

JOESandbox Cloud BASIC



ID: 518903

Sample Name: arm7

Cookbook:
defaultlinuxfilecookbook.jbs

Time: 04:19:45

Date: 10/11/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Linux Analysis Report arm7	12
Overview	12
General Information	12
Detection	12
Signatures	12
Classification	12
Analysis Advice	12
General Information	12
Process Tree	12
Yara Overview	16
Initial Sample	16
PCAP (Network Traffic)	16
Jbx Signature Overview	16
AV Detection:	16
Networking:	16
System Summary:	16
Data Obfuscation:	16
Persistence and Installation Behavior:	16
Hooking and other Techniques for Hiding and Protection:	17
Language, Device and Operating System Detection:	17
Stealing of Sensitive Information:	17
Remote Access Functionality:	17
Mitre Att&ck Matrix	17
Malware Configuration	17
Behavior Graph	17
Antivirus, Machine Learning and Genetic Malware Detection	18
Initial Sample	18
Dropped Files	18
Domains	18
URLs	18
Domains and IPs	18
Contacted Domains	18
URLs from Memory and Binaries	18
Contacted IPs	19
Public	19
Joe Sandbox View / Context	21
IPs	21
Domains	21
ASN	21
JA3 Fingerprints	22
Dropped Files	23
Created / dropped Files	23
Static File Info	32
General	33
Static ELF Info	33
ELF header	33
Program Segments	33
Network Behavior	33
TCP Packets	33
DNS Queries	33
DNS Answers	34
System Behavior	34
Analysis Process: dash PID: 5209 Parent PID: 4331	34
General	34
Analysis Process: cat PID: 5209 Parent PID: 4331	34
General	34
File Activities	34
File Read	34
Analysis Process: dash PID: 5210 Parent PID: 4331	34
General	34
Analysis Process: head PID: 5210 Parent PID: 4331	34
General	34
File Activities	35
File Read	35
Analysis Process: dash PID: 5211 Parent PID: 4331	35
General	35
Analysis Process: tr PID: 5211 Parent PID: 4331	35
General	35
File Activities	35
File Read	35
Analysis Process: dash PID: 5212 Parent PID: 4331	35
General	35
Analysis Process: cut PID: 5212 Parent PID: 4331	35
General	35
File Activities	36
File Read	36

Analysis Process: dash PID: 5213 Parent PID: 4331	36
General	36
Analysis Process: cat PID: 5213 Parent PID: 4331	36
General	36
File Activities	36
File Read	36
Analysis Process: dash PID: 5214 Parent PID: 4331	36
General	36
Analysis Process: head PID: 5214 Parent PID: 4331	36
General	36
File Activities	37
File Read	37
Analysis Process: dash PID: 5215 Parent PID: 4331	37
General	37
Analysis Process: tr PID: 5215 Parent PID: 4331	37
General	37
File Activities	37
File Read	37
Analysis Process: dash PID: 5216 Parent PID: 4331	37
General	37
Analysis Process: cut PID: 5216 Parent PID: 4331	37
General	37
File Activities	37
File Read	38
File Written	38
Analysis Process: dash PID: 5219 Parent PID: 4331	38
General	38
Analysis Process: rm PID: 5219 Parent PID: 4331	38
General	38
File Activities	38
File Deleted	38
File Read	38
Analysis Process: arm7 PID: 5249 Parent PID: 5110	38
General	38
File Activities	38
File Read	38
Analysis Process: arm7 PID: 5251 Parent PID: 5249	38
General	38
Analysis Process: arm7 PID: 5252 Parent PID: 5249	39
General	39
Analysis Process: arm7 PID: 5256 Parent PID: 5252	39
General	39
File Activities	39
File Read	39
Directory Enumerated	39
Analysis Process: arm7 PID: 5258 Parent PID: 5252	39
General	39
Analysis Process: arm7 PID: 5260 Parent PID: 5258	39
General	39
Analysis Process: systemd PID: 5296 Parent PID: 1	40
General	40
Analysis Process: whoopsie PID: 5296 Parent PID: 1	40
General	40
File Activities	40
File Read	40
File Written	40
File Moved	40
Directory Enumerated	40
Directory Created	40
Permission Modified	40
Analysis Process: systemd PID: 5308 Parent PID: 1	40
General	40
Analysis Process: sshd PID: 5308 Parent PID: 1	40
General	40
File Activities	41
File Read	41
Directory Enumerated	41
Analysis Process: systemd PID: 5309 Parent PID: 1	41
General	41
Analysis Process: sshd PID: 5309 Parent PID: 1	41
General	41
File Activities	41
File Read	41
File Written	41
Directory Enumerated	41
Analysis Process: gdm3 PID: 5314 Parent PID: 1320	41
General	41
Analysis Process: Default PID: 5314 Parent PID: 1320	41
General	41
File Activities	42
File Read	42
Analysis Process: gdm3 PID: 5318 Parent PID: 1320	42
General	42
Analysis Process: Default PID: 5318 Parent PID: 1320	42
General	42
File Activities	42
File Read	42
Analysis Process: systemd PID: 5319 Parent PID: 1	42
General	42
Analysis Process: accounts-daemon PID: 5319 Parent PID: 1	42
General	42
File Activities	43
File Read	43
File Written	43
File Moved	43

Directory Enumerated	43
Directory Created	43
Permission Modified	43
Analysis Process: accounts-daemon PID: 5334 Parent PID: 5319	43
General	43
File Activities	43
Directory Enumerated	43
Analysis Process: language-validate PID: 5334 Parent PID: 5319	43
General	43
File Activities	43
File Read	43
Analysis Process: language-validate PID: 5335 Parent PID: 5334	43
General	43
Analysis Process: language-options PID: 5335 Parent PID: 5334	44
General	44
File Activities	44
File Read	44
Directory Enumerated	44
Analysis Process: language-options PID: 5336 Parent PID: 5335	44
General	44
Analysis Process: sh PID: 5336 Parent PID: 5335	44
General	44
File Activities	44
File Read	44
Analysis Process: sh PID: 5337 Parent PID: 5336	44
General	44
Analysis Process: locale PID: 5337 Parent PID: 5336	45
General	45
File Activities	45
File Read	45
Directory Enumerated	45
Analysis Process: sh PID: 5338 Parent PID: 5336	45
General	45
Analysis Process: grep PID: 5338 Parent PID: 5336	45
General	45
File Activities	45
File Read	45
Analysis Process: gdm3 PID: 5339 Parent PID: 1320	45
General	45
Analysis Process: gdm-session-worker PID: 5339 Parent PID: 1320	46
General	46
File Activities	46
File Read	46
File Written	46
Directory Enumerated	46
Analysis Process: gdm-session-worker PID: 5343 Parent PID: 5339	46
General	46
Analysis Process: gdm-wayland-session PID: 5343 Parent PID: 5339	46
General	46
File Activities	46
File Read	46
Analysis Process: gdm-wayland-session PID: 5348 Parent PID: 5343	46
General	46
File Activities	47
Directory Enumerated	47
Analysis Process: dbus-run-session PID: 5348 Parent PID: 5343	47
General	47
File Activities	47
File Read	47
Analysis Process: dbus-run-session PID: 5349 Parent PID: 5348	47
General	47
Analysis Process: dbus-daemon PID: 5349 Parent PID: 5348	47
General	47
File Activities	47
File Read	47
Directory Enumerated	47
Directory Created	47
Analysis Process: dbus-daemon PID: 5353 Parent PID: 5349	48
General	48
Analysis Process: dbus-daemon PID: 5354 Parent PID: 5353	48
General	48
File Activities	48
File Written	48
Analysis Process: false PID: 5354 Parent PID: 5353	48
General	48
File Activities	48
File Read	48
Analysis Process: dbus-daemon PID: 5356 Parent PID: 5349	48
General	48
Analysis Process: dbus-daemon PID: 5357 Parent PID: 5356	48
General	49
File Activities	49
File Written	49
Analysis Process: false PID: 5357 Parent PID: 5356	49
General	49
File Activities	49
File Read	49
Analysis Process: dbus-daemon PID: 5358 Parent PID: 5349	49
General	49
Analysis Process: dbus-daemon PID: 5359 Parent PID: 5358	49
General	49
File Activities	49
File Written	49
Analysis Process: false PID: 5359 Parent PID: 5358	50
General	50

File Activities	50
File Read	50
Analysis Process: dbus-daemon PID: 5360 Parent PID: 5349	50
General	50
Analysis Process: dbus-daemon PID: 5361 Parent PID: 5360	50
General	50
File Activities	50
File Written	50
Analysis Process: false PID: 5361 Parent PID: 5360	50
General	50
File Activities	50
File Read	50
Analysis Process: dbus-daemon PID: 5362 Parent PID: 5349	51
General	51
Analysis Process: dbus-daemon PID: 5363 Parent PID: 5362	51
General	51
File Activities	51
File Written	51
Analysis Process: false PID: 5363 Parent PID: 5362	51
General	51
File Activities	51
File Read	51
Analysis Process: dbus-daemon PID: 5364 Parent PID: 5349	51
General	51
Analysis Process: dbus-daemon PID: 5365 Parent PID: 5364	51
General	52
File Activities	52
File Written	52
Analysis Process: false PID: 5365 Parent PID: 5364	52
General	52
File Activities	52
File Read	52
Analysis Process: dbus-daemon PID: 5367 Parent PID: 5349	52
General	52
Analysis Process: dbus-daemon PID: 5368 Parent PID: 5367	52
General	52
File Activities	52
File Written	52
Analysis Process: false PID: 5368 Parent PID: 5367	53
General	53
File Activities	53
File Read	53
Analysis Process: dbus-run-session PID: 5350 Parent PID: 5348	53
General	53
Analysis Process: gnome-session PID: 5350 Parent PID: 5348	53
General	53
File Activities	53
File Read	53
Analysis Process: gnome-session-binary PID: 5350 Parent PID: 5348	53
General	53
File Activities	53
File Created	53
File Deleted	54
File Read	54
File Written	54
Directory Enumerated	54
Directory Created	54
Link Created	54
Analysis Process: gnome-session-binary PID: 5369 Parent PID: 5350	54
General	54
File Activities	54
Directory Enumerated	54
Analysis Process: session-migration PID: 5369 Parent PID: 5350	54
General	54
File Activities	54
File Read	54
Analysis Process: gnome-session-binary PID: 5370 Parent PID: 5350	54
General	54
File Activities	54
Directory Enumerated	55
Analysis Process: sh PID: 5370 Parent PID: 5350	55
General	55
File Activities	55
File Read	55
Analysis Process: gnome-shell PID: 5370 Parent PID: 5350	55
General	55
File Activities	55
File Read	55
Directory Enumerated	55
Analysis Process: gdm3 PID: 5398 Parent PID: 1320	55
General	55
Analysis Process: gdm-session-worker PID: 5398 Parent PID: 1320	55
General	55
File Activities	56
File Read	56
File Written	56
Directory Enumerated	56
Analysis Process: gdm-session-worker PID: 5405 Parent PID: 5398	56
General	56
Analysis Process: gdm-x-session PID: 5405 Parent PID: 5398	56
General	56
File Activities	56
File Read	56
File Written	56
Directory Created	56
Analysis Process: gdm-x-session PID: 5407 Parent PID: 5405	56

