ID: 324350
Sample Name: nsu
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:26:59
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report nsu

Overview

General Information

Sample Name:	nsu
Analysis ID:	324350
MD5:	856d3c4cd13172..
SHA1:	8f8a112aecddc2f..
SHA256:	b1047a2a9faf9e0..

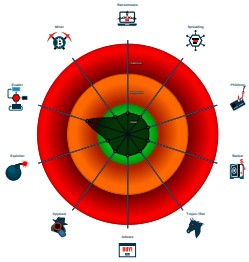
Detection

Score:	4
Range:	0 - 100
Whitelisted:	false

Signatures

- 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 strings that are pot…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…

Classification



Startup

- **system is lnxubuntu1**
- dash New Fork (PID: 3191, Parent: 3190)
  - sed (PID: 3191, Parent: 3190, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3192, Parent: 3190)
  - sort (PID: 3192, Parent: 3190, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3198, Parent: 2523)
  - sleep (PID: 3198, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3219, Parent: 3218)
  - sed (PID: 3219, Parent: 3218, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3220, Parent: 3218)
  - sort (PID: 3220, Parent: 3218, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3221, Parent: 2523)
  - sleep (PID: 3221, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3247, Parent: 3246)
  - sed (PID: 3247, Parent: 3246, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3248, Parent: 3246)
  - sort (PID: 3248, Parent: 3246, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3258, Parent: 2523)
  - sleep (PID: 3258, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3275, Parent: 3274)
  - sed (PID: 3275, Parent: 3274, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3276, Parent: 3274)
  - sort (PID: 3276, Parent: 3274, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3277, Parent: 2523)
  - sleep (PID: 3277, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3303, Parent: 3302)
  - sed (PID: 3303, Parent: 3302, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3304, Parent: 3302)
  - sort (PID: 3304, Parent: 3302, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3306, Parent: 2523)
  - sleep (PID: 3306, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3331, Parent: 3330)
  - sed (PID: 3331, Parent: 3330, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3332, Parent: 3330)
  - sort (PID: 3332, Parent: 3330, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3338, Parent: 2523)
  - sleep (PID: 3338, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3359, Parent: 3358)
  - sed (PID: 3359, Parent: 3358, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3360, Parent: 3358)
  - sort (PID: 3360, Parent: 3358, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3370, Parent: 2523)
  - sleep (PID: 3370, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3387, Parent: 3386)
  - sed (PID: 3387, Parent: 3386, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3388, Parent: 3386)
  - sort (PID: 3388, Parent: 3386, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3403, Parent: 2523)
  - sleep (PID: 3403, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1

