ID: 323091
Sample Name: Mozi.m
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 10:19:59
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	323091
MD5:	fbe51695e97a45d.
SHA1:	1ed14334b5b717..
SHA256:	2e4506802aedea..

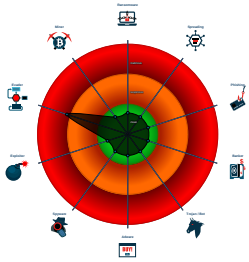
Detection

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: 3190, Parent: 3189)
  - sed (PID: 3190, Parent: 3189, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3191, Parent: 3189)
  - sort (PID: 3191, Parent: 3189, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3198, Parent: 2522)
  - sleep (PID: 3198, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3218, Parent: 3217)
  - sed (PID: 3218, Parent: 3217, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3219, Parent: 3217)
  - sort (PID: 3219, Parent: 3217, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3220, Parent: 2522)
  - sleep (PID: 3220, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3246, Parent: 3245)
  - sed (PID: 3246, Parent: 3245, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3247, Parent: 3245)
  - sort (PID: 3247, Parent: 3245, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3248, Parent: 2522)
  - sleep (PID: 3248, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3274, Parent: 3273)
  - sed (PID: 3274, Parent: 3273, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3275, Parent: 3273)
  - sort (PID: 3275, Parent: 3273, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3278, Parent: 2522)
  - sleep (PID: 3278, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3302, Parent: 3301)
  - sed (PID: 3302, Parent: 3301, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3303, Parent: 3301)
  - sort (PID: 3303, Parent: 3301, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3304, Parent: 2522)
  - sleep (PID: 3304, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3330, Parent: 3329)
  - sed (PID: 3330, Parent: 3329, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3331, Parent: 3329)
  - sort (PID: 3331, Parent: 3329, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3346, Parent: 2522)
  - sleep (PID: 3346, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3358, Parent: 3357)
  - sed (PID: 3358, Parent: 3357, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3359, Parent: 3357)
  - sort (PID: 3359, Parent: 3357, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3372, Parent: 2522)
  - sleep (PID: 3372, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3386, Parent: 3385)
  - sed (PID: 3386, Parent: 3385, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3387, Parent: 3385)
  - sort (PID: 3387, Parent: 3385, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3401, Parent: 2522)
  - sleep (PID: 3401, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1

