encrypted:	false
SSDEEP:	3:FtPa5qBO0YYLB0trl1mlwdn:XPa5W2Yt02g6n
MD5:	32CF70DC61DECD8DFBC64EB2F2529FAC
SHA1:	DAC70D15E4E11407299DC63AAA6774A2393C2316
SHA-256:	5F46EF0AAB4AD28F5384537011EDB096F22592BE4EA83194C1A52A11ECAD51D5
SHA-512:	D89B691D4403CB3B836F4B50795046DE26AC588D2C03020EC9B944B97259DD7ED759509229E92B601C5050F2A43DCAFA0D098E2EE5E324A56F69E1EE4BB35E8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....._..+...MLO.+Q(../../(J.-I,*.Q((.ON-.V024.....["(...

/home/user/.cache/upstart/startxfce4.log.1.gz	
Process:	/bin/gzip
File Type:	Sun Nov 22 15:41:17 2020, from Unix
Category:	dropped
Size (bytes):	1151
Entropy (8bit):	7.839699344526511
Encrypted:	false
SSDEEP:	24:XB+BojMnJnBU5Lk9eIEtZHE9LYIOzgczACtLQ1vzKpDk/aR:XB+iI9u5LCEtFE9LBOzjACEKQA
MD5:	CCA8A4216E7E2572ED6C667BD34F12ED
SHA1:	6E44ADAFF251BBE1463C04C502F8471844F68BBB
SHA-256:	D05AAAC162B5D605FB2EFDD3B30C01B461D68D0C4AD1BBDF3AB8042286C7A7E8
SHA-512:	40259068A9CC7CA9CFFD2DEBFFB3E57FD77FE82F29DD45980A5ADEAF611F7B96A0543FE2D5F75BD1F8DCD3D1ED1057A3AF64FE2E5AFB42FA86238B3D490D9979
Malicious:	false
Reputation:	low
Preview:	....._...V.n.8....?....d;.M.t#....i'...@Ke..D...V.~....9...s. ..W.{E...7.u}..?.~:J...<.3...w..t...)L..`.....R..z.T.fi...g....%7...s.....1\...`%.....T._.e.Ln.}.0.....y.@K...$us...;A..jH..`.gt2."1.i..I_.X....h'....(.Q.k.....oW..Z1.g...n...U.....B..-.....k.$..t.K.v.`.c...~..nKU&.,"J]X..:.-.n.#j..uoq.....Y%Y.=G.O..w...?.]@..U...$.Y....7..7s.....u:8.K.....pc..-.g)c..KH@.j.m...9._X.S..4...).O.-.k>...&.....N....L.L.:3.W5.f(^...v.~.....}.3bE.O.....5.....<.4y..4.{..3q.R*u..5b'..e+.'.....R.5... X.[..%...}k..kf@H.J../...!r5...*P..$...p..R..a<HG..w..n.$..r.....f,_V.\.x:g.N$f.4.?p3"y.y.).....m....]...x.i..1....3...^.Z....6}.....\...A(y..#.g..a...@.....Rc.....8Z..f..tHf.^"%.....(i...[..Q....6.t4.....+"..l.E!..9..$..V.S..h.H..F....BF..Q..d.y.<a..H.../..U.I.]0.9.h...c.J.;....p;.<.I6k....Y.:...9..>.....^...w.4..e..K..u...i.DPIg.....rP.....;....>..).(.+*.....E.p..W$....<;..vE\P..*.l.^S....e.>.1|.v.K...EK.B....;...uZPG.8.:J.&.....@

/home/user/.cache/upstart/update-notifier-release.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	73
Entropy (8bit):	5.311208593298957
Encrypted:	false
SSDEEP:	3:FtPacK82rsFX+TP4P2gt:XPacf2rNWt
MD5:	6B9C8B79E6508C02BCACF1C11363D3BC
SHA1:	F450E69D5A258FCF4D89E7CDB1FBD7EEC5E19A77
SHA-256:	735DFDFE533A05589BFDC9044627395F29312064CFBA09CCB60E010AEC692411

/home/user/.cache/upstart/update-notifier-release.log.1.gz	
SHA-512:	AAE4EF554245D1419335B80EA6ED0E357FCC7032BF991D4808B8A2E09F671BA318B7EF0A8824FA334D6B51EF7104351461814D1EE096D357305914A83380CC35
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	......_.....S.*.Q02W04.20.22Rpv..Q0202P.K-W(J.IM,NUH,K..IL.I.....5...