- dash New Fork (PID: 3415, Parent: 3414)
  - sed (PID: 3415, Parent: 3414, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3416, Parent: 3414)
  - sort (PID: 3416, Parent: 3414, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3427, Parent: 2523)
  - sleep (PID: 3427, Parent: 2523, 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: 3454, Parent: 2523)
  - sleep (PID: 3454, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
  - nsu (PID: 3479, Parent: 3133, MD5: 856d3c4cd13172355643638458e72f39) Arguments: /tmp/nsu
- dash New Fork (PID: 3490, Parent: 3489)
  - sed (PID: 3490, Parent: 3489, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3491, Parent: 3489)
  - sort (PID: 3491, Parent: 3489, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3492, Parent: 2523)
  - sleep (PID: 3492, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3518, Parent: 3517)
  - sed (PID: 3518, Parent: 3517, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3519, Parent: 3517)
  - sort (PID: 3519, Parent: 3517, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3535, Parent: 2523)
  - sleep (PID: 3535, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3546, Parent: 3545)
  - sed (PID: 3546, Parent: 3545, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3547, Parent: 3545)
  - sort (PID: 3547, Parent: 3545, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3558, Parent: 2523)
  - sleep (PID: 3558, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3574, Parent: 3573)
  - sed (PID: 3574, Parent: 3573, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3575, Parent: 3573)
  - sort (PID: 3575, Parent: 3573, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3576, Parent: 2523)
  - sleep (PID: 3576, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3601, Parent: 2523)
  - sed (PID: 3601, Parent: 2523, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DOMAINS=/ { s/^.*=/search /; p}" /run/systemd/netif/state
- dash New Fork (PID: 3602, Parent: 2523)
  - resolvconf (PID: 3602, Parent: 2523, MD5: 4e4ff2bfda7a6d18405a462937b63a2e) Arguments: /bin/sh /sbin/resolvconf -a networkd
    - resolvconf New Fork (PID: 3613, Parent: 3602)
      - mkdir (PID: 3613, Parent: 3602, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /run/resolvconf/interface
    - resolvconf New Fork (PID: 3620, Parent: 3602)
      - resolvconf New Fork (PID: 3621, Parent: 3620)
        - sed (PID: 3621, Parent: 3620, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/#.*$// -e s/[[:blank:]]\\+$// -e s/^[[:blank:]]\\+// -e "s/[[:blank:]]\\+/ /g" -e "/^nameserver/!b ENDOFCYCLE" -e "s/$/ /" -e "s/\\([:.]\\)0\\+/\\10/g" -e "s/\\([:.]\\)0\\([123456789abcdefABCDEF][[:xdigit:]]*\\)/\\1\\2/g" -e "/::/b ENDOFCYCLE; s/ \\(0[:]\\)\\+/ ::/" -e "/::/b ENDOFCYCLE; s/:\\(0[:]\\)\\+/::/" -e ": ENDOFCYCLE" -
      - resolvconf New Fork (PID: 3622, Parent: 3620)
        - sed (PID: 3622, Parent: 3620, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/[[:blank:]]\\+$// -e /^$/d
- dash New Fork (PID: 3652, Parent: 2079)
  - mkdir (PID: 3652, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/logrotate
- dash New Fork (PID: 3653, Parent: 2079)
  - mkdir (PID: 3653, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/upstart
- dash New Fork (PID: 3654, Parent: 2079)
  - egrep (PID: 3654, Parent: 2079, MD5: ef55d1537377114cc24cdc398fbdd930) Arguments: /bin/sh /bin/egrep [^[:print:]] /home/user/.cache/logrotate/status
  - grep (PID: 3654, Parent: 2079, MD5: fc9b0a0ff848b35b3716768695bf2427) Arguments: grep -E [^[:print:]] /home/user/.cache/logrotate/status
- dash New Fork (PID: 3689, Parent: 2079)
  - mktemp (PID: 3689, Parent: 2079, MD5: 91cf2e2a84f3b49fdecdd8b631902009) Arguments: mktemp
- dash New Fork (PID: 3724, Parent: 2079)
  - cat (PID: 3724, Parent: 2079, MD5: efa10d52f37361f2e3a5d22742f0fcc4) Arguments: cat
- dash New Fork (PID: 3725, Parent: 2079)
  - logrotate (PID: 3725, Parent: 2079, MD5: d0eaf9942936032d217478b93e9cd4b1) Arguments: logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.zmF3WJPRCX
    - logrotate New Fork (PID: 3726, Parent: 3725)
      - gzip (PID: 3726, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3727, Parent: 3725)
      - gzip (PID: 3727, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3728, Parent: 3725)
      - gzip (PID: 3728, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3733, Parent: 3725)
      - gzip (PID: 3733, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3772, Parent: 3725)
      - gzip (PID: 3772, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3779, Parent: 3725)
      - gzip (PID: 3779, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3780, Parent: 3725)
      - gzip (PID: 3780, Parent: 3725, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
- dash New Fork (PID: 3787, Parent: 2079)
  - rm (PID: 3787, Parent: 2079, MD5: b79876063d894c449856cca508ecca7f) Arguments: rm -f /tmp/tmp.zmF3WJPRCX
- **cleanup**

Yara Overview

No yara matches

Signature Overview

- System Summary
- Persistence and Installation Behavior
- Malware Analysis System Evasion