- dash New Fork (PID: 3414, Parent: 3413)
  - sed (PID: 3414, Parent: 3413, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3415, Parent: 3413)
  - sort (PID: 3415, Parent: 3413, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3416, Parent: 2522)
  - sleep (PID: 3416, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3443, Parent: 3442)
  - sed (PID: 3443, Parent: 3442, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3444, Parent: 3442)
  - sort (PID: 3444, Parent: 3442, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3456, Parent: 2522)
  - sleep (PID: 3456, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
  - Mozi.m (PID: 3472, Parent: 3132, MD5: fbe51695e97a45dc61967dc3241a37dc) Arguments: /usr/bin/qemu-mips /tmp/Mozi.m
- upstart New Fork (PID: 3490, Parent: 2015)
  - sh (PID: 3490, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3491, Parent: 3490)
    - date (PID: 3491, Parent: 3490, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3492, Parent: 3490)
    - apport-checkreports (PID: 3492, Parent: 3490, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 3517, Parent: 2015)
  - sh (PID: 3517, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3518, Parent: 3517)
    - date (PID: 3518, Parent: 3517, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3527, Parent: 3517)
    - apport-gtk (PID: 3527, Parent: 3517, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 3544, Parent: 2015)
  - sh (PID: 3544, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3545, Parent: 3544)
    - date (PID: 3545, Parent: 3544, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3546, Parent: 3544)
    - apport-gtk (PID: 3546, Parent: 3544, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- dash New Fork (PID: 3572, Parent: 3571)
  - sed (PID: 3572, Parent: 3571, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3573, Parent: 3571)
  - sort (PID: 3573, Parent: 3571, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3574, Parent: 2522)
  - sleep (PID: 3574, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3600, Parent: 3599)
  - sed (PID: 3600, Parent: 3599, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3601, Parent: 3599)
  - sort (PID: 3601, Parent: 3599, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3602, Parent: 2522)
  - sleep (PID: 3602, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3628, Parent: 3627)
  - sed (PID: 3628, Parent: 3627, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3629, Parent: 3627)
  - sort (PID: 3629, Parent: 3627, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3630, Parent: 2522)
  - sleep (PID: 3630, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3656, Parent: 3655)
  - sed (PID: 3656, Parent: 3655, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3657, Parent: 3655)
  - sort (PID: 3657, Parent: 3655, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3663, Parent: 2522)
  - sleep (PID: 3663, Parent: 2522, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3683, Parent: 2522)
  - sed (PID: 3683, Parent: 2522, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DOMAINS=/ { s/^.*=/search /; p}" /run/systemd/netif/state
- dash New Fork (PID: 3684, Parent: 2522)
  - resolvconf (PID: 3684, Parent: 2522, MD5: 4e4ff2bfda7a6d18405a462937b63a2e) Arguments: /bin/sh /sbin/resolvconf -a networkd
    - resolvconf New Fork (PID: 3685, Parent: 3684)
    - mkdir (PID: 3685, Parent: 3684, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /run/resolvconf/interface
    - resolvconf New Fork (PID: 3686, Parent: 3684)
      - resolvconf New Fork (PID: 3687, Parent: 3686)
      - sed (PID: 3687, Parent: 3686, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/#.*$// -e s/[[:blank:]]\\+$// -e s/^[[:blank:]]\\+// -e "s/[[:blank:]]\\+/ /g" -e "/^nameserver/!b ENDOFCYCLE" -e "s/$/ /" -e "s/\\([:.]\\)0\\+/\\10/g" -e "s/\\([:.]\\)0\\([123456789abcdefABCDEF][[:xdigit:]]*\\)/\\1\\2/g" -e "/::/b ENDOFCYCLE; s/ \\(0[:]\\)\\+/ ::/" -e "/::/b ENDOFCYCLE; s/:\\(0[:]\\)\\+/::/" -e ": ENDOFCYCLE" -
      - resolvconf New Fork (PID: 3688, Parent: 3686)
      - sed (PID: 3688, Parent: 3686, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/[[:blank:]]\\+$// -e /^$/d
- dash New Fork (PID: 3734, Parent: 2079)
  - mkdir (PID: 3734, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/logrotate
- dash New Fork (PID: 3735, Parent: 2079)
  - mkdir (PID: 3735, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/upstart
- dash New Fork (PID: 3737, Parent: 2079)
  - egrep (PID: 3737, Parent: 2079, MD5: ef55d1537377114cc24cdc398fbdd930) Arguments: /bin/sh /bin/egrep [^[:print:]] /home/user/.cache/logrotate/status
  - grep (PID: 3737, Parent: 2079, MD5: fc9b0a0ff848b35b3716768695bf2427) Arguments: grep -E [^[:print:]] /home/user/.cache/logrotate/status
- dash New Fork (PID: 3785, Parent: 2079)
  - mktemp (PID: 3785, Parent: 2079, MD5: 91cf2e2a84f3b49fdecdd8b631902009) Arguments: mktemp
- dash New Fork (PID: 3789, Parent: 2079)
  - cat (PID: 3789, Parent: 2079, MD5: efa10d52f37361f2e3a5d22742f0fcc4) Arguments: cat
- dash New Fork (PID: 3793, Parent: 2079)
  - logrotate (PID: 3793, Parent: 2079, MD5: d0eaf9942936032d217478b93e9cd4b1) Arguments: logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.krni3EbUJS
    - logrotate New Fork (PID: 3824, Parent: 3793)
    - gzip (PID: 3824, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3825, Parent: 3793)
    - gzip (PID: 3825, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3826, Parent: 3793)
    - gzip (PID: 3826, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3832, Parent: 3793)
    - gzip (PID: 3832, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3840, Parent: 3793)