General	56
File Activities	56
Directory Enumerated	56
Analysis Process: Xorg PID: 5407 Parent PID: 5405	57
General	57
File Activities	57
File Read	57
Analysis Process: Xorg.wrap PID: 5407 Parent PID: 5405	57
General	57
File Activities	57
File Read	57
Analysis Process: Xorg PID: 5407 Parent PID: 5405	57
General	57
File Activities	57
File Deleted	57
File Read	57
File Written	57
File Moved	57
Directory Enumerated	57
Analysis Process: Xorg PID: 5443 Parent PID: 5407	57
General	58
Analysis Process: sh PID: 5443 Parent PID: 5407	58
General	58
File Activities	58
File Read	58
Analysis Process: sh PID: 5444 Parent PID: 5443	58
General	58
Analysis Process: xkbcomp PID: 5444 Parent PID: 5443	58
General	58
File Activities	58
File Deleted	58
File Read	58
File Written	58
Analysis Process: Xorg PID: 5866 Parent PID: 5407	59
General	59
Analysis Process: sh PID: 5866 Parent PID: 5407	59
General	59
File Activities	59
File Read	59
Analysis Process: sh PID: 5869 Parent PID: 5866	59
General	59
Analysis Process: xkbcomp PID: 5869 Parent PID: 5866	59
General	59
File Activities	59
File Deleted	59
File Read	59
File Written	59
Analysis Process: gdm-x-session PID: 5452 Parent PID: 5405	60
General	60
File Activities	60
Directory Enumerated	60
Analysis Process: Default PID: 5452 Parent PID: 5405	60
General	60
File Activities	60
File Read	60
Analysis Process: gdm-x-session PID: 5453 Parent PID: 5405	60
General	60
File Activities	60
Directory Enumerated	60
Analysis Process: dbus-run-session PID: 5453 Parent PID: 5405	60
General	60
File Activities	61
File Read	61
Analysis Process: dbus-run-session PID: 5454 Parent PID: 5453	61
General	61
Analysis Process: dbus-daemon PID: 5454 Parent PID: 5453	61
General	61
File Activities	61
File Read	61
Directory Enumerated	61
Directory Created	61
Analysis Process: dbus-daemon PID: 5509 Parent PID: 5454	61
General	61
Analysis Process: dbus-daemon PID: 5510 Parent PID: 5509	61
General	61
File Activities	62
File Written	62
Analysis Process: at-spi-bus-launcher PID: 5510 Parent PID: 5509	62
General	62
File Activities	62
File Read	62
File Written	62
Directory Enumerated	62
Directory Created	62
Analysis Process: at-spi-bus-launcher PID: 5515 Parent PID: 5510	62
General	62
File Activities	62
Directory Enumerated	62
Analysis Process: dbus-daemon PID: 5515 Parent PID: 5510	62
General	62
File Activities	63
File Read	63
Directory Enumerated	63
Analysis Process: dbus-daemon PID: 5931 Parent PID: 5515	63
General	63
Analysis Process: dbus-daemon PID: 5934 Parent PID: 5931	63

General	63
File Activities	63
File Written	63
Analysis Process: at-spi2-registrd PID: 5934 Parent PID: 5931	63
General	63
File Activities	63
File Read	63
Analysis Process: dbus-daemon PID: 5539 Parent PID: 5454	63
General	63
Analysis Process: dbus-daemon PID: 5540 Parent PID: 5539	64
General	64
File Activities	64
File Written	64
Analysis Process: false PID: 5540 Parent PID: 5539	64
General	64
File Activities	64
File Read	64
Analysis Process: dbus-daemon PID: 5542 Parent PID: 5454	64
General	64
Analysis Process: dbus-daemon PID: 5543 Parent PID: 5542	64
General	64
File Activities	65
File Written	65
Analysis Process: false PID: 5543 Parent PID: 5542	65
General	65
File Activities	65
File Read	65
Analysis Process: dbus-daemon PID: 5544 Parent PID: 5454	65
General	65
Analysis Process: dbus-daemon PID: 5545 Parent PID: 5544	65
General	65
File Activities	65
File Written	65
Analysis Process: false PID: 5545 Parent PID: 5544	65
General	65
File Activities	66
File Read	66
Analysis Process: dbus-daemon PID: 5546 Parent PID: 5454	66
General	66
Analysis Process: dbus-daemon PID: 5547 Parent PID: 5546	66
General	66
File Activities	66
File Written	66
Analysis Process: false PID: 5547 Parent PID: 5546	66
General	66
File Activities	66
File Read	66
Analysis Process: dbus-daemon PID: 5548 Parent PID: 5454	66
General	66
Analysis Process: dbus-daemon PID: 5549 Parent PID: 5548	67
General	67
File Activities	67
File Written	67
Analysis Process: false PID: 5549 Parent PID: 5548	67
General	67
File Activities	67
File Read	67
Analysis Process: dbus-daemon PID: 5550 Parent PID: 5454	67
General	67
Analysis Process: dbus-daemon PID: 5551 Parent PID: 5550	67
General	67
File Activities	68
File Written	68
Analysis Process: false PID: 5551 Parent PID: 5550	68
General	68
File Activities	68
File Read	68
Analysis Process: dbus-daemon PID: 5553 Parent PID: 5454	68
General	68
Analysis Process: dbus-daemon PID: 5554 Parent PID: 5553	68
General	68
File Activities	68
File Written	68
Analysis Process: false PID: 5554 Parent PID: 5553	68
General	68
File Activities	69
File Read	69
Analysis Process: dbus-daemon PID: 5861 Parent PID: 5454	69
General	69
Analysis Process: dbus-daemon PID: 5862 Parent PID: 5861	69
General	69
File Activities	69
File Written	69
Analysis Process: ibus-portal PID: 5862 Parent PID: 5861	69
General	69
File Activities	69
File Read	69
Directory Enumerated	69
Directory Created	69
Analysis Process: dbus-daemon PID: 6095 Parent PID: 5454	69
General	70
Analysis Process: dbus-daemon PID: 6096 Parent PID: 6095	70
General	70

File Activities	70
File Written	70
Analysis Process: gjs PID: 6096 Parent PID: 6095	70
General	70
File Activities	70
File Read	70
Directory Enumerated	70
Analysis Process: dbus-daemon PID: 6163 Parent PID: 5454	70
General	70
Analysis Process: dbus-daemon PID: 6165 Parent PID: 6163	70
General	71
File Activities	71
File Written	71
Analysis Process: false PID: 6165 Parent PID: 6163	71
General	71
File Activities	71
File Read	71
Analysis Process: dbus-run-session PID: 5455 Parent PID: 5453	71
General	71
Analysis Process: gnome-session PID: 5455 Parent PID: 5453	71
General	71
File Activities	71
File Read	71
Analysis Process: gnome-session-binary PID: 5455 Parent PID: 5453	72
General	72
File Activities	72
File Created	72
File Deleted	72
File Read	72
File Written	72
Directory Enumerated	72
Directory Created	72
Link Created	72
Analysis Process: gnome-session-binary PID: 5456 Parent PID: 5455	72
General	72
File Activities	72
Directory Enumerated	72
Analysis Process: gnome-session-check-accelerated PID: 5456 Parent PID: 5455	72
General	72
File Activities	72
File Read	72
Directory Enumerated	73
Analysis Process: gnome-session-check-accelerated PID: 5516 Parent PID: 5456	73
General	73
File Activities	73
Directory Enumerated	73
Analysis Process: gnome-session-check-accelerated-gi-helper PID: 5516 Parent PID: 5456	73
General	73
File Activities	73
File Read	73
Directory Enumerated	73
Analysis Process: gnome-session-check-accelerated PID: 5528 Parent PID: 5456	73
General	73
File Activities	73
Directory Enumerated	73
Analysis Process: gnome-session-check-accelerated-gles-helper PID: 5528 Parent PID: 5456	73
General	74
File Activities	74
File Read	74
Directory Enumerated	74
Analysis Process: gnome-session-binary PID: 5555 Parent PID: 5455	74
General	74
File Activities	74
Directory Enumerated	74
Analysis Process: session-migration PID: 5555 Parent PID: 5455	74
General	74
File Activities	74
File Read	74
Analysis Process: gnome-session-binary PID: 5558 Parent PID: 5455	74
General	74
File Activities	75
Directory Enumerated	75
Analysis Process: sh PID: 5558 Parent PID: 5455	75
General	75
File Activities	75
File Read	75
Analysis Process: gnome-shell PID: 5558 Parent PID: 5455	75
General	75
File Activities	75
File Deleted	75
File Read	75
File Written	75
Directory Enumerated	75
Directory Created	75
Analysis Process: gnome-shell PID: 5609 Parent PID: 5558	75
General	75
File Activities	75
Directory Enumerated	76
Analysis Process: ibus-daemon PID: 5609 Parent PID: 5558	76
General	76
File Activities	76
File Deleted	76
File Read	76
File Written	76
Directory Enumerated	76
Directory Created	76
Analysis Process: ibus-daemon PID: 5857 Parent PID: 5609	76
General	76

File Activities	76
Directory Enumerated	76
Analysis Process: ibus-memconf PID: 5857 Parent PID: 5609	76
General	76
File Activities	76
File Read	76
Directory Enumerated	77
Directory Created	77
Analysis Process: ibus-daemon PID: 5859 Parent PID: 5609	77
General	77
Analysis Process: ibus-daemon PID: 5860 Parent PID: 5859	77
General	77
File Activities	77
Directory Enumerated	77
Analysis Process: ibus-x11 PID: 5860 Parent PID: 1	77
General	77
File Activities	77
File Read	77
Directory Enumerated	77
Directory Created	77
Analysis Process: ibus-daemon PID: 6130 Parent PID: 5609	77
General	77
File Activities	78
Directory Enumerated	78
Analysis Process: ibus-engine-simple PID: 6130 Parent PID: 5609	78
General	78
File Activities	78
File Read	78
Directory Enumerated	78
Directory Created	78
Analysis Process: gnome-session-binary PID: 6116 Parent PID: 5455	78
General	78
File Activities	78
Directory Enumerated	78
Analysis Process: sh PID: 6116 Parent PID: 5455	78
General	78
File Activities	78
File Read	79
Analysis Process: gsd-sharing PID: 6116 Parent PID: 5455	79
General	79
File Activities	79
File Read	79
File Written	79
Directory Enumerated	79
Directory Created	79
Analysis Process: gnome-session-binary PID: 6118 Parent PID: 5455	79
General	79
File Activities	79
Directory Enumerated	79
Analysis Process: sh PID: 6118 Parent PID: 5455	79
General	79
File Activities	79
File Read	79
Analysis Process: gsd-wacom PID: 6118 Parent PID: 5455	80
General	80
File Activities	80
File Read	80
Directory Enumerated	80
Analysis Process: gnome-session-binary PID: 6120 Parent PID: 5455	80
General	80
File Activities	80
Directory Enumerated	80
Analysis Process: sh PID: 6120 Parent PID: 5455	80
General	80
File Activities	80
File Read	80
Analysis Process: gsd-color PID: 6120 Parent PID: 5455	80
General	80
File Activities	81
File Read	81
File Written	81
Directory Enumerated	81
Directory Created	81
Analysis Process: gnome-session-binary PID: 6121 Parent PID: 5455	81
General	81
File Activities	81
Directory Enumerated	81
Analysis Process: sh PID: 6121 Parent PID: 5455	81
General	81
File Activities	81
File Read	81
Analysis Process: gsd-keyboard PID: 6121 Parent PID: 5455	81
General	81
File Activities	81
File Read	81
File Written	82
Directory Enumerated	82
Directory Created	82
Analysis Process: gnome-session-binary PID: 6122 Parent PID: 5455	82
General	82
File Activities	82
Directory Enumerated	82
Analysis Process: sh PID: 6122 Parent PID: 5455	82
General	82
File Activities	82
File Read	82
Analysis Process: gsd-print-notifications PID: 6122 Parent PID: 5455	82
General	82