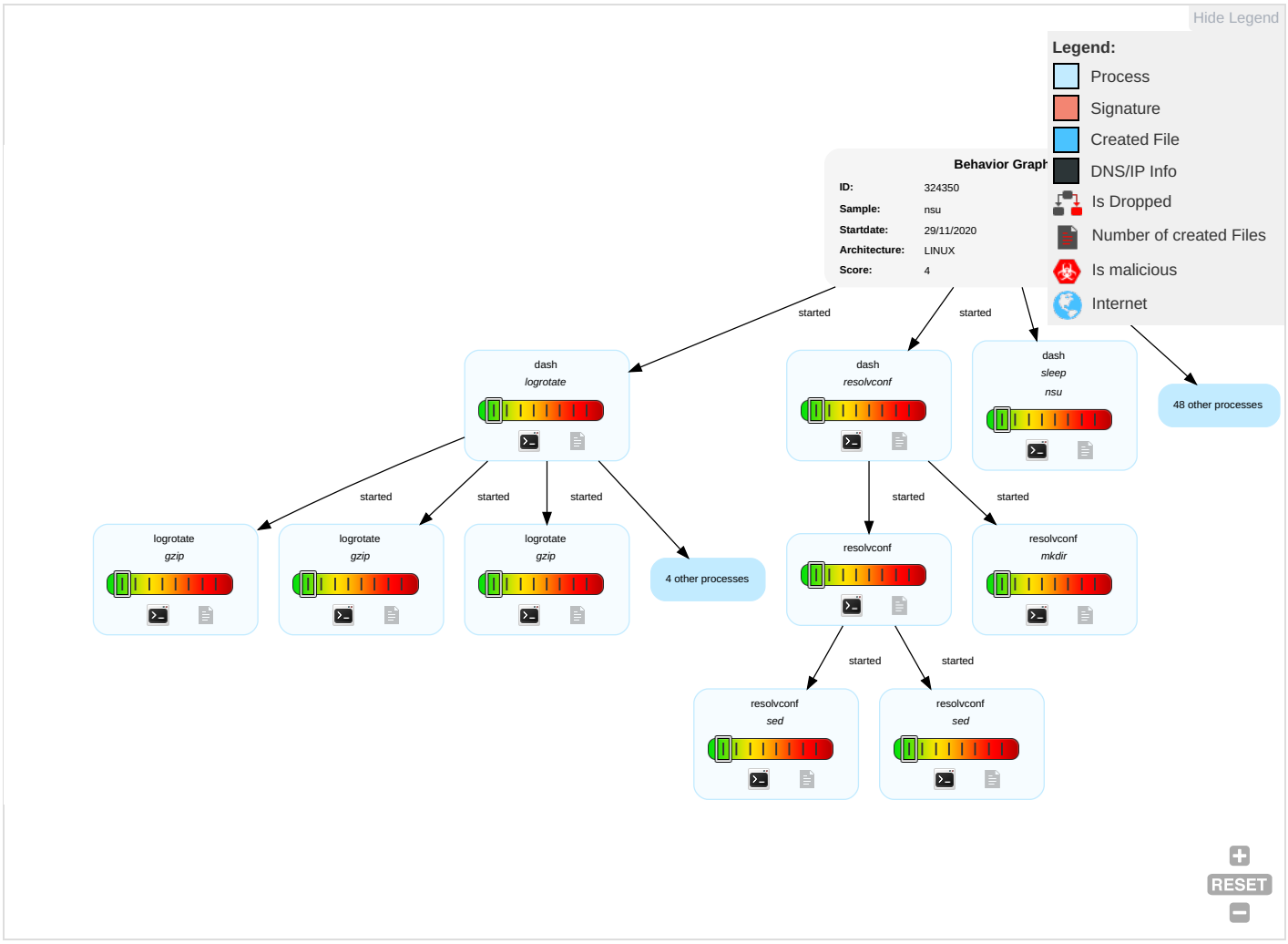
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Command and Scripting Interpreter 1	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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File Deletion 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	Device Lockout

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nsu	0%	Virustotal		Browse
nsu	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324350
Start date:	29.11.2020
Start time:	13:26:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nsu
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:	CLEAN
Classification:	clean4.lin@0/9@0/0

Runtime Messages

Command:	/tmp/nsu
Exit Code:	1
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	nsu: Can't open /etc/ppf Error: 2 (No such file or directory)

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):	1087
Entropy (8bit):	4.891886996638601
Encrypted:	false
SSDEEP:	24:fOeWfnS8JWfnrkNLWfnw7WfnDvIT6bWMHtW8MF8iQl6wWfnRvu:2elIs4noHtWbFLIsW
MD5:	57089C03CDB6823AB0096C266AE9165F
SHA1:	32ECE44A2A0214658524F52401098A7C4C1022D0
SHA-256:	FEF0A79D3CE40FB68E1CAB2B3FC6F275785CF0666A6A004CEE97514B6C810AB5
SHA-512:	2F1E2E2B46B0893665BE6DD177DC7CF410D6056D4F397107210256FD6AE574EDD73BA02F0F27C4DC0773FDF137A0044F137B7A3D83C6D1C4D538D0BC0D29FB
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/indicator-session.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/dbus.log" 2020-11-29-14:27:45."/home/user/.cache/upstart/gnome-keyring-ssh.log" 2020-11-29-14:27:45."/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" 2020-11-29-14:27:45."/home/user/.cache/upstart/update-notifier-release.log" 2020-11-29-14:27:45."/home/user/.cache/upstart/ssh-agent.log" 2020-11-29-14:27:45."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr_bin_blueman-applet.0.crash.log" 2018-5-7-10:33:19."/home/user/.cache/upstart/indicator-keyboard.log" 2018-5-7-10:33:19."/home/user/.cache/upstart/upstart-event-bridge.log" 2020-11-29-14:27:45."/home/user/.cache/upstart/indicator-powe