- logrotate New Fork (PID: 3840, Parent: 3793)
  - gzip (PID: 3840, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
  - logrotate New Fork (PID: 3868, Parent: 3793)
  - gzip (PID: 3868, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
  - logrotate New Fork (PID: 3870, Parent: 3793)
  - gzip (PID: 3870, Parent: 3793, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
- dash New Fork (PID: 3871, Parent: 2079)
  - rm (PID: 3871, Parent: 2079, MD5: b79876063d894c449856cca508ecca7f) Arguments: rm -f /tmp/tmp.krni3EbUJS
  - **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Mozi.m	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x1fce8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x1fd57:$s2: $Id: UPX • 0x1fd08:$s3: $Info: This file is packed with the UPX executable packer

Signature Overview

Click to jump to signature section

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

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Data Obfuscation:

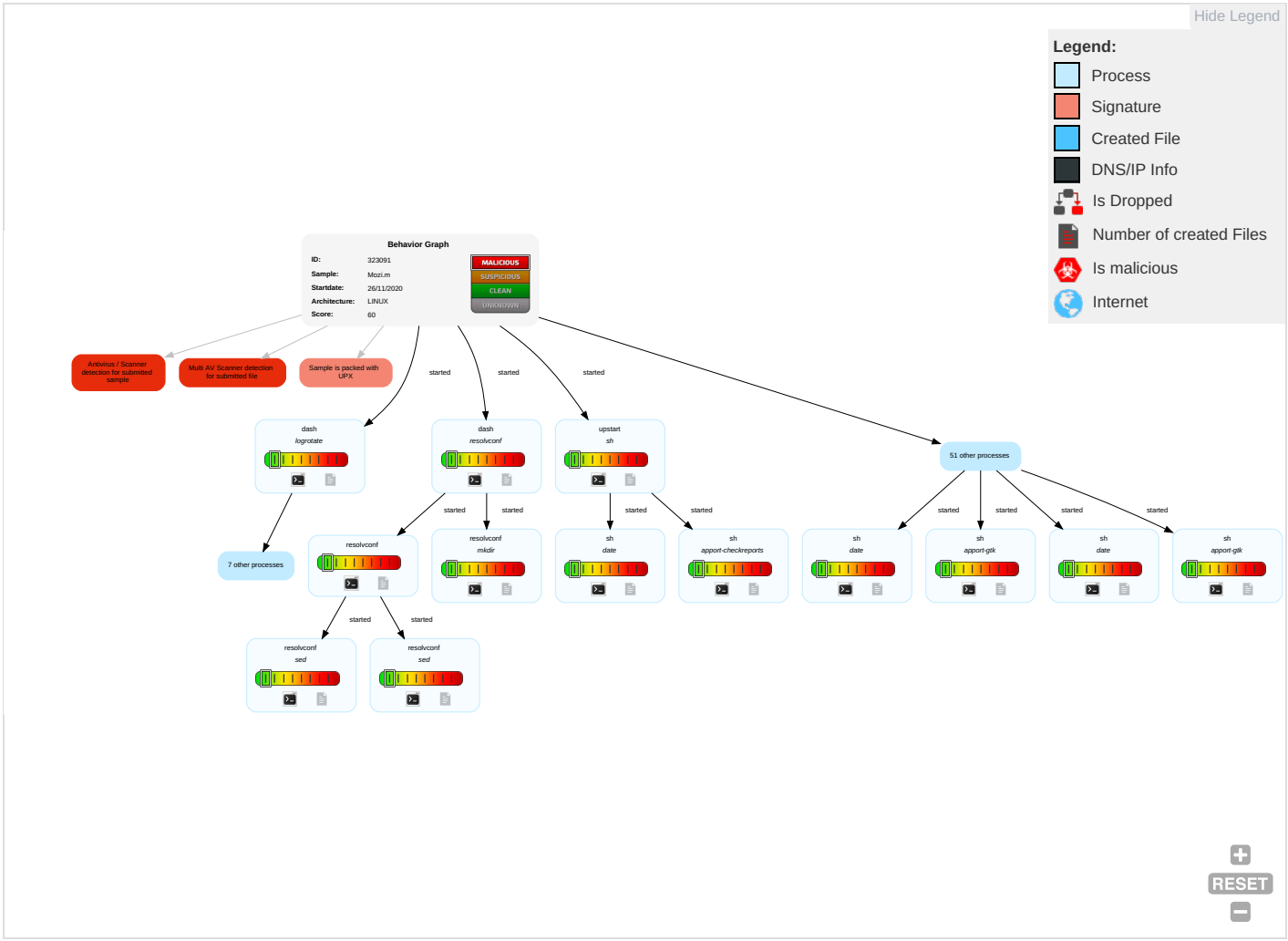
Sample is packed with UPX

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 Syst 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
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
Mozi.m	63%	Virustotal		Browse
Mozi.m	42%	Metadefender		Browse
Mozi.m	59%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.m	100%	Avira	LINUX/Mirai.souoo	

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:	323091
Start date:	26.11.2020
Start time:	10:19:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mozi.m
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.linM@0/11@0/0

Runtime Messages

Command:	/tmp/Mozi.m
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):	4.857712597745051
Encrypted:	false