File Activities	82
File Read	82
Analysis Process: gsd-print-notifications PID: 6442 Parent PID: 6122	82
General	83
Analysis Process: gsd-print-notifications PID: 6443 Parent PID: 6442	83
General	83
File Activities	83
Directory Enumerated	83
Analysis Process: gsd-printer PID: 6443 Parent PID: 1	83
General	83
File Activities	83
File Read	83
Analysis Process: gnome-session-binary PID: 6123 Parent PID: 5455	83
General	83
File Activities	83
Directory Enumerated	83
Analysis Process: sh PID: 6123 Parent PID: 5455	84
General	84
File Activities	84
File Read	84
Analysis Process: gsd-rfkill PID: 6123 Parent PID: 5455	84
General	84
File Activities	84
File Read	84
Analysis Process: gnome-session-binary PID: 6124 Parent PID: 5455	84
General	84
File Activities	84
Directory Enumerated	84
Analysis Process: sh PID: 6124 Parent PID: 5455	84
General	84
File Activities	85
File Read	85
Analysis Process: gsd-smartcard PID: 6124 Parent PID: 5455	85
General	85
File Activities	85
File Read	85
File Written	85
Directory Enumerated	85
Directory Created	85
Analysis Process: gnome-session-binary PID: 6128 Parent PID: 5455	85
General	85
File Activities	85
Directory Enumerated	85
Analysis Process: sh PID: 6128 Parent PID: 5455	85
General	85
File Activities	85
File Read	85
Analysis Process: gsd-datetime PID: 6128 Parent PID: 5455	86
General	86
File Activities	86
File Read	86
File Written	86
Directory Enumerated	86
Directory Created	86
Analysis Process: gnome-session-binary PID: 6129 Parent PID: 5455	86
General	86
File Activities	86
Directory Enumerated	86
Analysis Process: sh PID: 6129 Parent PID: 5455	86
General	86
File Activities	86
File Read	86
Analysis Process: gsd-media-keys PID: 6129 Parent PID: 5455	86
General	86
File Activities	87
File Read	87
File Written	87
Directory Enumerated	87
Directory Created	87
Analysis Process: gnome-session-binary PID: 6131 Parent PID: 5455	87
General	87
File Activities	87
Directory Enumerated	87
Analysis Process: sh PID: 6131 Parent PID: 5455	87
General	87
File Activities	87
File Read	87
Analysis Process: gsd-screensaver-proxy PID: 6131 Parent PID: 5455	87
General	87
File Activities	88
File Read	88
Analysis Process: gnome-session-binary PID: 6134 Parent PID: 5455	88
General	88
Analysis Process: sh PID: 6134 Parent PID: 5455	88
General	88
Analysis Process: gsd-sound PID: 6134 Parent PID: 5455	88
General	88
Analysis Process: gnome-session-binary PID: 6137 Parent PID: 5455	88
General	88
Analysis Process: sh PID: 6137 Parent PID: 5455	88
General	88
Analysis Process: gsd-a11y-settings PID: 6137 Parent PID: 5455	89
General	89
Analysis Process: gnome-session-binary PID: 6139 Parent PID: 5455	89
General	89

Analysis Process: sh PID: 6139 Parent PID: 5455	89
General	89
Analysis Process: gsd-housekeeping PID: 6139 Parent PID: 5455	89
General	89
Analysis Process: gnome-session-binary PID: 6144 Parent PID: 5455	89
General	90
Analysis Process: sh PID: 6144 Parent PID: 5455	90
General	90
Analysis Process: gsd-power PID: 6144 Parent PID: 5455	90
General	90
Analysis Process: gnome-session-binary PID: 6995 Parent PID: 5455	90
General	90
Analysis Process: sh PID: 6995 Parent PID: 5455	90
General	90
Analysis Process: spice-vdagent PID: 6995 Parent PID: 5455	91
General	91
Analysis Process: gnome-session-binary PID: 7018 Parent PID: 5455	91
General	91
Analysis Process: sh PID: 7018 Parent PID: 5455	91
General	91
Analysis Process: xbrlapi PID: 7018 Parent PID: 5455	91
General	91
Analysis Process: gdm3 PID: 5399 Parent PID: 1320	91
General	91
Analysis Process: Default PID: 5399 Parent PID: 1320	92
General	92
Analysis Process: gdm3 PID: 5400 Parent PID: 1320	92
General	92
Analysis Process: Default PID: 5400 Parent PID: 1320	92
General	92
Analysis Process: gdm3 PID: 5408 Parent PID: 1320	92
General	92
Analysis Process: Default PID: 5408 Parent PID: 1320	92
General	92
Analysis Process: systemd PID: 5414 Parent PID: 1860	93
General	93
Analysis Process: pulseaudio PID: 5414 Parent PID: 1860	93
General	93
Analysis Process: gvfsd-fuse PID: 5460 Parent PID: 2038	93
General	93
Analysis Process: fusermount PID: 5460 Parent PID: 2038	93
General	93
Analysis Process: systemd PID: 5475 Parent PID: 1	93
General	93
Analysis Process: systemd-user-runtime-dir PID: 5475 Parent PID: 1	94
General	94
Analysis Process: systemd PID: 5583 Parent PID: 1	94
General	94
Analysis Process: systemd-localealed PID: 5583 Parent PID: 1	94
General	94
Analysis Process: systemd PID: 5873 Parent PID: 1334	94
General	94
Analysis Process: pulseaudio PID: 5873 Parent PID: 1334	94
General	94
Analysis Process: systemd PID: 5876 Parent PID: 1	95
General	95
Analysis Process: geoclue PID: 5876 Parent PID: 1	95
General	95
Analysis Process: systemd PID: 6169 Parent PID: 1	95
General	95
Analysis Process: systemd-hostnamed PID: 6169 Parent PID: 1	95
General	95
Analysis Process: systemd PID: 6497 Parent PID: 1	95
General	95
Analysis Process: systemd-localealed PID: 6497 Parent PID: 1	96
General	96
Analysis Process: systemd PID: 6783 Parent PID: 1	96
General	96
Analysis Process: fprintd PID: 6783 Parent PID: 1	96
General	96

Linux Analysis Report arm7

Overview

General Information

Sample Name:	arm7
Analysis ID:	518903
MD5:	18e0a7425fa5b74.
SHA1:	32fb441007353ad.
SHA256:	ac4582bf75332e1.
Tags:	Mirai
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

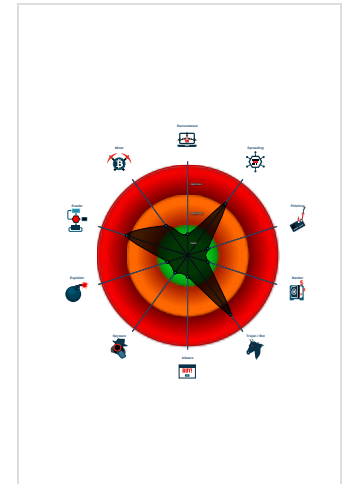
Mirai

Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e...
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample tries to kill many processes...
- Reads system files that contain reco...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample reads /proc/mounts (often u...
- Sample contains only a LOAD segm...
- Reads CPU information from /sys in...
- Yara signature match
- Executes the "grep" command read

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	518903
Start date:	10.11.2021
Start time:	04:19:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arm7
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal84.spre.troj.evad.lin@0/52@3/0
Warnings:	Show All

Process Tree

- system is Inxubuntu20
- dash New Fork (PID: 5209, Parent: 4331)
- cat (PID: 5209, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.F8yqW15XWY
- dash New Fork (PID: 5210, Parent: 4331)
- head (PID: 5210, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5211, Parent: 4331)
- tr (PID: 5211, Parent: 4331, MD5: fbd1402dd9f72d8ebff00ce7c3a7bb5) Arguments: tr -d \000-\011\013\014\016-\037
- dash New Fork (PID: 5212, Parent: 4331)
- cut (PID: 5212, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80