/home/user/.cache/upstart/dbus.log.1.gz	
Process:	/bin/gzip
File Type:	Sun Nov 29 12:27:04 2020, from Unix
Category:	dropped
Size (bytes):	267
Entropy (8bit):	7.174768615278084
Encrypted:	false
SSDEEP:	6:XOYlQuom0gW0F46ASWpC8t0BEP80ryEbjL+swraiuWRGI:XO/nLT0F48WUTBEEAJPyROi0l
MD5:	5D34DDBA137C2FA72088BC59597862AC
SHA1:	9976302C26C6BFFAD842E8E16D5DEC6C7A2314DD
SHA-256:	C30FD9B3A06FA8AB93117A05BA9EECAB9A87881ED1F4A09CC0C3232552D862C8
SHA-512:	9608A3BDD2D1ECD816EC87844EAE474C922A87F95F755C1BA7AE54FD9D102C2910504987692831D3919B98E97EEC5CE0D274CD25A97AAE95D0F57485C6CF7E5
Malicious:	false
Reputation:	low
Preview:	....._.....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:	C2CA8D2DFC0B0E28FDB3E94EF2BE74D7D663E9943EE55D03F9F8C8E1425AC4C0C07391020DEE0931EC9967185BDD75BDA438BC413DDBC6AB18D2EF28388CD59
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

/home/user/.cache/upstart/gpg-agent.log.1.gz	
SHA1:	062CEC7C61E642887CE10970A7353066C4283DFD
SHA-256:	0D9475D2511F0A2C555242326C2D4EB69E4456726BDDB84913B95EC59F8FDCF6
SHA-512:	EB0A9DDC9D084934F42DF3AC9FE92CE534A841B38F6008774F29788EEFEC4FD22BFE12570B30558A351755347E92742C867B3B65E0616294146C390FB60A3388
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......_.....0....=I...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:	Sun Nov 29 13:27:28 2020, from Unix
Category:	dropped
Size (bytes):	1151
Entropy (8bit):	7.838014518681856
Encrypted:	false
SSDEEP:	24:Xm+BojMnJnBU5Lk9eIEtZHE9LYIOzgczACtLQ1vzKpDk/aR:Xm+iI9u5LCEtFE9LBOzjACEKQA
MD5:	0737129F9674C51BAEC2B763ACD3532C
SHA1:	D41FC542AB57C920E0FC717217B6CA66CB12C1AE
SHA-256:	5445A97F93B0EE0371E2EC361D5F33328CE6FC931F2ECB98EAD41AEAAF79D68D
SHA-512:	1C4FD05980E000D0E25A2BA49FB31DBF152A7B409BBCA6E8371DE6F794C035C78A26FFF71331E8FF2AD6CB0BCAD719B770EC8944709832AC1FC6CE1B58C335 6
Malicious:	false
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.....+"..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
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
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

/home/user/.cache/upstart/upstart-event-bridge.log.1.gz	
Entropy (8bit):	5.395998870534845
Encrypted:	false
SSDEEP:	3:FtPa5wG0BMPWNLPgXseOBMky:XPa5wG+OQP4OBMV
MD5:	1395D405968C76307CBA75C5DDC9CA19
SHA1:	C36CEE03E5DF12FBFB57A5EBCEAE329B41AFA1F7
SHA-256:	33785027CEE82E878434593B532FE1DF25D46676379757272C1E15C9AADD3B1F
SHA-512:	09CAB8DFF495DA9ED715C94E9F24B0C5C40CF0BC8C1B0DEEFB90C54081020AD80AF51636ADCBA368980E2C69119697A65E2E4AC5B834E0F08F88AEA52EFDA57
Malicious:	false
Preview:	......_..+-(.I,*.M-K.+.M*.LIOU(.././(J....(...'...+..X..r.....3...