SSDEEP:	24:fOeWfnS8MHEIJWfnr3KLWfnw7WfnDvzTNMHAIbRMHtW8MF8iQlNwWfnRvRMHa:2elNHEcsUnbHAXHtWbFLtseHa
MD5:	70B6484DEC8D48F9661CDFFF1E336700
SHA1:	4F542473AF66E6F700B7D10BAB17554A911898AE
SHA-256:	0708166FBC346B7BFB4DCE7643B6E2B79E38FF4AED39BEE077C0A8C25A47DB24
SHA-512:	6C47C88F7133D73DFB3C185E1D9EA7BF071DC6CE6B7F9C47F0DC1B20FF30E978A8FFCE99B10262A3E166DD32C6EBB05F3BA0A34FDB19BBEDB9DD284BFF7DEF8
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" 2020-11-26-11:0:0."/home/user/.cache/upstart/indicator-session.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/dbus.log" 2020-11-26-11:20:45."/home/user/.cache/upstart/gnome-keyring-ssh.log" 2020-11-26-11:20:45."/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" 2020-11-26-11:20:45."/home/user/.cache/upstart/update-notifier-release.log" 2020-11-26-11:20:45."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr_share_apport_apport.0.crash.log" 2020-11-26-11:0:0."/home/user/.cache/upstart/ssh-agent.log" 2020-11-26-11:20:45."/home/user/.cache/upstart/update-notifier-crash-_var_crash

/home/user/.cache/upstart/dbus.log.1.gz	
Process:	/bin/gzip
File Type:	Thu Nov 26 09:20:04 2020, from Unix
Category:	dropped
Size (bytes):	267
Entropy (8bit):	7.1812680066395425
Encrypted:	false
SSDEEP:	6:XpJGYlQuom0gW0F46ASWpC8t0BEP80ryEbjL+swraiuWRGI:XpJG/nLT0F48WUTBEEAJPyROi0l
MD5:	8D140284503EE0CB68F2DDEFE438E1CC
SHA1:	2D7978E5943C27F8D46AB7BFCF9E1A3FA77AE623
SHA-256:	A0430C64515E15D89DEF76DAE5FDEBB07B6F4A7E6BA23E59F2ECB62BA397EC00
SHA-512:	F26C934A1B46CE8B46A56EDB90DCE73B1D7345DB535E79279A155E1DCAC58A02E7E92FA28CD60B5436E7555840AA3DF14F6B63F0F9B859C61B9A21825141ADD2
Malicious:	false
Reputation:	low
Preview:	....Ds._.....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