- **dash** New Fork (PID: 5213, Parent: 4331)
- **cat** (PID: 5213, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.F8yqW15XWY
- **dash** New Fork (PID: 5214, Parent: 4331)
- **head** (PID: 5214, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- **dash** New Fork (PID: 5215, Parent: 4331)
- **tr** (PID: 5215, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d '\000\011\013\014\016\037'
- **dash** New Fork (PID: 5216, Parent: 4331)
- **cut** (PID: 5216, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- **dash** New Fork (PID: 5219, Parent: 4331)
- **rm** (PID: 5219, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.F8yqW15XWY /tmp/tmp.FsztahAst /tmp/tmp.rbFTGPyqD
- **arm7** (PID: 5249, Parent: 5110, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm7
 - **arm7** New Fork (PID: 5251, Parent: 5249)
 - **arm7** New Fork (PID: 5252, Parent: 5249)
 - **arm7** New Fork (PID: 5256, Parent: 5252)
 - **arm7** New Fork (PID: 5258, Parent: 5252)
 - **arm7** New Fork (PID: 5260, Parent: 5258)
- **systemd** New Fork (PID: 5296, Parent: 1)
- **whoopsie** (PID: 5296, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- **systemd** New Fork (PID: 5308, Parent: 1)
- **sshd** (PID: 5308, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- **systemd** New Fork (PID: 5309, Parent: 1)
- **sshd** (PID: 5309, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **gdm3** New Fork (PID: 5314, Parent: 1320)
- **Default** (PID: 5314, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- **gdm3** New Fork (PID: 5318, Parent: 1320)
- **Default** (PID: 5318, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- **systemd** New Fork (PID: 5319, Parent: 1)
- **accounts-daemon** (PID: 5319, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accounts-service/accounts-daemon
- **accounts-daemon** New Fork (PID: 5334, Parent: 5319)
 - **language-validate** (PID: 5334, Parent: 5319, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
 - **language-validate** New Fork (PID: 5335, Parent: 5334)
 - **language-options** (PID: 5335, Parent: 5334, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
 - **language-options** New Fork (PID: 5336, Parent: 5335)
 - **sh** (PID: 5336, Parent: 5335, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
 - **sh** New Fork (PID: 5337, Parent: 5336)
 - **locale** (PID: 5337, Parent: 5336, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
 - **sh** New Fork (PID: 5338, Parent: 5336)
 - **grep** (PID: 5338, Parent: 5336, MD5: 1e6ebb9dd094f774478f72727dbda0f5) Arguments: grep -F .utf8
- **gdm3** New Fork (PID: 5339, Parent: 1320)
- **gdm-session-worker** (PID: 5339, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
 - **gdm-session-worker** New Fork (PID: 5343, Parent: 5339)
 - **gdm-wayland-session** (PID: 5343, Parent: 5339, MD5: d3def63cf1e837fb8a0f13b1744ff7c) Arguments: /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
 - **gdm-wayland-session** New Fork (PID: 5348, Parent: 5343)
 - **dbus-run-session** (PID: 5348, Parent: 5343, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
 - **dbus-run-session** New Fork (PID: 5349, Parent: 5348)
 - **dbus-daemon** (PID: 5349, Parent: 5348, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
 - **dbus-daemon** New Fork (PID: 5353, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5354, Parent: 5353)
 - **false** (PID: 5354, Parent: 5353, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-daemon** New Fork (PID: 5356, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5357, Parent: 5356)
 - **false** (PID: 5357, Parent: 5356, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-daemon** New Fork (PID: 5358, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5359, Parent: 5358)
 - **false** (PID: 5359, Parent: 5358, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-daemon** New Fork (PID: 5360, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5361, Parent: 5360)
 - **false** (PID: 5361, Parent: 5360, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-daemon** New Fork (PID: 5362, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5363, Parent: 5362)
 - **false** (PID: 5363, Parent: 5362, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-daemon** New Fork (PID: 5364, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5365, Parent: 5364)
 - **false** (PID: 5365, Parent: 5364, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-daemon** New Fork (PID: 5367, Parent: 5349)
 - **dbus-daemon** New Fork (PID: 5368, Parent: 5367)
 - **false** (PID: 5368, Parent: 5367, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **dbus-run-session** New Fork (PID: 5350, Parent: 5348)
 - **gnome-session** (PID: 5350, Parent: 5348, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
 - **gnome-session-binary** (PID: 5350, Parent: 5348, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
 - **gnome-session-binary** New Fork (PID: 5369, Parent: 5350)
 - **session-migration** (PID: 5369, Parent: 5350, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
 - **gnome-session-binary** New Fork (PID: 5370, Parent: 5350)
 - **sh** (PID: 5370, Parent: 5350, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/bin/gnome-shell
 - **gnome-shell** (PID: 5370, Parent: 5350, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
 - **gdm3** New Fork (PID: 5398, Parent: 1320)
 - **gdm-session-worker** (PID: 5398, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
 - **gdm-session-worker** New Fork (PID: 5405, Parent: 5398)
 - **gdm-x-session** (PID: 5405, Parent: 5398, MD5: 498a824333f1c1ec7767f4612d1887cc) Arguments: /usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
 - **gdm-x-session** New Fork (PID: 5407, Parent: 5405)
 - **Xorg** (PID: 5407, Parent: 5405, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeppty -verbose 3
 - **Xorg.wrap** (PID: 5407, Parent: 5405, MD5: 48993830888200cef19d7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeppty -verbose 3
 - **Xorg** (PID: 5407, Parent: 5405, MD5: 730cf4c45a7ee8bea8abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none

```

-noreset -keeptry -verbose 3
• Xorg New Fork (PID: 5443, Parent: 5407)
• sh (PID: 5443, Parent: 5407, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\/usr/bin/xkbcomp" -w 1 "\-R/usr/share/X11/xkb" -xkm "\-" -em1 "\The XKEYBOARD keymap compiler (xkbcomp) reports:\\" -emp "\>" -eml "\Errors from xkbcomp are not fatal to the X server" "\/tmp/server-0.xkm"
  • sh New Fork (PID: 5444, Parent: 5443)
  • xkbcomp (PID: 5444, Parent: 5443, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp ">" -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
• Xorg New Fork (PID: 5866, Parent: 5407)
• sh (PID: 5866, Parent: 5407, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\/usr/bin/xkbcomp" -w 1 "\-R/usr/share/X11/xkb" -xkm "\-" -em1 "\The XKEYBOARD keymap compiler (xkbcomp) reports:\\" -emp "\>" -eml "\Errors from xkbcomp are not fatal to the X server" "\/tmp/server-0.xkm"
  • sh New Fork (PID: 5869, Parent: 5866)
  • xkbcomp (PID: 5869, Parent: 5866, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp ">" -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
• gdm-x-session New Fork (PID: 5452, Parent: 5405)
• Default (PID: 5452, Parent: 5405, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
• gdm-x-session New Fork (PID: 5453, Parent: 5405)
• dbus-run-session (PID: 5453, Parent: 5405, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
  • dbus-run-session New Fork (PID: 5454, Parent: 5453)
  • dbus-daemon (PID: 5454, Parent: 5453, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
    • dbus-daemon New Fork (PID: 5509, Parent: 5454)
    • dbus-daemon New Fork (PID: 5510, Parent: 5509)
    • at-spi-bus-launcher (PID: 5510, Parent: 5509, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
      • at-spi-bus-launcher New Fork (PID: 5515, Parent: 5510)
      • dbus-daemon (PID: 5515, Parent: 5510, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
        • dbus-daemon New Fork (PID: 5931, Parent: 5515)
        • dbus-daemon New Fork (PID: 5934, Parent: 5931)
        • at-spi2-registrtyd (PID: 5934, Parent: 5931, MD5: 1d904c2693452ede3c7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registrtyd --use-gnome-session
    • dbus-daemon New Fork (PID: 5539, Parent: 5454)
      • dbus-daemon New Fork (PID: 5540, Parent: 5539)
      • false (PID: 5540, Parent: 5539, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5542, Parent: 5454)
      • dbus-daemon New Fork (PID: 5543, Parent: 5542)
      • false (PID: 5543, Parent: 5542, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5544, Parent: 5454)
      • dbus-daemon New Fork (PID: 5545, Parent: 5544)
      • false (PID: 5545, Parent: 5544, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5546, Parent: 5454)
      • dbus-daemon New Fork (PID: 5547, Parent: 5546)
      • false (PID: 5547, Parent: 5546, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5548, Parent: 5454)
      • dbus-daemon New Fork (PID: 5549, Parent: 5548)
      • false (PID: 5549, Parent: 5548, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5550, Parent: 5454)
      • dbus-daemon New Fork (PID: 5551, Parent: 5550)
      • false (PID: 5551, Parent: 5550, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5553, Parent: 5454)
      • dbus-daemon New Fork (PID: 5554, Parent: 5553)
      • false (PID: 5554, Parent: 5553, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    • dbus-daemon New Fork (PID: 5861, Parent: 5454)
      • dbus-daemon New Fork (PID: 5862, Parent: 5861)
      • ibus-portal (PID: 5862, Parent: 5861, MD5: 562ad55bd9a4d54bd7b76746b01e37d3d) Arguments: /usr/libexec/ibus-portal
    • dbus-daemon New Fork (PID: 6095, Parent: 5454)
      • dbus-daemon New Fork (PID: 6096, Parent: 6095)
      • gjs (PID: 6096, Parent: 6095, MD5: 5f3e3eb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
    • dbus-daemon New Fork (PID: 6163, Parent: 5454)
      • dbus-daemon New Fork (PID: 6165, Parent: 6163)
      • false (PID: 6165, Parent: 6163, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
• dbus-run-session New Fork (PID: 5455, Parent: 5453)
• gnome-session (PID: 5455, Parent: 5453, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
• gnome-session-binary (PID: 5455, Parent: 5453, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
  • gnome-session-binary New Fork (PID: 5456, Parent: 5455)
  • gnome-session-check-accelerated (PID: 5456, Parent: 5455, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
    • gnome-session-check-accelerated New Fork (PID: 5516, Parent: 5456)
    • gnome-session-check-accelerated-gl-helper (PID: 5516, Parent: 5456, MD5: b1ab9a384f9e98a39ae5c3603dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
    • gnome-session-check-accelerated New Fork (PID: 5528, Parent: 5456)
    • gnome-session-check-accelerated-gles-helper (PID: 5528, Parent: 5456, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
  • gnome-session-binary New Fork (PID: 5555, Parent: 5455)
  • session-migration (PID: 5555, Parent: 5455, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
  • gnome-session-binary New Fork (PID: 5558, Parent: 5455)
  • sh (PID: 5558, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec "\$@" sh /usr/bin/gnome-shell
  • gnome-shell (PID: 5558, Parent: 5455, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
    • gnome-shell New Fork (PID: 5609, Parent: 5558)
    • ibus-daemon (PID: 5609, Parent: 5558, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
      • ibus-daemon New Fork (PID: 5857, Parent: 5609)
      • ibus-memconf (PID: 5857, Parent: 5609, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
      • ibus-daemon New Fork (PID: 5859, Parent: 5609)
        • ibus-daemon New Fork (PID: 5860, Parent: 5859)
        • ibus-x11 (PID: 5860, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
      • ibus-daemon New Fork (PID: 6130, Parent: 5609)
      • ibus-engine-simple (PID: 6130, Parent: 5609, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
    • gnome-session-binary New Fork (PID: 6116, Parent: 5455)
    • sh (PID: 6116, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec "\$@" sh /usr/libexec/gsd-sharing
    • gsd-sharing (PID: 6116, Parent: 5455, MD5: e29d9025d98590fb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing

```


- [gnome-session-binary](#) New Fork (PID: 6118, Parent: 5455)
- [sh](#) (PID: 6118, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-wacom
- [gsd-wacom](#) (PID: 6118, Parent: 5455, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- [gnome-session-binary](#) New Fork (PID: 6120, Parent: 5455)
- [sh](#) (PID: 6120, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-color
- [gsd-color](#) (PID: 6120, Parent: 5455, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- [gnome-session-binary](#) New Fork (PID: 6121, Parent: 5455)
- [sh](#) (PID: 6121, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-keyboard
- [gsd-keyboard](#) (PID: 6121, Parent: 5455, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- [gnome-session-binary](#) New Fork (PID: 6122, Parent: 5455)
- [sh](#) (PID: 6122, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-print-notifications
- [gsd-print-notifications](#) (PID: 6122, Parent: 5455, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
 - [gsd-print-notifications](#) New Fork (PID: 6442, Parent: 6122)
 - [gsd-print-notifications](#) New Fork (PID: 6443, Parent: 6442)
 - [gsd-printer](#) (PID: 6443, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- [gnome-session-binary](#) New Fork (PID: 6123, Parent: 5455)
- [sh](#) (PID: 6123, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-rfkill
- [gsd-rfkill](#) (PID: 6123, Parent: 5455, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- [gnome-session-binary](#) New Fork (PID: 6124, Parent: 5455)
- [sh](#) (PID: 6124, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-smartcard
- [gsd-smartcard](#) (PID: 6124, Parent: 5455, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- [gnome-session-binary](#) New Fork (PID: 6128, Parent: 5455)
- [sh](#) (PID: 6128, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-datetime
- [gsd-datetime](#) (PID: 6128, Parent: 5455, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- [gnome-session-binary](#) New Fork (PID: 6129, Parent: 5455)
- [sh](#) (PID: 6129, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-media-keys
- [gsd-media-keys](#) (PID: 6129, Parent: 5455, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- [gnome-session-binary](#) New Fork (PID: 6131, Parent: 5455)
- [sh](#) (PID: 6131, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-screensaver-proxy
- [gsd-screensaver-proxy](#) (PID: 6131, Parent: 5455, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- [gnome-session-binary](#) New Fork (PID: 6134, Parent: 5455)
- [sh](#) (PID: 6134, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-sound
- [gsd-sound](#) (PID: 6134, Parent: 5455, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- [gnome-session-binary](#) New Fork (PID: 6137, Parent: 5455)
- [sh](#) (PID: 6137, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-a11y-settings
- [gsd-a11y-settings](#) (PID: 6137, Parent: 5455, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- [gnome-session-binary](#) New Fork (PID: 6139, Parent: 5455)
- [sh](#) (PID: 6139, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-housekeeping
- [gsd-housekeeping](#) (PID: 6139, Parent: 5455, MD5: b55f3394a84976db92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- [gnome-session-binary](#) New Fork (PID: 6144, Parent: 5455)
- [sh](#) (PID: 6144, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-power
- [gsd-power](#) (PID: 6144, Parent: 5455, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- [gnome-session-binary](#) New Fork (PID: 6995, Parent: 5455)
- [sh](#) (PID: 6995, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/bin/spice-vdagent
- [spice-vdagent](#) (PID: 6995, Parent: 5455, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- [gnome-session-binary](#) New Fork (PID: 7018, Parent: 5455)
- [sh](#) (PID: 7018, Parent: 5455, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh xbrlapi -q
- [xbrlapi](#) (PID: 7018, Parent: 5455, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q
- [gdm3](#) New Fork (PID: 5399, Parent: 1320)
- [Default](#) (PID: 5399, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- [gdm3](#) New Fork (PID: 5400, Parent: 1320)
- [Default](#) (PID: 5400, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- [gdm3](#) New Fork (PID: 5408, Parent: 1320)
- [Default](#) (PID: 5408, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- [systemd](#) New Fork (PID: 5414, Parent: 1860)
- [pulseaudio](#) (PID: 5414, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- [gvfsd-fuse](#) New Fork (PID: 5460, Parent: 2038)
- [fusermount](#) (PID: 5460, Parent: 2038, MD5: 576a1b135c82bdc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- [systemd](#) New Fork (PID: 5475, Parent: 1)
- [systemd-user-runtime-dir](#) (PID: 5475, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- [systemd](#) New Fork (PID: 5583, Parent: 1)
- [systemd-locale](#) (PID: 5583, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-locale
- [systemd](#) New Fork (PID: 5873, Parent: 1334)
- [pulseaudio](#) (PID: 5873, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- [systemd](#) New Fork (PID: 5876, Parent: 1)
- [geoclue](#) (PID: 5876, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- [systemd](#) New Fork (PID: 6169, Parent: 1)
- [systemd-hostnamed](#) (PID: 6169, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- [systemd](#) New Fork (PID: 6497, Parent: 1)
- [systemd-locale](#) (PID: 6497, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-locale
- [systemd](#) New Fork (PID: 6783, Parent: 1)
- [fprintd](#) (PID: 6783, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- [cleanup](#)

Yara Overview

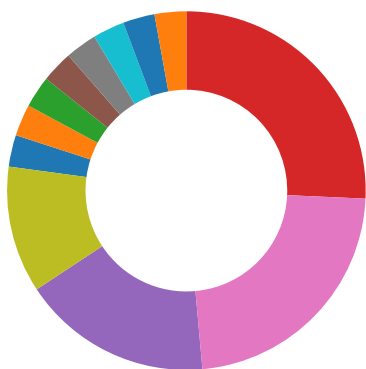
Initial Sample

| Source | Rule | Description | Author | Strings |
|--------|---------------------------------|------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| arm7 | SUSP_ELF_LNX_UPX_Compresed_File | Detects a suspicious ELF binary with UPX compression | Florian Roth | <ul style="list-style-type: none"> 0xafcc:\$s1: PROT_EXEC PROT_WRITE failed. 0xb03b:\$s2: \$!d: UPX 0xafec:\$s3: \$!info: This file is packed with the UPX executable packer |