/home/user/.cache/upstart/upstart-event-bridge.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	68
Entropy (8bit):	5.395998870534845
Encrypted:	false
SSDEEP:	3:FtPa5wG0BMPWNLPgXseOBMky:XPa5wG+OQP4OBMV
MD5:	1395D405968C76307CBA75C5DDC9CA19
SHA1:	C36CEE03E5DF12FBFB57A5EBCEAE329B41AFA1F7
SHA-256:	33785027CEE82E878434593B532FE1DF25D46676379757272C1E15C9AADD3B1F
SHA-512:	09CAB8DFF495DA9ED715C94E9F24B0C5C40CF0BC8C1B0DEEFB90C54081020AD80AF51636ADCBA368980E2C69119697A65E2E4AC5B834E0F08F88AEA52EFDA57
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	......_..+-(.I,*.M-K.+.M*.LIOU(.././(J....(...'...+..X..r.....3...

/tmp/tmp.d54CkEbiVw	
Process:	/bin/cat
File Type:	ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	3.7760909131289533
Encrypted:	false
SSDEEP:	3:PgWA0uU95y/1aF/g2FFXwyyVDoGeRqcOAvC:PgWl195y9aF/g2FFgfNepvK
MD5:	46261223A62EF65D03C70F15EE935267
SHA1:	E9102D8808BA6E171405F1830BD7C6B8179C9BF2
SHA-256:	DFECC8990014230F50FBAD269AD523A74D16CFB455065EC8D9041764D684C239
SHA-512:	380CFA479D6DB2361DCE6A52A516ECBA4D5CCE647299A87C3C3ED5887DB929C81A0F970097E6CF02C11440BCE87299D611B01CE56CF9AF09DCFBBA14249E9F9
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	"/home/user/.cache/upstart/*.log" {. hourly. missingok. rotate 7. compress. notifempty. nocreate.}.

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
Process:	/usr/share/apport/apport-checkreports
File Type:	ASCII text
Category:	dropped
Size (bytes):	14915
Entropy (8bit):	4.697516332022307
Encrypted:	false
SSDEEP:	192:uYq5ps3IZjjs9BjfL2532sFjE/WVPI3hbm:en2AE2L
MD5:	37721ED2DA65464679FBFC9487F46687
SHA1:	74CBBCFB307759084261FA482B08562EBD30B936
SHA-256:	84105540AAB974F2F675EAD2DD087F60FF197B5ED8CF1515541FF0C6BAD85F86
SHA-512:	A7EB7725A0AA130187E8D486C8142053C45AC4627B4A35255760709DAE47CBDF03FC304644F123DC6A311D6E4E19FFA9191EBAF150BBFA8EC2091EDE7C0EF785
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sun Nov 22 16:41:18 2020.ExecutablePath: /usr/share/apport/apport-checkreports.ExecutableTimestamp: 1514927430.InterpreterPath: /usr/bin/python3.5.ProcCmdline: /usr/bin/python3 /usr/share/apport/apport-checkreports --system.ProcCwd: /home/user.ProcEnviron:. LANGUAGE=en_US. PATH=(custom, user). XDG_RUNTIME_DIR=<set>. LANG=en_US.UTF-8. SHELL=/bin/bash.ProcMaps:. 00400000-007a9000 r-xp 00000000 fc:00 217 /usr/bin/python3.5. 009a9000-009ab000 r--p 003a9000 fc:00 217 /usr/bin/python3.5. 009ab000-00a42000 rw-p 003ab000 fc:00 217 /usr/bin/python3.5. 00a42000-00a73000 rw-p 00000000 00:00 0 . 028ab000-02c04000 rw-p 00000000 00:00 0 [heap]. 7f2992003000-7f2992184000 rw-p 00000000 00:00 0 . 7f2992184000-7f299219b000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f299219b000-7f299239a000 ---p 00017000 fc:0

/var/crash/_usr_share_apport_apport-gtk.1000.crash	
Process:	/usr/share/apport/apport-gtk