/home/user/.cache/upstart/gnome-keyring-ssh.log.1.gz	
SHA1:	E6348E8BB25396F0542E7E74AE30AF03F48E237E
SHA-256:	606AE477FACBE88A7BF8C1718AE0259E50487BB5F98B80F0E2895DD799BBE858
SHA-512:	C2CA8D2DFC0B0E28FDB3E94EF2BE74D7D663E9943EE55D03F9F8C8E1425AC4C0C07391020DEE0931EC9967185BDD75BDA438BC413DDBC6AB18D2EF28388C D59
Malicious:	false
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:FtPa5qBO0YYLB0trI1mlwdn: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:	Thu Nov 26 10:20:28 2020, from Unix
Category:	dropped
Size (bytes):	1151
Entropy (8bit):	7.839662990069546
Encrypted:	false
SSDEEP:	24:XG+BojMnJnBU5Lk9eIEtZHE9LYIOzgczACtLQ1vzKpDk/aR:XG+iI9u5LCEtFE9LBOzjACEKQA
MD5:	1616762E572B166004B19A4132E6FD69
SHA1:	F2121F5A2784A362A18EEBD61A8C8BBC97A54B28
SHA-256:	8B82466F1F45A8A46A9F1308D399DA1ED66D8E37566DA268B081277F306A6DA0
SHA-512:	7BDD8CF79CEA04AE92DCC4F9E603AFFCD6581B71DA0B71616636CD1B96278FD7123B35B2281A0DA0A2F82AB155AFEB776F0353B40AEFA6A8C5B0E37FD69DF B2A
Malicious:	false
Reputation:	low
Preview:	....I.._...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.....+"..I.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..*.I.^S....e.>.1|.v.K...EK.B....;...uZPG.8.:J.&.....@

/home/user/.cache/upstart/update-notifier-release.log.1.gz	
Process:	/bin/gzip

/home/user/.cache/upstart/update-notifier-release.log.1.gz	
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
SHA-512:	AAE4EF554245D1419335B80EA6ED0E357FCC7032BF991D4808B8A2E09F671BA318B7EF0A8824FA334D6B51EF7104351461814D1EE096D357305914A83380CC35
Malicious:	false
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:	false
Reputation:	moderate, very likely benign file
Preview:	....._..+-(.I,*.M-K.+.M*.LIOU(.././(J....(...'...+..X..r.....3...

/tmp/tmp.krni3EbUJS	
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:	false
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):	4.670630160235773
Encrypted:	false
SSDEEP:	96:3G8hu3F44/fZbhSEEnj3lVJ8WQ5wvHqX9CK7Sqd4UIEzxPICd4YXrm:3GlxbhSEEnj3DrX9CJUIEzxPIehbm
MD5:	D87E3CEF148E96E369CBBFB92740737D
SHA1:	7E7E166F26541F695FB5BD00B49EA751784F1910
SHA-256:	0CB7934CADF4D31781B1CDE3A3122DB36D4BE3CF4181DED66A736C750E248B90
SHA-512:	469E735B6D9D5BA6DCAC67AB0ABB6605B410A3CA5C4DC65FD1D40975C31CDBF7DFBA70250C26764DDC030453B2BFF9A0DC6AC77F2E0A369AF9893F788C54E539
Malicious:	false
Reputation:	low

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
Preview:	ProblemType: Crash.Date: Thu Nov 26 11:20:28 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 . 01c19000-01f72000 rw-p 00000000 00:00 0 [heap]. 7f755e753000-7f755e8d4000 rw-p 00000000 00:00 0 . 7f755e8d4000-7f755e8eb000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f755e8eb000-7f755eaea000 ---p 00017000 fc:0