PCAP (Network Traffic)

| Source | Rule | Description | Author | Strings |
|-----------|----------------------|---------------------|--------------|---------|
| dump.pcap | JoeSecurity_Mirai_12 | Yara detected Mirai | Joe Security | |

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

System Summary:



Sample tries to kill many processes (SIGKILL)

Data Obfuscation:



Sample is packed with UPX

Persistence and Installation Behavior:



Sample reads /proc/mounts (often used for finding a writable filesystem)

Hooking and other Techniques for Hiding and Protection:



Uses known network protocols on non-standard ports

Language, Device and Operating System Detection:



Reads system files that contain records of logged in users

Stealing of Sensitive Information:



Yara detected Mirai

Remote Access Functionality:



Yara detected Mirai

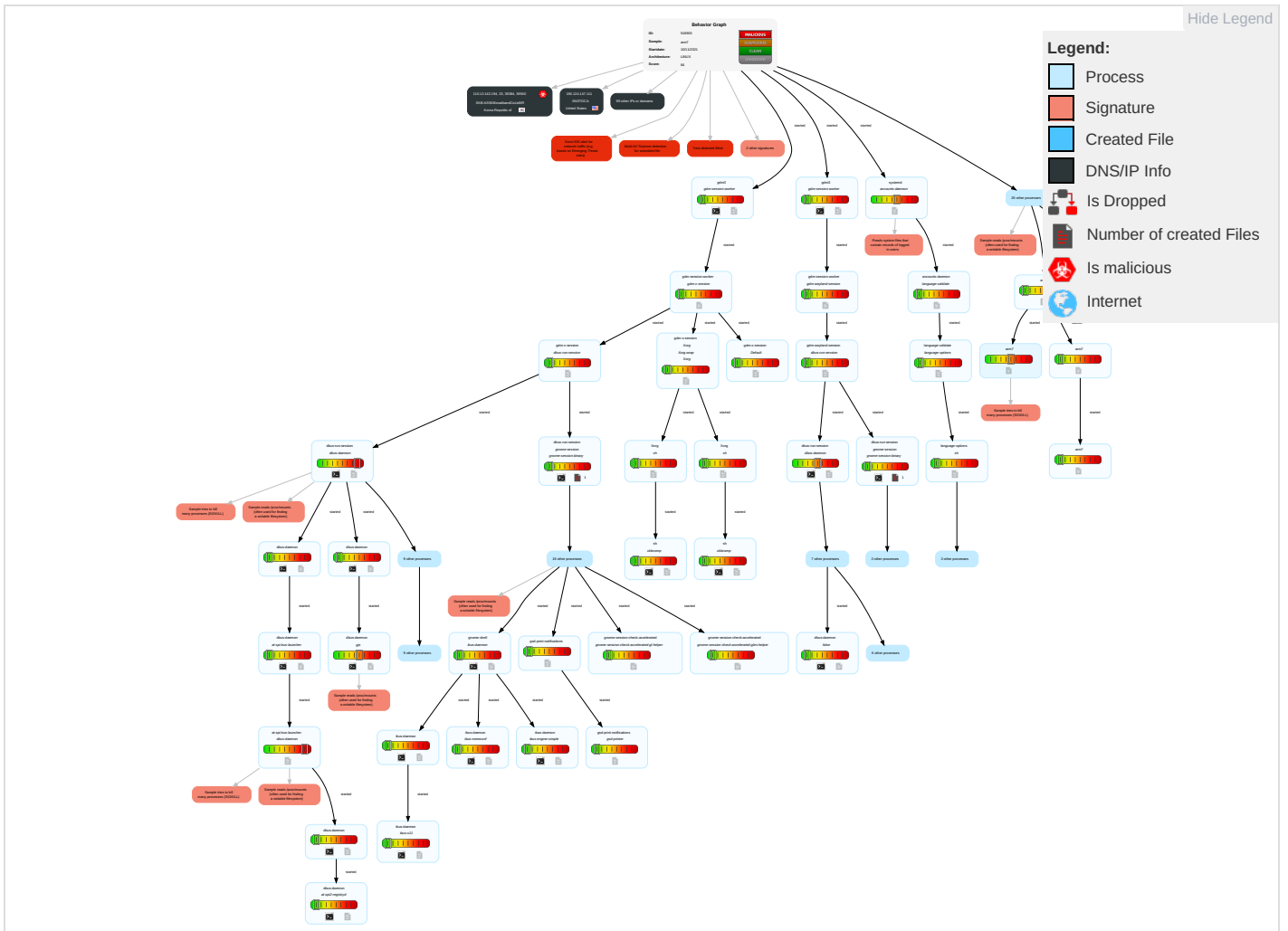
Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects |
|-------------------------------------|------------------------|--------------------------------------|--------------------------------------|----------------------------------------------------------|------------------------------------|-------------------------------------------------------|------------------------------------|--------------------------------|----------------------------------------|---------------------------------------------|---------------------------------------------|---------------------------------------------|
| Valid Accounts | Scripting ¹ | Path Interception | Path Interception | File and Directory Permissions Modification ¹ | OS Credential Dumping ¹ | Security Software Discovery ¹ ¹ | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel ¹ | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Scripting ¹ | LSASS Memory | System Owner/User Discovery ¹ | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Standard Port ¹ ¹ | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Hidden Files and Directories ¹ | Security Account Manager | File and Directory Discovery ¹ | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol ¹ | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information ¹ | NTDS | System Information Discovery ¹ | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol ² | SIM Card Swap | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Indicator Removal on Host ¹ | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | File Deletion ¹ | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | |

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

| Source | Detection | Scanner | Label | Link |
|--------|-----------|---------------|--------------------|------|
| arm7 | 16% | ReversingLabs | Linux.Trojan.Mirai | |

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs







































Contacted Domains













































| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|------------------|----------------|--------|-----------|---------------------|------------|
| daisy.ubuntu.com | 162.213.33.132 | true | false | | high |

















URLs from Memory and Binaries

Contacted IPs

Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|-----------------|---------|---------------------------------|-------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------|-----------|
| 170.212.145.26 | unknown | United States |  | 46274 | UPHSUS | false |
| 105.65.190.125 | unknown | Morocco |  | 36884 | MAROCCONNECTMA | false |
| 188.246.20.171 | unknown | Germany |  | 15987 | PORTUNITY-ASDE | false |
| 180.120.16.34 | unknown | China |  | 137702 | CHINATELECOM-
JIANGSU-NANJING-
IDCNanjingJiangsuProvince | false |
| 209.195.10.55 | unknown | United States |  | 6597 | CBDC-6597US | false |
| 76.113.207.15 | unknown | United States |  | 7922 | COMCAST-7922US | false |
| 175.12.182.161 | unknown | China |  | 4134 | CHINANET-
BACKBONENo31Jin-
rongStreetCN | false |
| 128.12.205.42 | unknown | United States |  | 32 | STANFORDUS | false |
| 153.144.103.33 | unknown | Japan |  | 4713 | OCNNTTCommunicationsCo
rporationJP | false |
| 20.180.146.143 | unknown | United States |  | 8075 | MICROSOFT-CORP-MSN-
AS-BLOCKUS | false |
| 95.195.139.139 | unknown | Sweden |  | 3301 | TELIANET-
SWEDENTeliaCompanySE | false |
| 190.18.242.84 | unknown | Argentina |  | 10318 | TelecomArgentinaSAAR | false |
| 109.48.20.63 | unknown | Portugal |  | 2860 | NOS_COMUNICAOESPT | false |
| 98.21.254.198 | unknown | United States |  | 7029 | WINDSTREAMUS | false |
| 79.185.87.133 | unknown | Poland |  | 5617 | TPNETPL | false |
| 156.73.219.193 | unknown | United States |  | 2024 | NUUS | false |
| 103.153.197.182 | unknown | unknown |  | 134687 | TWIDC-AS-
APTWIDCLimitedHK | false |
| 211.100.37.85 | unknown | China |  | 23724 | CHINANET-IDC-BJ-
APIDCChinaTelecommunica
tionsCorporation | false |
| 114.38.29.71 | unknown | Taiwan; Republic of China (ROC) |  | 3462 | HINETDataCommunicationB
usinessGroupTW | false |
| 119.13.248.48 | unknown | Australia |  | 9723 | ISEEK-AS-
APiseekCommunicationsPty
LtdAU | false |
| 59.89.206.225 | unknown | India |  | 9829 | BSNL-
NIBNationalInternetBackbon
eIN | false |
| 16.233.48.150 | unknown | United States |  | unknown | unknown | false |
| 86.61.47.5 | unknown | Slovenia |  | 5603 | SIOL-
NETTelekomSlovenijeddSI | false |
| 172.76.159.4 | unknown | United States |  | 5650 | FRONTIER-FRTRUS | false |
| 82.139.21.125 | unknown | Poland |  | 29314 | VECTRANET-
ASAIZwyciestwa25381-
525GdyniaPolandPL | false |
| 83.126.63.20 | unknown | European Union |  | 44307 | MDSOLDE | false |
| 223.197.123.195 | unknown | Hong Kong |  | 132585 | SIA-HK-
ASSkyExchangeInternetAcc
essHK | false |
| 59.75.11.76 | unknown | China |  | 4538 | ERX-CERNET-
BKChinaEducationandRes
earchNetworkCenter | false |
| 128.150.78.4 | unknown | United States |  | 102 | NSF-HQ-ASUS | false |
| 111.188.156.126 | unknown | Japan |  | 37903 | EMOBILEYmobileCorporatio
nJP | false |
| 168.114.199.237 | unknown | United States |  | 36026 | AS-CHI-CORPUS | false |
| 85.22.119.239 | unknown | Germany |  | 15763 | ASDOKOMDE | false |
| 213.25.144.224 | unknown | Poland |  | 5617 | TPNETPL | false |
| 139.245.51.216 | unknown | United States |  | 37963 | CNNIC-ALIBABA-CN-NET-
APHangzhouAlibabaAdvertis
ingCoLtd | false |
| 85.91.248.195 | unknown | United Kingdom |  | 34270 | INETCInternetConnectionsLt
dGB | false |
| 106.97.90.23 | unknown | Korea Republic of |  | 17853 | LGTELECOM-AS-
KRLGTELECOMKR | false |
| 134.111.224.1 | unknown | United States |  | 394990 | STRATUS | false |
| 4.199.89.71 | unknown | United States |  | 3356 | LEVEL3US | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|-----------------|---------|--------------------|-------------------------------------------------------------------------------------|--------|--------------------------------------------------------|-----------|
| 145.83.49.160 | unknown | Netherlands |  | 1103 | SURFNET-NLSURFnetTheNetherlandsNL | false |
| 107.59.27.67 | unknown | United States |  | 16567 | NETRIX-16567US | false |
| 47.183.28.100 | unknown | United States |  | 5650 | FRONTIER-FRTRUS | false |
| 9.155.176.99 | unknown | United States |  | 3356 | LEVEL3US | false |
| 155.251.195.38 | unknown | Gambia |  | 37309 | QCellGM | false |
| 172.116.139.149 | unknown | United States |  | 20001 | TWC-20001-PACWESTUS | false |
| 204.43.48.115 | unknown | United States |  | 62600 | ABOR-SUN-CORRIDORUS | false |
| 39.188.163.203 | unknown | China |  | 56041 | CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC | false |
| 63.255.73.32 | unknown | United States |  | 7029 | WINDSTREAMUS | false |
| 76.4.235.154 | unknown | United States |  | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 129.49.188.202 | unknown | United States |  | 5719 | SUNYSBUS | false |
| 156.124.147.111 | unknown | United States |  | 393504 | XNSTGCA | false |
| 183.1.94.120 | unknown | China |  | 4134 | CHINANET-BACKBONENo31JinrongStreetCN | false |
| 130.107.97.233 | unknown | United States |  | 30 | SRI-AICNETUS | false |
| 190.10.105.36 | unknown | Costa Rica |  | 11830 | InstitutoCostarricensedeElectricidadTelecomCR | false |
| 141.249.35.45 | unknown | Switzerland |  | 559 | SWITCHPeeringrequestspeeringswitchEU | false |
| 191.27.216.180 | unknown | Brazil |  | 26599 | TELEFONICABRASILSABR | false |
| 173.45.88.166 | unknown | United States |  | 10297 | ENET-2US | false |
| 95.29.14.199 | unknown | Russian Federation |  | 8402 | CORBINA-ASOJSCVimpelcomRU | false |
| 141.194.211.199 | unknown | France |  | 3215 | FranceTelecom-OrangeFR | false |
| 80.154.177.192 | unknown | Germany |  | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 169.74.17.62 | unknown | United States |  | 37611 | AfrihostZA | false |
| 173.213.255.221 | unknown | United States |  | 6130 | AIS-WESTUS | false |
| 37.220.16.93 | unknown | United Kingdom |  | 20860 | IOMART-ASGB | false |
| 110.229.133.172 | unknown | China |  | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 73.36.184.226 | unknown | United States |  | 7922 | COMCAST-7922US | false |
| 187.226.12.43 | unknown | Mexico |  | 8151 | UninetSAdeCVMX | false |
| 223.24.215.96 | unknown | Thailand |  | 7470 | TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH | false |
| 195.189.97.168 | unknown | Lithuania |  | 59642 | CHERRYSERVERS2-ASLT | false |
| 169.106.1.81 | unknown | United States |  | 37611 | AfrihostZA | false |
| 90.141.14.164 | unknown | Sweden |  | 2119 | TELENOR-NEXTELTeleNorNorgeASNO | false |
| 212.198.158.88 | unknown | France |  | 21502 | ASN-NUMERICABLEFR | false |
| 182.127.195.29 | unknown | China |  | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 62.137.142.218 | unknown | United Kingdom |  | 12337 | NORIS-NETWORKITServiceProvidelocatedinNuernbergGerm | false |
| 219.158.227.86 | unknown | China |  | 4808 | CHINA169-BJChinaUnicomBeijingProvinceNetworkCN | false |
| 187.183.39.5 | unknown | Brazil |  | 28573 | CLAROSABR | false |
| 147.12.222.5 | unknown | United Kingdom |  | 201838 | ASN-COMMUNITYFIBREGB | false |
| 164.71.189.136 | unknown | Japan |  | 2510 | INFOWEBFUJITSULIMITEDJP | false |
| 79.246.126.247 | unknown | Germany |  | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 189.207.91.14 | unknown | Mexico |  | 6503 | AxtelSABdeCVMX | false |
| 86.184.165.197 | unknown | United Kingdom |  | 2856 | BT-UK-ASBTnetUKRegionalnetworkGB | false |
| 199.117.111.48 | unknown | United States |  | 26819 | TOIBGP1US | false |
| 121.15.186.182 | unknown | China |  | 58466 | CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN | false |
| 99.179.58.217 | unknown | United States |  | 7018 | ATT-INTERNET4US | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|-----------------|---------|----------------------|-----------------------------------------------------------------------------------|-------|---------------------------------------|-----------|
| 170.249.28.54 | unknown | United States |  | 46208 | PFNL-ASNUS | false |
| 110.12.142.194 | unknown | Korea Republic of |  | 9318 | SKB-ASSKBroadbandCoLtdKR | true |
| 46.12.7.13 | unknown | Greece |  | 1241 | FORTHNET-GRForthnetEU | false |
| 204.134.225.188 | unknown | United States |  | 17380 | PROJ-MUT-TELUS | false |
| 72.106.171.198 | unknown | United States |  | 22394 | CELLCOUS | false |
| 201.116.34.142 | unknown | Mexico |  | 8151 | UninetSAdeCVMX | false |
| 94.252.222.15 | unknown | Syrian Arab Republic |  | 29256 | INT-PDN-STE-ASSTEPDNInternalASSY | false |
| 161.13.166.242 | unknown | United States |  | 14351 | SOUTHWESTERN-EDUUS | false |
| 98.244.162.230 | unknown | United States |  | 7922 | COMCAST-7922US | false |
| 89.47.85.218 | unknown | Syrian Arab Republic |  | 29256 | INT-PDN-STE-ASSTEPDNInternalASSY | false |
| 218.87.200.152 | unknown | China |  | 4134 | CHINANET-BACKBONeNo31Jin-rongStreetCN | false |
| 97.208.169.168 | unknown | United States |  | 6167 | CELLCO-PARTUS | false |
| 84.239.60.225 | unknown | Romania |  | 5541 | ADNET-TELECOMRO | false |
| 116.226.86.236 | unknown | China |  | 4812 | CHINANET-SH-APChinaTelecomGroupCN | false |
| 178.252.201.48 | unknown | Russian Federation |  | 24689 | ROSINTEL-ASRU | false |
| 183.34.226.62 | unknown | China |  | 4134 | CHINANET-BACKBONeNo31Jin-rongStreetCN | false |
| 32.20.49.106 | unknown | United States |  | 2686 | ATGS-MMD-ASUS | false |
| 62.248.99.166 | unknown | Turkey |  | 9121 | TTNETTR | false |