/var/crash/_usr_share_apport_apport-gtk.1000.crash	
File Type:	ASCII text
Category:	dropped
Size (bytes):	47094
Entropy (8bit):	4.5211252081106625
Encrypted:	false
SSDEEP:	768:vd0/R/P/H/jfq56kYwaLDpAe65wjC8EYb:6/R/P/H/5kYwame65wjC8EYb
MD5:	CD44385052AE289B22E22628D5084BF8
SHA1:	2F3A910CFF703B6F1F766BE925DE8303C92B1E45
SHA-256:	C1665DE53FB2AB58ABA4F060AF6D714401419ECC894620272CD0D80D2199532D
SHA-512:	408CE4957D65FC6B7A61742D4CCBB34FEFF8D898B73E999B298FCDBA79E53636C58F24503F20623D525B382353F8502045DCC723E1D0DF4F577DC7A37A25643
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sun Nov 22 16:41:19 2020.ExecutablePath: /usr/share/apport/apport-gtk.ExecutableTimestamp: 1514927430.InterpreterPath: /usr/bin/python3.5.ProcCmdline: /usr/bin/python3 /usr/share/apport/apport-gtk.ProcCwd: /home/user.ProcEnviron:. LANGUAGE=en_US. PATH=(custom, user). XDG_RUNTIME_DIR=<set>. LANG=en_US.UTF-8. SHELL=/bin/bash.ProcMaps:. 00400000-007a9000 r-xp 00000000 fc:00 217 /usr/bin/python3.5. 009a9000-009ab000 r--p 003a9000 fc:00 217 /usr/bin/python3.5. 009ab000-00a42000 rw-p 003ab000 fc:00 217 /usr/bin/python3.5. 00a42000-00a73000 rw-p 00000000 00:00 0 . 028a0000-02dc2000 rw-p 00000000 00:00 0 [heap]. 7f1ed512e000-7f1ed522e000 rw-p 00000000 00:00 0 . 7f1ed522e000-7f1ed5245000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f1ed5245000-7f1ed5444000 ---p 00017000 fc:00 2382

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.813637944981102
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	i
File size:	135472
MD5:	a73ddd6ec22462db955439f665cad4e6
SHA1:	ac6962542a4b23ac13bddff22f8df9aeb702ef12
SHA256:	b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605
SHA512:	92a52f68a7324c4d5876e1f7e2cb87d14b8604b057ceee2e537815568faa96abf576a22111c5c976eff72ab9015f1261b2331d4b4d711f4e62c8eb403c2377aa
SSDEEP:	3072:2glZ3FtCKXhkmHtZ9TEKzjfj/WMngyIfsJ0F7xPtoM:2IIKXhZtL7jOTyIG87Xl
File Content Preview:	.ELF.....B.x...4.....4. ...(.....@...@.....C...C.....*.*UPX!.X.....]....|.$..ELF.....@.`....4...p... ...(.....<...@.....[v.....H...`.t/._...dt.Q.....].M.....P.....

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:	0x420578
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

ELF header

Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x20fc2	0x20fc2	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x91f18	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: dash PID: 3193 Parent PID: 3192

General

Start time:	15:41:09
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3193 Parent PID: 3192

General

Start time:	15:41:09
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3194 Parent PID: 3192

General

Start time:	15:41:09
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3194 Parent PID: 3192

General

Start time:	15:41:09
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3195 Parent PID: 2520

General

Start time:	15:41:09
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3195 Parent PID: 2520

General

Start time:	15:41:09
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3223 Parent PID: 3222

General

Start time:	15:41:10
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3223 Parent PID: 3222

General

Start time:	15:41:10
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3224 Parent PID: 3222

General

Start time:	15:41:10
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3224 Parent PID: 3222

General

Start time:	15:41:10
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3230 Parent PID: 2520

General

Start time:	15:41:10
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3230 Parent PID: 2520

General

Start time:	15:41:10
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3251 Parent PID: 3250

General

Start time:	15:41:11
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3251 Parent PID: 3250

General

Start time:	15:41:11
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3252 Parent PID: 3250

General

Start time:	15:41:11
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3252 Parent PID: 3250

General

Start time:	15:41:11
Start date:	22/11/2020
Path:	/usr/bin/sort

Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3263 Parent PID: 2520

General

Start time:	15:41:11
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3263 Parent PID: 2520

General

Start time:	15:41:11
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3279 Parent PID: 3278

General

Start time:	15:41:12
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3279 Parent PID: 3278

General

Start time:	15:41:12
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3280 Parent PID: 3278

General

Start time:	15:41:12
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3280 Parent PID: 3278

General

Start time:	15:41:12
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3281 Parent PID: 2520

General

Start time:	15:41:12
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3281 Parent PID: 2520

General

Start time:	15:41:12
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3307 Parent PID: 3306

General

Start time:	15:41:13
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3307 Parent PID: 3306

General

Start time:	15:41:13
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3308 Parent PID: 3306