/var/crash/_usr_share_apport_apport-gtk.1000.crash	
Process:	/usr/share/apport/apport-gtk
File Type:	ASCII text
Category:	dropped
Size (bytes):	47094
Entropy (8bit):	4.505156357986673
Encrypted:	false
SSDEEP:	768:91gBbhDbUqbwNJlIaBXalrzjcwOC7LuU/SLwQ2z7wz4JkOzqqFyYApvXG2+ZMALx:ihHUewpFvw/0/X/P/Mo8r3a4FB+0s66c
MD5:	DB041CAB433D7C346A0F1E43AD66A1A1
SHA1:	1299AAF824842E39650F51A58B02B9ABF054E8D1
SHA-256:	C71743402153E39E193538283D62E7FE49C51C7FD4EF3EF62116011A5949BBCE
SHA-512:	F9BE45EEDA20B51E6EA98743FAE915AB8B1336B44EEAEB80F540EC28B1CE4FFE17D86D26C3118AAEAACCA1581DE3A209036D5BA293DDA9B8999213D715907DF1
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Thu Nov 26 11:20:29 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 . 01b26000-02049000 rw-p 00000000 00:00 0 [heap]. 7f48ee2ce000-7f48ee3ce000 rw-p 00000000 00:00 0 . 7f48ee3ce000-7f48ee3e5000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f48ee3e5000-7f48ee5e4000 ---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):	7.813753507680382
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	Mozi.m
File size:	132876
MD5:	fbe51695e97a45dc61967dc3241a37dc
SHA1:	1ed14334b5b71783cd6ec14b8a704fe48e600cf0
SHA256:	2e4506802aedea2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6
SHA512:	c35eab56ba59beb2ec2b362e4d1aae734fadc2d9db1d720439337dcade13ec9c7b68da9d03821efc7277abaf9bace342ff35593373e04c67327d5f7db460ad8a
SSDEEP:	3072:/TNVO/QJHZcfFj4rwLQGTNO5VZLwHm7vuQTpZUyY6cot:7O/QJHZweEL/NOjCHm7FZZncI
File Content Preview:	.ELF.....A.h...4.....4. ...(.....@...@.....C...C.....*.*UPX!.X.....\....|.$..ELF.....@.`....4..^h... ...(.....<...@.....ll.....H.W.`.t.d.....dt.Q.....].M.....6...

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

ELF header

ABI Version:	0
Entry Point Address:	0x41fb68
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x205b2	0x205b2	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x8ac18	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: dash PID: 3190 Parent PID: 3189

General

Start time:	10:20:19
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3190 Parent PID: 3189

General

Start time:	10:20:19
Start date:	26/11/2020
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: 3191 Parent PID: 3189

General

Start time:	10:20:19
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3191 Parent PID: 3189

General

Start time:	10:20:19
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3198 Parent PID: 2522

General

Start time:	10:20:19
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3198 Parent PID: 2522

General

Start time:	10:20:19
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3218 Parent PID: 3217

General

Start time:	10:20:20
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3218 Parent PID: 3217

General

Start time:	10:20:20
Start date:	26/11/2020
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: 3219 Parent PID: 3217

General

Start time:	10:20:20
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3219 Parent PID: 3217

General

Start time:	10:20:20
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3220 Parent PID: 2522

General

Start time:	10:20:20

Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3220 Parent PID: 2522

General

Start time:	10:20:20
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3246 Parent PID: 3245

General

Start time:	10:20:21
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3246 Parent PID: 3245

General

Start time:	10:20:21
Start date:	26/11/2020
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: 3247 Parent PID: 3245

General

Start time:	10:20:21
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3247 Parent PID: 3245

General

Start time:	10:20:21
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3248 Parent PID: 2522

General

Start time:	10:20:21
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3248 Parent PID: 2522

General

Start time:	10:20:21
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3274 Parent PID: 3273

General

Start time:	10:20:22
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3274 Parent PID: 3273

General

Start time:	10:20:22
Start date:	26/11/2020
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: 3275 Parent PID: 3273

General

Start time:	10:20:22
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3275 Parent PID: 3273

General

Start time:	10:20:22
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3278 Parent PID: 2522

General

Start time:	10:20:22
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3278 Parent PID: 2522