Joe Sandbox View / Context

IPs

No context

Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|------------------|------------------------------|--------------------------|------------------------|------------------------|------------------|
| daisy.ubuntu.com | x86 | Get hash | malicious | Browse | • 162.213.33.132 |
| | arm | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.132 |
| | Filecoder.Hive_linux.bin | Get hash | malicious | Browse | • 162.213.33.108 |
| | yFbmGHoONE | Get hash | malicious | Browse | • 162.213.33.108 |
| | zju8TB277I | Get hash | malicious | Browse | • 162.213.33.108 |
| | JYWlIP5wHP | Get hash | malicious | Browse | • 162.213.33.108 |
| | uwgXkY20gB | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.132 |
| | FWsCarsq8Q | Get hash | malicious | Browse | • 162.213.33.108 |
| | x86 | Get hash | malicious | Browse | • 162.213.33.108 |
| | arm7 | Get hash | malicious | Browse | • 162.213.33.132 |
| | arm | Get hash | malicious | Browse | • 162.213.33.132 |
| | 7qvn4qlmi3 | Get hash | malicious | Browse | • 162.213.33.132 |
| JuofJwjQMT | Get hash | malicious | Browse | • 162.213.33.108 | |
| GRPVtMlbK5 | Get hash | malicious | Browse | • 162.213.33.108 | |

ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|----------------|------------------------------|--------------------------|-----------|------------------------|------------------|
| MAROCCONNECTMA | SQFoFeC1jQ | Get hash | malicious | Browse | • 197.145.41.202 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context | |
|------------|------------------------------|--------------------------|--------------------------|------------------------|------------------------|--------------------|
| | NEaRhAVeo9 | Get hash | malicious | Browse | • 197.144.26.138 | |
| | Hilix.arm7 | Get hash | malicious | Browse | • 197.144.11.5.203 | |
| | x86 | Get hash | malicious | Browse | • 105.71.60.181 | |
| | x86_64 | Get hash | malicious | Browse | • 105.64.212.1 | |
| | U1WRbn3wOa | Get hash | malicious | Browse | • 197.144.11.5.243 | |
| | b3astmode.x86 | Get hash | malicious | Browse | • 105.77.187.180 | |
| | JYWlIP5wHP | Get hash | malicious | Browse | • 197.146.25.4.217 | |
| | GRPVtMlBk5 | Get hash | malicious | Browse | • 197.144.26.151 | |
| | arm | Get hash | malicious | Browse | • 197.144.16.3.105 | |
| | 7vmT7Q2se0 | Get hash | malicious | Browse | • 105.71.48.24 | |
| | UCeLJ4imjH | Get hash | malicious | Browse | • 105.64.212.3 | |
| | B2WBaqkm8k | Get hash | malicious | Browse | • 105.73.29.133 | |
| | x86.light | Get hash | malicious | Browse | • 197.144.11.5.246 | |
| | arm.light | Get hash | malicious | Browse | • 41.137.188.218 | |
| | KEgx4IC3Ni | Get hash | malicious | Browse | • 197.144.26.132 | |
| | JOKLVsEL8u | Get hash | malicious | Browse | • 105.69.125.132 | |
| | jew.arm7 | Get hash | malicious | Browse | • 105.77.187.192 | |
| | sMzJ1RkRk6 | Get hash | malicious | Browse | • 105.77.76.129 | |
| | b3astmode.x86 | Get hash | malicious | Browse | • 105.75.71.106 | |
| | UPHSUS | DvwfkRaTRo | Get hash | malicious | Browse | • 170.213.1.18 |
| | | P82zcbRMNt | Get hash | malicious | Browse | • 170.212.23.3.216 |
| | | auzkes | Get hash | malicious | Browse | • 170.213.66.14 |
| | | WmEErPtdS9 | Get hash | malicious | Browse | • 170.213.42.63 |
| eNrYzJWFvB | | Get hash | malicious | Browse | • 170.212.121.43 | |
| bqrHRKVNod | | Get hash | malicious | Browse | • 170.214.183.91 | |
| hWT9RJDotD | | Get hash | malicious | Browse | • 170.213.91.12 | |
| x86.light | | Get hash | malicious | Browse | • 170.213.91.17 | |
| JOKLVsEL8u | | Get hash | malicious | Browse | • 170.214.195.73 | |
| lOuZkpwjxy | | Get hash | malicious | Browse | • 170.212.121.54 | |
| 666.arm7 | | Get hash | malicious | Browse | • 170.212.121.51 | |
| 666.arm | | Get hash | malicious | Browse | • 170.212.121.65 | |
| K3h3TPEpze | | Get hash | malicious | Browse | • 170.212.121.63 | |
| 3FjsOtbexQ | | Get hash | malicious | Browse | • 170.212.121.72 | |
| LRLZJUXBpk | | Get hash | malicious | Browse | • 170.213.17.21 | |
| 1UK4uee6lr | | Get hash | malicious | Browse | • 170.212.121.55 | |
| tW7pu9B8A0 | | Get hash | malicious | Browse | • 170.212.14.5.242 | |
| DDy9cpZul8 | | Get hash | malicious | Browse | • 170.214.158.52 | |
| Y3A7DmxPYo | Get hash | malicious | Browse | • 170.212.169.32 | | |
| Vc750ym6VO | Get hash | malicious | Browse | • 170.213.66.26 | | |

JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|----------------------------------|------------------------------|--------------------------|-----------|------------------------|------------------|
| 8662467bc96db2d387755570446a7946 | Filecoder.Hive_linux.bin | Get hash | malicious | Browse | • 162.213.33.108 |
| | mirai.arm | Get hash | malicious | Browse | • 162.213.33.108 |
| | 2j7dEG022b | Get hash | malicious | Browse | • 162.213.33.108 |
| | sora.arm7 | Get hash | malicious | Browse | • 162.213.33.108 |
| | sora.x86 | Get hash | malicious | Browse | • 162.213.33.108 |
| | sora.arm | Get hash | malicious | Browse | • 162.213.33.108 |
| | EHqBakwhNU | Get hash | malicious | Browse | • 162.213.33.108 |
| | vq0sPINJDK | Get hash | malicious | Browse | • 162.213.33.108 |
| | w07UCYGzBe | Get hash | malicious | Browse | • 162.213.33.108 |
| | Rry5mHEWuH | Get hash | malicious | Browse | • 162.213.33.108 |
| | ofgE8wetW4 | Get hash | malicious | Browse | • 162.213.33.108 |
| | 0bqzNlp9PV | Get hash | malicious | Browse | • 162.213.33.108 |
| | yjJXz4a3u6 | Get hash | malicious | Browse | • 162.213.33.108 |
| | g3wyMOTecE | Get hash | malicious | Browse | • 162.213.33.108 |
| | 7k6FKvDl0x | Get hash | malicious | Browse | • 162.213.33.108 |
| | KSzA1ujvIV | Get hash | malicious | Browse | • 162.213.33.108 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|-------|------------------------------|--------------------------|-----------|------------------------|------------------|
| | y66dLhUn0G | Get hash | malicious | Browse | • 162.213.33.108 |
| | 5j9ZIHs8fD | Get hash | malicious | Browse | • 162.213.33.108 |
| | 1isequal9.arm7 | Get hash | malicious | Browse | • 162.213.33.108 |
| | 1isequal9.x86 | Get hash | malicious | Browse | • 162.213.33.108 |