/tmp/tmp.zmF3WJPRCX	
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
Preview:	"/home/user/.cache/upstart/*.log" {. hourly. missingok. rotate 7. compress. notifempty. nocreate.}.

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.0, stripped
Entropy (8bit):	6.222609435477498
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	nsu
File size:	473276
MD5:	856d3c4cd131723556436384 58e72f39
SHA1:	8f8a112aecddc2fbef07f989dca48862b70b0628
SHA256:	b1047a2a9faf9e080c8cc8422fdb2ec4fd087963b597378903d2ebb8f24372dd
SHA512:	a622d2cad703b642b97bc39bc50717cb7150f161c828031ad7668ae9df92a980f61884c4f44656c0d11055eb22280e1982b41217e0ac44a2c205ce867d006376
SSDEEP:	6144:BafZP95pFoEACjhCuNC7BhqOtz8kI2vmFILv7aRsdpxGWidWe8X11111111111hj:BO9VoEAC9CuNC7BhqOdbISWIXxGdWj
File Content Preview:	.ELF.....4....5.....4. ...(.....l...l.....t...t.."..... ... .Q.td.....GNU.....U.....E.....'u.....

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V

ELF header	
ABI Version:	0
Entry Point Address:	0x8048100
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	4
Section Header Offset:	472516
Section Header Size:	40
Number of Section Headers:	19
Header String Table Index:	18

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80480d4	0xd4	0x17	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x8048100	0x100	0x57621	0x0	0x6	AX	0	0	32
__libc_freeres_fn	PROGBITS	0x809f730	0x57730	0x4ea	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x809fc1c	0x57c1c	0x1b	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x809fc40	0x57c40	0x167fb	0x0	0x2	A	0	0	32
__libc_subfreeres	PROGBITS	0x80b643c	0x6e43c	0x2c	0x0	0x2	A	0	0	4
__libc_atexit	PROGBITS	0x80b6468	0x6e468	0x4	0x0	0x2	A	0	0	4
.data	PROGBITS	0x80b7480	0x6e480	0x1040	0x0	0x3	WA	0	0	32
.eh_frame	PROGBITS	0x80b84c0	0x6f4c0	0x1270	0x0	0x3	WA	0	0	4
.ctors	PROGBITS	0x80b9730	0x70730	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80b9738	0x70738	0x8	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x80b9740	0x70740	0x10	0x4	0x3	WA	0	0	4
.bss	NOBITS	0x80b9760	0x70760	0x2a4a4	0x0	0x3	WA	0	0	32
__libc_freeres_ptrs	NOBITS	0x80e3c04	0x70760	0x24	0x0	0x3	WA	0	0	4
.comment	PROGBITS	0x0	0x70760	0x2c86	0x0	0x0		0	0	1
.note.ABI-tag	NOTE	0x80480b4	0xb4	0x20	0x0	0x2	A	0	0	4
.note	NOTE	0x0	0x733e6	0x12c	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x73512	0xb0	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x6e46c	0x6e46c	0x5	R E	0x1000		.init .text __libc_freeres_fn .fini .rodata __libc_subfreeres __libc_atexit .note.ABI-tag
LOAD	0x6e480	0x80b7480	0x80b7480	0x22d0	0x2c7a8	0x6	RW	0x1000		.data .eh_frame .ctors .dtors .got .bss __libc_freeres_ptrs
NOTE	0xb4	0x80480b4	0x80480b4	0x20	0x20	0x4	R	0x4		.note.ABI-tag
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0x7	RWE	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: dash PID: 3191 Parent PID: 3190

General

Start time:	13:27:18

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

Analysis Process: sed PID: 3191 Parent PID: 3190

General

Start time:	13:27:18
Start date:	29/11/2020
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: 3192 Parent PID: 3190

General

Start time:	13:27:18
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3192 Parent PID: 3190

General

Start time:	13:27:18
Start date:	29/11/2020
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: 2523

General

Start time:	13:27:18
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3198 Parent PID: 2523

General

Start time:	13:27:18
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3219 Parent PID: 3218

General

Start time:	13:27:19
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3219 Parent PID: 3218

General

Start time:	13:27:19
Start date:	29/11/2020
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: 3220 Parent PID: 3218