General

Start time:	10:20:22
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3302 Parent PID: 3301

General

Start time:	10:20:23
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3302 Parent PID: 3301

General

Start time:	10:20:23
Start date:	26/11/2020
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: 3303 Parent PID: 3301

General

Start time:	10:20:23
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3303 Parent PID: 3301

General

Start time:	10:20:23
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3304 Parent PID: 2522

General

Start time:	10:20:23
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3304 Parent PID: 2522

General

Start time:	10:20:23
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3330 Parent PID: 3329

General

Start time:	10:20:24
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3330 Parent PID: 3329

General

Start time:	10:20:24

Start date:	26/11/2020
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: 3331 Parent PID: 3329

General

Start time:	10:20:24
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3331 Parent PID: 3329

General

Start time:	10:20:24
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3346 Parent PID: 2522

General

Start time:	10:20:24
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3346 Parent PID: 2522

General

Start time:	10:20:24
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1

File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3358 Parent PID: 3357

General

Start time:	10:20:25
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3358 Parent PID: 3357

General

Start time:	10:20:25
Start date:	26/11/2020
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: 3359 Parent PID: 3357

General

Start time:	10:20:25
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3359 Parent PID: 3357

General

Start time:	10:20:25
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3372 Parent PID: 2522

General

Start time:	10:20:25
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3372 Parent PID: 2522

General

Start time:	10:20:25
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3386 Parent PID: 3385

General

Start time:	10:20:26
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3386 Parent PID: 3385

General

Start time:	10:20:26
Start date:	26/11/2020
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: 3387 Parent PID: 3385

General

Start time:	10:20:26
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3387 Parent PID: 3385

General

Start time:	10:20:26
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3401 Parent PID: 2522

General

Start time:	10:20:26
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3401 Parent PID: 2522

General

Start time:	10:20:26
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3414 Parent PID: 3413

General

Start time:	10:20:27
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3414 Parent PID: 3413

General

Start time:	10:20:27
Start date:	26/11/2020
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: 3415 Parent PID: 3413

General

Start time:	10:20:27
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3415 Parent PID: 3413

General

Start time:	10:20:27
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3416 Parent PID: 2522

General

Start time:	10:20:27
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3416 Parent PID: 2522

General

Start time:	10:20:27
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3443 Parent PID: 3442

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3443 Parent PID: 3442

General

Start time:	10:20:28
Start date:	26/11/2020
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: 3444 Parent PID: 3442

General

Start time:	10:20:28

Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3444 Parent PID: 3442

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3456 Parent PID: 2522

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3456 Parent PID: 2522

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: Mozi.m PID: 3472 Parent PID: 3132

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/tmp/Mozi.m
Arguments:	/usr/bin/qemu-mips /tmp/Mozi.m

File size:	132876 bytes
MD5 hash:	fbe51695e97a45dc61967dc3241a37dc

File Activities

File Read

Analysis Process: upstart PID: 3490 Parent PID: 2015

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3490 Parent PID: 2015

General

Start time:	10:20:28
Start date:	26/11/2020
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: 3491 Parent PID: 3490

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3491 Parent PID: 3490

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3492 Parent PID: 3490

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 3492 Parent PID: 3490

General

Start time:	10:20:28
Start date:	26/11/2020
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: 3517 Parent PID: 2015

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3517 Parent PID: 2015

General

Start time:	10:20:28
Start date:	26/11/2020
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: 3518 Parent PID: 3517

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3518 Parent PID: 3517

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3527 Parent PID: 3517

General

Start time:	10:20:28
Start date:	26/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 3527 Parent PID: 3517

General

Start time:	10:20:28
Start date:	26/11/2020
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: upstart PID: 3544 Parent PID: 2015

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3544 Parent PID: 2015

General

Start time:	10:20:29
Start date:	26/11/2020
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: 3545 Parent PID: 3544

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3545 Parent PID: 3544

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes

MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3546 Parent PID: 3544

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 3546 Parent PID: 3544

General

Start time:	10:20:29
Start date:	26/11/2020
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: 3572 Parent PID: 3571