Dropped Files

No context

Created / dropped Files

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink

| | |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 10 |
| Entropy (8bit): | 2.9219280948873623 |
| Encrypted: | false |
| SSDEEP: | 3:5bkPn:pkP |
| MD5: | FF001A15CE15CF062A3704CEA2991B5F |
| SHA1: | B06F6855F376C3245B82212AC73ADED55DFE5DEF |
| SHA-256: | C54830B41ECFA1B6FBDC30397188DDA86B7B200E62AEAC21AE69A46192DCC38A |
| SHA-512: | 65EBF7C31F6F65713CE01B38A112E97D0AE64A6BD1DA40CE4C1B998F10CD3912EE1A48BB2B279B24493062118AAB3B8753742E2AF28E56A31A7AAB27DE80E7BF |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | auto_null. |

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source

| | |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 18 |
| Entropy (8bit): | 3.4613201402110088 |
| Encrypted: | false |
| SSDEEP: | 3:5bkrlZsXvn:pkckv |
| MD5: | 28FE6435F34B3367707BB1C5D5F6B430 |
| SHA1: | EB8FE2D16BD6BBCCCE106C94E4D284543B2573CF6 |
| SHA-256: | 721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0 |
| SHA-512: | 6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | auto_null.monitor. |

/proc/5309/oom_score_adj

| | |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/sbin/sshd |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 6 |
| Entropy (8bit): | 1.7924812503605778 |
| Encrypted: | false |
| SSDEEP: | 3:ptn:Dn |
| MD5: | CBF282CC55ED0792C33D10003D1F760A |
| SHA1: | 007DD8BD75468E6B7ABA4285E9B267202C7EAEED |
| SHA-256: | FCDBAB99FC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22 |
| SHA-512: | 4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | -1000. |

/proc/5309/oom_score_adj

/proc/5354/oom_score_adj

| | |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FCECB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

/proc/5357/oom_score_adj

| | |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FCECB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

/proc/5359/oom_score_adj

| | |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FCECB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

/proc/5361/oom_score_adj

| | |
|-----------------|----------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |

| /proc/5361/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5363/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5365/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5368/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5510/oom_score_adj | |
|---------------------------------|----------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |

| /proc/5510/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5540/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5543/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5545/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5547/oom_score_adj | |
|---------------------------------|----------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /proc/5547/oom_score_adj | |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /proc/5549/oom_score_adj | |
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /proc/5551/oom_score_adj | |
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /proc/5554/oom_score_adj | |
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| | |
|---------------------------------|----------------------------|
| /proc/5862/oom_score_adj | |
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |

| /proc/5862/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5934/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/6096/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /proc/6165/oom_score_adj | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A199 |
| Malicious: | false |
| Preview: | 0 |

| /run/sshd.pid | |
|----------------------|----------------|
| Process: | /usr/sbin/sshd |
| File Type: | ASCII text |
| Category: | dropped |

| | |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /run/sshd.pid | |
| Size (bytes): | 5 |
| Entropy (8bit): | 2.321928094887362 |
| Encrypted: | false |
| SSDEEP: | 3:DVcv:Je |
| MD5: | 67C6C7A19AD77C7A022F3CA0F47B5DC1 |
| SHA1: | B20FED7048E1ED1D30F1FC309347CCD80D323D10 |
| SHA-256: | 645DEDF45F2201B624D44BA9389274520328A9D16568BBE99B0CD60F675E5B23 |
| SHA-512: | A2F6C519536D91C5EC081DDF2522DA04A121868B005CFB89E074000D44A4A3907B3F87B144133D6FA8BF29C3E59DC95985653F659D0F72EE9149C66AFB00F229 |
| Malicious: | false |
| Preview: | 5309. |

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /run/user/1000/pulse/pid | |
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 1.9219280948873623 |
| Encrypted: | false |
| SSDEEP: | 3:ESn:ES |
| MD5: | 01895904E99DFA92AE03CD54B4FBC6FB |
| SHA1: | C38A1109FF3907ACFC3163B6C90629159D2AFCAF |
| SHA-256: | B6E80AFF395E6420FC6A40066BB683EB0AF0DC336428F54DD533BAFC1359603E |
| SHA-512: | 92E9461FF816D59D2AF7BA04A8E8FD1A941CE754C3BC956999E67C1CDBB3271CFE7AE0AF9603935F09EFA4B58878DCF489EC532B48D190B0070409E9F018FF9A |
| Malicious: | false |
| Preview: | 5414. |

| | |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /run/user/127/ICEauthority | |
| Process: | /usr/libexec/gnome-session-binary |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1304 |
| Entropy (8bit): | 5.971492084482531 |
| Encrypted: | false |
| SSDEEP: | 12:OxPinYPMveY+inYKxPbo0eveY+bxaxP5mhijveY+5tWmxPwWoveY+wcZVveY+wYN:dLg07MwqrY5+u0 |
| MD5: | 103AC039CA34E1FCAD294A4B16997227 |
| SHA1: | 12E91CF7107A182DA4DD3BDF1DB9DD3DEEE09974 |
| SHA-256: | 57B896B8D33C6B2A509779E049A940F205066278F281E2E28D72499F71039E65 |
| SHA-512: | FF81DBAD664C2ED1FC6915EC6C819953BBA6A8E3E22D7606AA58EABD504C41D82802A14E6C395BE110CD5DF767F40376F40B08EE2C118E27F4673D270F6AEE8 |
| Malicious: | false |
| Preview: | ..XSMP...!unix/galassia:/tmp/.ICE-unix/5455..MIT-MAGIC-COOKIE-1....f.9.T.....XSMP...#local/galassia:@/tmp/.ICE-unix/5455..MIT-MAGIC-COOKIE-1...[/u?X.F..."
...ICE...!unix/galassia:/tmp/.ICE-unix/5350..MIT-MAGIC-COOKIE-1...X..nU.....ICE...#local/galassia:@/tmp/.ICE-unix/5350..MIT-MAGIC-COOKIE-1....vd,M89.g.R.
.D...XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.....A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1....o.(R...).
9...ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w\$....^..fi..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f.....E.
.c..XSMP...#ocal/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... ..Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#.....:B.
o.....ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...N.yte 4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN....
.N+..\$.XSMP...#ocal/galass |

| | |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /run/user/127/dconf/user | |
| Process: | /usr/libexec/gsd-power |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:: |
| MD5: | 93B885ADFE0DA089CDF634904FD59F71 |
| SHA1: | 5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F |
| SHA-256: | 6E340B9CFFB37A989CA544E6BB780A2C78901D3FB33738768511A30617AFA01D |
| SHA-512: | B8244D028981D693AF7B456AF8EFA4CAD63D282E19FF14942C246E50D9351D22704A802A71C3580B6370DE4CEB293C324A8423342557D4E5C38438F0E36910EE |
| Malicious: | false |
| Preview: | . |

| | |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| /run/user/127/gdm/Xauthority | |
| Process: | /usr/lib/gdm3/gdm-x-session |
| File Type: | X11 Xauthority data |
| Category: | dropped |
| Size (bytes): | 104 |
| Entropy (8bit): | 5.0217563256604105 |
| Encrypted: | false |
| SSDEEP: | 3:rg/WFIlaO93UAa9WFIlaO93Ul:rg/WFI2kAa9WFI2kl |
| MD5: | 78C15B5CA0F46184CA853F3B6F026C10 |
| SHA1: | 4E34A81DECA4EB927F28F630B530007168BEEFC7 |
| SHA-256: | C58D2AF355F230BC5848CB15D53CFF99C5D4430DBD20582D76B948DB539F400C |
| SHA-512: | F2571326097E91BF5CE2269208134BE408669D40119ED01EC6C2C5DCDE306A9B7FCBB6D95AE52E8FF1ED4E41EF62284DDAF9282344CEF82A79CCC6B40BDF71 |
| Malicious: | false |
| Preview: |galassia....MIT-MAGIC-COOKIE-1..m...k....B.....galassia....MIT-MAGIC-COOKIE-1..m...k....B..... |

| | |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| /run/user/127/pulse/pid | |
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 2.321928094887362 |
| Encrypted: | false |
| SSDEEP: | 3:llv:llv |
| MD5: | 47F88514E1FCFA836614BA96A8E1C5BF |
| SHA1: | 751DC412C22BB5737961269C7D901F78BBA94BF5 |
| SHA-256: | 8C726B4FAEDFB4F2FF9B430181FD654C91E39F20AA6F2F9571CD649A0CE24AA6 |
| SHA-512: | E92BDAC552DCEAF7FD0C608576E207192FE8C01CA50EA8552266BB8847813DE84CADB28FD766EC31A8BA24F0D9B98484FCFCC29AC36BED3115B0780233E10FB |
| Malicious: | false |
| Preview: | 5873. |

| | |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /tmp/server-0.xkm | |
| Process: | /usr/bin/xkbcomp |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 12060 |
| Entropy (8bit): | 4.8492493153178975 |
| Encrypted: | false |
| SSDEEP: | 192:tDyb2zOmnECQmwTVfFlaSLus4UVcqLkjoqd//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ |
| MD5: | B4E3EB0B8B60FC1F46740C573E18D86 |
| SHA1: | 7D35426357695EBA77850757E8939A62DCEFF2D1 |
| SHA-256: | 7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91 |
| SHA-512: | 8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE01 |
| Malicious: | false |
| Preview: | .mkx.....D.....h.....<....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt...RAIt...RControl....LControl....ScrollLock..LevelFive...AltGr...Meta
....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD
06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB
08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSKLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP
3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTMUHEJPCMKPENRCTLKPDVPRSCRALTlnFDHOMEUP..PGUPLEFTRGHTEND.DOWN
PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI
NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181
I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18 |

| | |
|-----------------------------|--------------------------------------------------------------------------------------------|
| /var/cache/motd-news | |
| Process: | /usr/bin/cut |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 191 |
| Entropy (8bit): | 4.515771857099866 |
| Encrypted: | false |
| SSDEEP: | 3:P2lnl+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTI/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn |
| MD5: | DD514F892B5F93ED615D366E58AC58AF |
| SHA1: | BA75EDB3C2232CC260BC187F604DC8F25AA72C11 |
| SHA-256: | F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF |

| | |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /var/cache/motd-news | |
| SHA-512: | 9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACDCBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42A2D0 |
| Malicious: | false |
| Preview: | * Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation . |

| | |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| /var/lib/AccountsService/users/gdm.G9YJC1 | |
| Process: | /usr/lib/accounts-service/accounts-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 61 |
| Entropy (8bit): | 4.66214589518167 |
| Encrypted: | false |
| SSDEEP: | 3:urzMQvNT+PzKlRAn4R8AKn:gzMqIzKlRaa4M |
| MD5: | 542BA3FB41206AE43928AF1C5E61FEBC |
| SHA1: | F56F574DAF50D609526B36B5B54FDD59EA4D6A26 |
| SHA-256: | 730D9509D4EAA7266829A8F5A8CFEBA6BBDD5873FC2BD580AD464F4A237E11A |
| SHA-512: | D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42FAEA |
| Malicious: | false |
| Preview: | [User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true. |

| | |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| /var/lib/AccountsService/users/gdm.WH5PC1 | |
| Process: | /usr/lib/accounts-service/accounts-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 61 |
| Entropy (8bit): | 4.66214589518167 |
| Encrypted: | false |
| SSDEEP: | 3:urzMQvNT+PzKlRAn4R8AKn:gzMqIzKlRaa4M |
| MD5: | 542BA3FB41206AE43928AF1C5E61FEBC |
| SHA1: | F56F574DAF50D609526B36B5B54FDD59EA4D6A26 |
| SHA-256: | 730D9509D4EAA7266829A8F5A8CFEBA6BBDD5873FC2BD580AD464F4A237E11A |
| SHA-512: | D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42FAEA |
| Malicious: | false |
| Preview: | [User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true. |