General

Start time:	13:27:19
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3220 Parent PID: 3218

General

Start time:	13:27:19
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3221 Parent PID: 2523

General

Start time:	13:27:19
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3221 Parent PID: 2523

General

Start time:	13:27:19
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3247 Parent PID: 3246

General

Start time:	13:27:20
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3247 Parent PID: 3246

General

Start time:	13:27:20
Start date:	29/11/2020
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: 3248 Parent PID: 3246

General

Start time:	13:27:20
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3248 Parent PID: 3246

General

Start time:	13:27:20
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3258 Parent PID: 2523

General

Start time:	13:27:20
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3258 Parent PID: 2523

General

Start time:	13:27:20
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3275 Parent PID: 3274

General

Start time:	13:27:21
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3275 Parent PID: 3274

General

Start time:	13:27:21
Start date:	29/11/2020
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: 3276 Parent PID: 3274

General

Start time:	13:27:21
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3276 Parent PID: 3274

General

Start time:	13:27:21

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

File Activities

File Read

Analysis Process: dash PID: 3277 Parent PID: 2523

General

Start time:	13:27:21
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3277 Parent PID: 2523

General

Start time:	13:27:21
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3303 Parent PID: 3302

General

Start time:	13:27:22
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3303 Parent PID: 3302

General

Start time:	13:27:22
Start date:	29/11/2020
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: 3304 Parent PID: 3302

General

Start time:	13:27:22
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3304 Parent PID: 3302

General

Start time:	13:27:22
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3306 Parent PID: 2523

General

Start time:	13:27:22
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3306 Parent PID: 2523

General

Start time:	13:27:22
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3331 Parent PID: 3330

General

Start time:	13:27:23
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3331 Parent PID: 3330

General

Start time:	13:27:23
Start date:	29/11/2020
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: 3332 Parent PID: 3330

General

Start time:	13:27:23
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3332 Parent PID: 3330

General

Start time:	13:27:23
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3338 Parent PID: 2523

General

Start time:	13:27:23
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3338 Parent PID: 2523

General

Start time:	13:27:23
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3359 Parent PID: 3358

General

Start time:	13:27:24
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3359 Parent PID: 3358

General

Start time:	13:27:24
Start date:	29/11/2020
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: 3360 Parent PID: 3358

General

Start time:	13:27:24
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3360 Parent PID: 3358

General

Start time:	13:27:24
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3370 Parent PID: 2523

General

Start time:	13:27:24
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3370 Parent PID: 2523

General

Start time:	13:27:24
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3387 Parent PID: 3386

General

Start time:	13:27:25
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3387 Parent PID: 3386

General

Start time:	13:27:25
Start date:	29/11/2020
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: 3388 Parent PID: 3386

General

Start time:	13:27:25
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3388 Parent PID: 3386

General

Start time:	13:27:25
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3403 Parent PID: 2523

General

Start time:	13:27:25

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

Analysis Process: sleep PID: 3403 Parent PID: 2523

General

Start time:	13:27:25
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3415 Parent PID: 3414

General

Start time:	13:27:27
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3415 Parent PID: 3414

General

Start time:	13:27:27
Start date:	29/11/2020
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: 3416 Parent PID: 3414

General

Start time:	13:27:26
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3416 Parent PID: 3414

General

Start time:	13:27:26
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3427 Parent PID: 2523

General

Start time:	13:27:27
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3427 Parent PID: 2523

General

Start time:	13:27:27
Start date:	29/11/2020
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:	13:27:28
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3443 Parent PID: 3442

General

Start time:	13:27:28
Start date:	29/11/2020
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:	13:27:28
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3444 Parent PID: 3442

General

Start time:	13:27:28
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3454 Parent PID: 2523

General

Start time:	13:27:28
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3454 Parent PID: 2523

General

Start time:	13:27:28
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: nsu PID: 3479 Parent PID: 3133

General

Start time:	13:27:28
Start date:	29/11/2020
Path:	/tmp/nsu
Arguments:	/tmp/nsu
File size:	473276 bytes
MD5 hash:	856d3c4cd13172355643638458e72f39

File Activities

File Read

Analysis Process: dash PID: 3490 Parent PID: 3489

General

Start time:	13:27:29
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3490 Parent PID: 3489

General

Start time:	13:27:29
Start date:	29/11/2020
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: 3491 Parent PID: 3489

General

Start time:	13:27:29
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3491 Parent PID: 3489