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3572 Parent PID: 3571

General

Start time:	10:20:29
Start date:	26/11/2020
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: 3573 Parent PID: 3571

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3573 Parent PID: 3571

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3574 Parent PID: 2522

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3574 Parent PID: 2522

General

Start time:	10:20:29
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3600 Parent PID: 3599

General

Start time:	10:20:30
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3600 Parent PID: 3599

General

Start time:	10:20:30
Start date:	26/11/2020
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: 3601 Parent PID: 3599

General

Start time:	10:20:30
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3601 Parent PID: 3599

General

Start time:	10:20:30
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3602 Parent PID: 2522

General

Start time:	10:20:30
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3602 Parent PID: 2522

General

Start time:	10:20:30
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3628 Parent PID: 3627

General

Start time:	10:20:31
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3628 Parent PID: 3627

General

Start time:	10:20:31
Start date:	26/11/2020
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: 3629 Parent PID: 3627

General

Start time:	10:20:31
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3629 Parent PID: 3627

General

Start time:	10:20:31
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3630 Parent PID: 2522

General

Start time:	10:20:31
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3630 Parent PID: 2522

General

Start time:	10:20:31
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3656 Parent PID: 3655

General

Start time:	10:20:32
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3656 Parent PID: 3655

General

Start time:	10:20:32
Start date:	26/11/2020
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: 3657 Parent PID: 3655

General

Start time:	10:20:32
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3657 Parent PID: 3655

General

Start time:	10:20:32
Start date:	26/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3663 Parent PID: 2522

General

Start time:	10:20:32

Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3663 Parent PID: 2522

General

Start time:	10:20:32
Start date:	26/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3683 Parent PID: 2522

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3683 Parent PID: 2522

General

Start time:	10:20:33
Start date:	26/11/2020
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: 3684 Parent PID: 2522

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: resolvconf PID: 3684 Parent PID: 2522

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/sbin/resolvconf
Arguments:	/bin/sh /sbin/resolvconf -a networkd
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

File Activities

File Read

Analysis Process: resolvconf PID: 3685 Parent PID: 3684

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: mkdir PID: 3685 Parent PID: 3684

General

Start time:	10:20:33
Start date:	26/11/2020
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: 3686 Parent PID: 3684

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a

File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: resolvconf PID: 3687 Parent PID: 3686

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: sed PID: 3687 Parent PID: 3686

General

Start time:	10:20:33
Start date:	26/11/2020
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: 3688 Parent PID: 3686

General

Start time:	10:20:33
Start date:	26/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: sed PID: 3688 Parent PID: 3686

General

Start time:	10:20:33
Start date:	26/11/2020
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: 3734 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3734 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
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: 3735 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3735 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
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: 3737 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: egrep PID: 3737 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
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: 3737 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
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: 3785 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mktemp PID: 3785 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/mktemp
Arguments:	mktemp
File size:	39728 bytes
MD5 hash:	91cf2e2a84f3b49fdecdd8b631902009

File Activities

File Read

Analysis Process: dash PID: 3789 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: cat PID: 3789 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/cat
Arguments:	cat
File size:	52080 bytes
MD5 hash:	efa10d52f37361f2e3a5d22742f0fcc4

File Activities

File Read

File Written

Analysis Process: dash PID: 3793 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: logrotate PID: 3793 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.krni3EbUJS
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: 3824 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3824 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3825 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3825 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3826 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3826 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3832 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3832 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3840 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3840 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3868 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3868 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3870 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3870 Parent PID: 3793

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: dash PID: 3871 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: rm PID: 3871 Parent PID: 2079

General

Start time:	10:20:45
Start date:	26/11/2020
Path:	/bin/rm
Arguments:	rm -f /tmp/tmp.krni3EbUJS
File size:	60272 bytes
MD5 hash:	b79876063d894c449856cca508ecca7f

File Activities

File Deleted

File Read