General

Start time:	15:41:13
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3308 Parent PID: 3306

General

Start time:	15:41:13
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3315 Parent PID: 2520

General

Start time:	15:41:13
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3315 Parent PID: 2520

General

Start time:	15:41:13
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3335 Parent PID: 3334

General

Start time:	15:41:14
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3335 Parent PID: 3334

General

Start time:	15:41:14
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3336 Parent PID: 3334

General

Start time:	15:41:14
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3336 Parent PID: 3334

General

Start time:	15:41:14
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3342 Parent PID: 2520

General

Start time:	15:41:14
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3342 Parent PID: 2520

General

Start time:	15:41:14
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3363 Parent PID: 3362

General

Start time:	15:41:15

Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3363 Parent PID: 3362

General

Start time:	15:41:15
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3364 Parent PID: 3362

General

Start time:	15:41:15
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3364 Parent PID: 3362

General

Start time:	15:41:15
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3374 Parent PID: 2520

General

Start time:	15:41:15
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3374 Parent PID: 2520

General

Start time:	15:41:15
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3391 Parent PID: 3390

General

Start time:	15:41:16
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3391 Parent PID: 3390

General

Start time:	15:41:16
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3392 Parent PID: 3390

General

Start time:	15:41:16
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3392 Parent PID: 3390

General

Start time:	15:41:16
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3407 Parent PID: 2520

General

Start time:	15:41:16
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3407 Parent PID: 2520

General

Start time:	15:41:16
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3419 Parent PID: 3418

General

Start time:	15:41:17
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3419 Parent PID: 3418

General

Start time:	15:41:17
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3420 Parent PID: 3418

General

Start time:	15:41:17
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3420 Parent PID: 3418

General

Start time:	15:41:17
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3432 Parent PID: 2520

General

Start time:	15:41:17
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3432 Parent PID: 2520

General

Start time:	15:41:17
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3447 Parent PID: 3446

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3447 Parent PID: 3446

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3448 Parent PID: 3446

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3448 Parent PID: 3446

General

Start time:	15:41:18

Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3457 Parent PID: 2520

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3457 Parent PID: 2520

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: i PID: 3482 Parent PID: 3133

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/tmp/i
Arguments:	/usr/bin/qemu-mips /tmp/i
File size:	135472 bytes
MD5 hash:	a73ddd6ec22462db955439f665cad4e6

File Activities

File Read

Analysis Process: upstart PID: 3495 Parent PID: 2015

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3495 Parent PID: 2015

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 3496 Parent PID: 3495

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3496 Parent PID: 3495

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3497 Parent PID: 3495

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sh

Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 3497 Parent PID: 3495

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/usr/share/apport/apport-checkreports
Arguments:	/usr/bin/python3 /usr/share/apport/apport-checkreports --system
File size:	1269 bytes
MD5 hash:	1a7d84ebc34df04e55ca3723541f48c9

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: 3522 Parent PID: 2015

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3522 Parent PID: 2015

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 3524 Parent PID: 3522

General

Start time:	15:41:18

Start date:	22/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3524 Parent PID: 3522

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3532 Parent PID: 3522

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 3532 Parent PID: 3522

General

Start time:	15:41:18
Start date:	22/11/2020
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: dash PID: 3550 Parent PID: 3549

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3550 Parent PID: 3549

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3551 Parent PID: 3549

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3551 Parent PID: 3549

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3552 Parent PID: 2520

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/dash

Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3552 Parent PID: 2520

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: upstart PID: 3577 Parent PID: 2015

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3577 Parent PID: 2015

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 3578 Parent PID: 3577

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3578 Parent PID: 3577

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3579 Parent PID: 3577

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 3579 Parent PID: 3577

General

Start time:	15:41:19
Start date:	22/11/2020
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

Directory Enumerated

Analysis Process: dash PID: 3605 Parent PID: 3604

General

Start time:	15:41:20
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3605 Parent PID: 3604

General

Start time:	15:41:20
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3606 Parent PID: 3604

General

Start time:	15:41:20
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3606 Parent PID: 3604

General

Start time:	15:41:20
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3622 Parent PID: 2520

General

Start time:	15:41:20
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3622 Parent PID: 2520

General

Start time:	15:41:20
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3633 Parent PID: 3632

General

Start time:	15:41:21
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3633 Parent PID: 3632

General

Start time:	15:41:21
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3634 Parent PID: 3632

General

Start time:	15:41:21
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3634 Parent PID: 3632