General

Start time:	13:27:29
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3492 Parent PID: 2523

General

Start time:	13:27:29
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3492 Parent PID: 2523

General

Start time:	13:27:29
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3518 Parent PID: 3517

General

Start time:	13:27:30
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3518 Parent PID: 3517

General

Start time:	13:27:30
Start date:	29/11/2020
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: 3519 Parent PID: 3517

General

Start time:	13:27:30
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3519 Parent PID: 3517

General

Start time:	13:27:30
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3535 Parent PID: 2523

General

Start time:	13:27:30
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3535 Parent PID: 2523

General

Start time:	13:27:30
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3546 Parent PID: 3545

General

Start time:	13:27:31
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3546 Parent PID: 3545

General

Start time:	13:27:31
Start date:	29/11/2020
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: 3547 Parent PID: 3545

General

Start time:	13:27:31
Start date:	29/11/2020
Path:	/bin/dash

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

Analysis Process: sort PID: 3547 Parent PID: 3545

General

Start time:	13:27:31
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3558 Parent PID: 2523

General

Start time:	13:27:31
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3558 Parent PID: 2523

General

Start time:	13:27:31
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3574 Parent PID: 3573

General

Start time:	13:27:32
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3574 Parent PID: 3573

General

Start time:	13:27:32
Start date:	29/11/2020
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: 3575 Parent PID: 3573

General

Start time:	13:27:32
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3575 Parent PID: 3573

General

Start time:	13:27:32
Start date:	29/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3576 Parent PID: 2523

General

Start time:	13:27:32
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3576 Parent PID: 2523

General

Start time:	13:27:32
Start date:	29/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3601 Parent PID: 2523

General

Start time:	13:27:33
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3601 Parent PID: 2523

General

Start time:	13:27:33
Start date:	29/11/2020
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: 3602 Parent PID: 2523

General

Start time:	13:27:33
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: resolvconf PID: 3602 Parent PID: 2523

General

Start time:	13:27:33
Start date:	29/11/2020
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: 3613 Parent PID: 3602

General

Start time:	13:27:33
Start date:	29/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: mkdir PID: 3613 Parent PID: 3602

General

Start time:	13:27:33
Start date:	29/11/2020
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: 3620 Parent PID: 3602

General

Start time:	13:27:33
Start date:	29/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: resolvconf PID: 3621 Parent PID: 3620

General

Start time:	13:27:33
Start date:	29/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: sed PID: 3621 Parent PID: 3620

General

Start time:	13:27:33
Start date:	29/11/2020
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: 3622 Parent PID: 3620

General

Start time:	13:27:33
Start date:	29/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: sed PID: 3622 Parent PID: 3620

General

Start time:	13:27:33
Start date:	29/11/2020
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: 3652 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3652 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
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: 3653 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3653 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
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: 3654 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: egrep PID: 3654 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
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: 3654 Parent PID: 2079

General

Start time:	13:27:44
Start date:	29/11/2020
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: 3689 Parent PID: 2079

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mktemp PID: 3689 Parent PID: 2079

General

Start time:	13:27:45

Start date:	29/11/2020
Path:	/bin/mktemp
Arguments:	mktemp
File size:	39728 bytes
MD5 hash:	91cf2e2a84f3b49fdecdd8b631902009

File Activities

File Read

Analysis Process: dash PID: 3724 Parent PID: 2079

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: cat PID: 3724 Parent PID: 2079

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/cat
Arguments:	cat
File size:	52080 bytes
MD5 hash:	efa10d52f37361f2e3a5d22742f0fcc4

File Activities

File Read

File Written

Analysis Process: dash PID: 3725 Parent PID: 2079

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: logrotate PID: 3725 Parent PID: 2079

General

Start time:	13:27:45

Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.zmF3WJPRCX
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: 3726 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3726 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3727 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a

File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3727 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3728 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3728 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3733 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020

Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3733 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3772 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3772 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3779 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3779 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3780 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3780 Parent PID: 3725

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: dash PID: 3787 Parent PID: 2079

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: rm PID: 3787 Parent PID: 2079

General

Start time:	13:27:45
Start date:	29/11/2020
Path:	/bin/rm
Arguments:	rm -f /tmp/tmp.zmF3WJPRCX
File size:	60272 bytes
MD5 hash:	b79876063d894c449856cca508ecca7f

File Activities

File Deleted

File Read