General

Start time:	15:41:21
Start date:	22/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3648 Parent PID: 2520

General

Start time:	15:41:21
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3648 Parent PID: 2520

General

Start time:	15:41:21
Start date:	22/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3660 Parent PID: 2520

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3660 Parent PID: 2520

General

Start time:	15:41:22

Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DOMAINS=/ { s/^.*=/search /; p}" /run/systemd/netif/state
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3661 Parent PID: 2520

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: resolvconf PID: 3661 Parent PID: 2520

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/sbin/resolvconf
Arguments:	/bin/sh /sbin/resolvconf -a networkd
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Read

Analysis Process: resolvconf PID: 3674 Parent PID: 3661

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: mkdir PID: 3674 Parent PID: 3661

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/bin/mkdir
Arguments:	mkdir -p /run/resolvconf/interface

File size:	76848 bytes
MD5 hash:	a97f666f21c85ec62ea47d022263ef41

File Activities

File Read

Directory Created

Analysis Process: resolvconf PID: 3677 Parent PID: 3661

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: resolvconf PID: 3678 Parent PID: 3677

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sed PID: 3678 Parent PID: 3677

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -e s/#.*$// -e s/[[:blank:]]\\+$// -e s/^[[:blank:]]\\+// -e "s/[[:blank:]]\\+/ /g" -e "/^nameserver/!b ENDOFCYCLE" -e "s/$/ /" -e "s/\\([:.]\\)0\\+/\\10/g" -e "s/\\([:.]\\)0\\([123456789abcdefABCDEF][[:xdigit:]]*\\)/\\1\\2/g" -e "/::/b ENDOFCYCLE; s/ \\(0[:]\\)\\+/ ::/" -e "/::/b ENDOFCYCLE; s/:\\(0[:]\\)\\+/::/" -e ": ENDOFCYCLE" -
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: resolvconf PID: 3679 Parent PID: 3677

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/sbin/resolvconf

Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sed PID: 3679 Parent PID: 3677

General

Start time:	15:41:22
Start date:	22/11/2020
Path:	/bin/sed
Arguments:	sed -e s/[[:blank:]]\\+$// -e /^$/d
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3711 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3711 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/mkdir
Arguments:	mkdir -p /home/user/.cache/logrotate
File size:	76848 bytes
MD5 hash:	a97f666f21c85ec62ea47d022263ef41

File Activities

File Read

Directory Created

Analysis Process: dash PID: 3712 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash

Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3712 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/mkdir
Arguments:	mkdir -p /home/user/.cache/upstart
File size:	76848 bytes
MD5 hash:	a97f666f21c85ec62ea47d022263ef41

File Activities

File Read

Directory Created

Analysis Process: dash PID: 3713 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: egrep PID: 3713 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/egrep
Arguments:	/bin/sh /bin/egrep [^[:print:]] /home/user/.cache/logrotate/status
File size:	28 bytes
MD5 hash:	ef55d1537377114cc24cdc398fbdd930

File Activities

File Read

Analysis Process: grep PID: 3713 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/grep

Arguments:	grep -E [^[:print:]] /home/user/.cache/logrotate/status
File size:	211224 bytes
MD5 hash:	fc9b0a0ff848b35b3716768695bf2427

File Activities

File Read

Analysis Process: dash PID: 3715 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mktemp PID: 3715 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/mktemp
Arguments:	mktemp
File size:	39728 bytes
MD5 hash:	91cf2e2a84f3b49fdecdd8b631902009

File Activities

File Read

Analysis Process: dash PID: 3783 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: cat PID: 3783 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/cat
Arguments:	cat
File size:	52080 bytes
MD5 hash:	efa10d52f37361f2e3a5d22742f0fcc4

File Activities

File Read

File Written

Analysis Process: dash PID: 3784 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: logrotate PID: 3784 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.d54CkEbiVw
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Permission Modified

Analysis Process: logrotate PID: 3786 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3786 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3802 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3802 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3803 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3803 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3807 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3807 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3837 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3837 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3838 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3838 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3839 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes

MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3839 Parent PID: 3784

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: dash PID: 3840 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: rm PID: 3840 Parent PID: 2079

General

Start time:	15:41:34
Start date:	22/11/2020
Path:	/bin/rm
Arguments:	rm -f /tmp/tmp.d54CkEbiVw
File size:	60272 bytes
MD5 hash:	b79876063d894c449856cca508ecca7f

File Activities

File Deleted

File Read