| | |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0 | |
| Process: | /usr/bin/ibus-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 381 |
| Entropy (8bit): | 5.184925060132627 |
| Encrypted: | false |
| SSDEEP: | 6:SbF4b2sONeZVksQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWW1ohX4pA19H:q5sU3LWfLUDmQymqSFbomSHohGafH |
| MD5: | 6C30425EBF0424831BB890F37511D738 |
| SHA1: | 635DBBF50FAD07A2858021FA291DC72D1A07FCA8 |
| SHA-256: | 556526E5305217FB12DB458CC145C0A31A71353C761580FC1C92863BAEA37A00 |
| SHA-512: | 956C9B9A926975925F644931AEA56670ED1DC0864094E98F3CF4E238361DD56D35A4230DDD8DC5A9488AEA56CD93B4F9E8BCD270DFF756FF75A05509CC070E |
| Malicious: | false |
| Preview: | # This file is created by ibus-daemon, please do not modify it.## This file allows processes on the machine to find the # ibus session bus with the below address.## If the IBUS_ADDRESS environment variable is set, it will # be used rather than this file. .IBUS_ADDRESS=unix:abstract=/var/lib/gdm3/.cache/ibus/dbus-MXBP39k,guid=8e502356918246cb6e477da7618b4903.IBUS_DAEMON_PID=5609. |

| | |
|----------------------------------------------------------------------------------|----------------------------|
| /var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink | |
| Process: | /usr/bin/pulseaudio |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:v:v |

| /var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink | |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| MD5: | 68B329DA9893E34099C7D8AD5CB9C940 |
| SHA1: | ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC |
| SHA-256: | 01BA4719C80B6FE911B091A7C05124B64EEEECE964E09C058EF8F9805DACA546B |
| SHA-512: | BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09 |
| Malicious: | false |
| Preview: | . |

| /var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source | |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/pulseaudio |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:v:v |
| MD5: | 68B329DA9893E34099C7D8AD5CB9C940 |
| SHA1: | ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC |
| SHA-256: | 01BA4719C80B6FE911B091A7C05124B64EEEECE964E09C058EF8F9805DACA546B |
| SHA-512: | BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09 |
| Malicious: | false |
| Preview: | . |

| /var/lib/whoopsie/whoopsie-id.Y8U6B1 | |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/bin/whoopsie |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 128 |
| Entropy (8bit): | 3.9410969045919657 |
| Encrypted: | false |
| SSDEEP: | 3:19y6UTAvBTdDVEQcNgAT0XUQhd3tjCzccCKcsVQWQ7JW:3y6BIVefQXU8djCZd40 |
| MD5: | D2B5AAF22916F8D6665CF9E835EAD5E7 |
| SHA1: | AAEF3CE527B8F1E3733BCD03EF7A6C0F30881E15 |
| SHA-256: | FEB925D4465BF6D30A42B19112406AD1B59BA90673DC4F91B25005A90FEFEB36 |
| SHA-512: | B55A45FA0DECE5A3B0348BC3F3031A7329590E57BAD5013690AFEA9825C0DE4B75D27057A56C33800F1626935840DA2262AAF14E795C75F39362B728D95F18A |
| Malicious: | false |
| Preview: | 9aadafe2051348cd32033e1cad68f0a5fe46fba3240ac1e6e42158f31b8a1371790c09baf3996b4979fe8e533446c7dedf30f654c68b25357334c66911dc6a9e |

| /var/log/Xorg.0.log | |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process: | /usr/lib/xorg/Xorg |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 41347 |
| Entropy (8bit): | 5.287066635729438 |
| Encrypted: | false |
| SSDEEP: | 384:XpgBwlDvMnd4did2dPdyd8dddldjgdRdFdhdT dndAdBd4dWd0dcDdZvdc2d+d7B:ZgBUY7wSiUj/WvMqOjfkH |
| MD5: | 51F3496C1A34781D172A478206DE9F93 |
| SHA1: | 513E4689FBFC01EAC87C040DAECC53F0C1F85D24 |
| SHA-256: | 0CC6FC9FE92F582ACBDD1784F817D6669272D52034683514BDAA9019F12D723F |
| SHA-512: | E74695AC0AFC539EAC11F329CA650918403AB396C27E1E2BE9CF75CB634BD69D8F7ED1BAC4C0DF5CAF16E460A4F8F3BBD7E1E4D1A61DC1FD24462BA05ECC0 |
| Malicious: | false |
| Preview: | [484.220] (--) Log file renamed from "/var/log/Xorg.pid-5407.log" to "/var/log/Xorg.0.log".[484.245] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[484.255] Build Operating System: linux Ubuntu.[484.261] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[484.268] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[484.285] Build Date: 06 July 2021 10:17:51AM.[484.290] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[484.296] Current version of pixman: 0.38.4.[484.302] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[484.316] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??) |

Static File Info

| General | |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File type: | ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped |
| Entropy (8bit): | 7.986206825808691 |
| TrID: | <ul style="list-style-type: none"> ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | arm7 |
| File size: | 64528 |
| MD5: | 18e0a7425fa5b743bb6dd7002a71cfcc |
| SHA1: | 32fb441007353ad30ae7c10c7e1368686c999d3c |
| SHA256: | ac4582bf75332e1b51b11e1dcaa362e5fa933bf13497bab1da64079dab0c1d6f |
| SHA512: | 766ce70e1936af18117aae83c4586f46757244bca8d8f41895403931dee8ae34a597ebec5b76639cb06a3a6f1ad991e4b48afecdfbdea452a7f526c5086771 |
| SSDEEP: | 1536:aTOic71ErNWpa9l9pH5KjyliUEBMHLc7fOhx68R4TLg:ztE63skXEBmLc7fOH6i4ng |
| File Content Preview: | .ELF.....(.....\$.4.....4.....(.....
.....x...x...x.....Q.td.....aUPX!.....
.....!.....?E.h;...#..\$.o.....b..-B.*...5N&"a...#R.
a..a...C...g...k'.. |

Static ELF Info

ELF header

| | |
|----------------------------|-------------------------------|
| Class: | ELF32 |
| Data: | 2's complement, little endian |
| Version: | 1 (current) |
| Machine: | ARM |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | UNIX - Linux |
| ABI Version: | 0 |
| Entry Point Address: | 0x124d8 |
| Flags: | 0x4000002 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 0 |
| Section Header Size: | 40 |
| Number of Section Headers: | 0 |
| Header String Table Index: | 0 |

Program Segments

| Type | Offset | Virtual Address | Physical Address | File Size | Memory Size | Entropy | Flags | Flags Description | Align | Prog Interpreter | Section Mappings |
|-----------|--------|-----------------|------------------|-----------|-------------|---------|-------|-------------------|--------|------------------|------------------|
| LOAD | 0x0 | 0x8000 | 0x8000 | 0xb6c5 | 0xb6c5 | 4.0445 | 0x5 | R E | 0x8000 | | |
| LOAD | 0x878 | 0x30878 | 0x30878 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x8000 | | |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

Network Behavior

TCP Packets

DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|-------------------------------------|--------------|---------|----------|--------------------|------------------|----------------|-------------|
| Nov 10, 2021 04:21:13.643590927 CET | 192.168.2.23 | 1.1.1.1 | 0x2c3b | Standard query (0) | daisy.ubuntu.com | A (IP address) | IN (0x0001) |
| Nov 10, 2021 04:21:13.643702984 CET | 192.168.2.23 | 1.1.1.1 | 0x596b | Standard query (0) | daisy.ubuntu.com | 28 | IN (0x0001) |
| Nov 10, 2021 04:21:13.735826969 CET | 192.168.2.23 | 1.1.1.1 | 0xe44a | Standard query (0) | daisy.ubuntu.com | 28 | IN (0x0001) |

DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|-------------------------------------------|-----------|--------------|----------|--------------|------------------|-------|----------------|----------------|-------------|
| Nov 10, 2021
04:21:13.672904968
CET | 1.1.1.1 | 192.168.2.23 | 0x2c3b | No error (0) | daisy.ubuntu.com | | 162.213.33.132 | A (IP address) | IN (0x0001) |
| Nov 10, 2021
04:21:13.672904968
CET | 1.1.1.1 | 192.168.2.23 | 0x2c3b | No error (0) | daisy.ubuntu.com | | 162.213.33.108 | A (IP address) | IN (0x0001) |

System Behavior

Analysis Process: dash PID: 5209 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: cat PID: 5209 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cat |
| Arguments: | cat /tmp/tmp.F8yqW15XWY |
| File size: | 43416 bytes |
| MD5 hash: | 7e9d213e404ad3bb82e4ebb2e1f2c1b3 |

File Activities

File Read

Analysis Process: dash PID: 5210 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: head PID: 5210 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/head |
| Arguments: | head -n 10 |
| File size: | 47480 bytes |
| MD5 hash: | fd96a67145172477dd57131396fc9608 |

File Activities

File Read

Analysis Process: dash PID: 5211 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: tr PID: 5211 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/tr |
| Arguments: | tr -d \000-\011\013\014\016-\037 |
| File size: | 51544 bytes |
| MD5 hash: | fb1402dd9f72d8ebff00ce7c3a7bb5 |

File Activities

File Read

Analysis Process: dash PID: 5212 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: cut PID: 5212 Parent PID: 4331

General

| | |
|-------------|--------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cut |

| | |
|------------|----------------------------------|
| Arguments: | cut -c -80 |
| File size: | 47480 bytes |
| MD5 hash: | d8ed0ea8f22c0de0f8692d4d9f1759d3 |

File Activities

File Read

Analysis Process: dash PID: 5213 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: cat PID: 5213 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cat |
| Arguments: | cat /tmp/tmp.F8yqW15XWY |
| File size: | 43416 bytes |
| MD5 hash: | 7e9d213e404ad3bb82e4ebb2e1f2c1b3 |

File Activities

File Read

Analysis Process: dash PID: 5214 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: head PID: 5214 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/head |
| Arguments: | head -n 10 |
| File size: | 47480 bytes |
| MD5 hash: | fd96a67145172477dd57131396fc9608 |

File Activities

File Read

Analysis Process: dash PID: 5215 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: tr PID: 5215 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/tr |
| Arguments: | tr -d \000-\011\013\014\016-\037 |
| File size: | 51544 bytes |
| MD5 hash: | fb1402dd9f72d8ebff00ce7c3a7bb5 |

File Activities

File Read

Analysis Process: dash PID: 5216 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: cut PID: 5216 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/cut |
| Arguments: | cut -c -80 |
| File size: | 47480 bytes |
| MD5 hash: | d8ed0ea8f22c0de0f8692d4d9f1759d3 |

File Activities

File Read

File Written

Analysis Process: dash PID: 5219 Parent PID: 4331

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dash |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: rm PID: 5219 Parent PID: 4331

General

| | |
|-------------|------------------------------------------------------------------|
| Start time: | 04:20:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/rm |
| Arguments: | rm -f /tmp/tmp.F8yqW15XWY /tmp/tmp.FsztahiAst /tmp/tmp.rbFGPyqdP |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

File Activities

File Deleted

File Read

Analysis Process: arm7 PID: 5249 Parent PID: 5110

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:28 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm7 |
| Arguments: | /tmp/arm7 |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

File Activities

File Read

Analysis Process: arm7 PID: 5251 Parent PID: 5249

General

| | |
|-------------|------------|
| Start time: | 04:20:28 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm7 |

| | |
|------------|----------------------------------|
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

Analysis Process: arm7 PID: 5252 Parent PID: 5249

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:28 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm7 |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

Analysis Process: arm7 PID: 5256 Parent PID: 5252

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:28 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm7 |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

File Activities

File Read

Directory Enumerated

Analysis Process: arm7 PID: 5258 Parent PID: 5252

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:28 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm7 |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

Analysis Process: arm7 PID: 5260 Parent PID: 5258

General

| | |
|-------------|----------------------------------|
| Start time: | 04:20:28 |
| Start date: | 10/11/2021 |
| Path: | /tmp/arm7 |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

Analysis Process: systemd PID: 5296 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:12 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: whoopsie PID: 5296 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:12 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/whoopsie |
| Arguments: | /usr/bin/whoopsie -f |
| File size: | 68592 bytes |
| MD5 hash: | d3a6915d0e7398fb4c89a037c13959c8 |

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5308 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: sshd PID: 5308 Parent PID: 1

General

| | |
|-------------|-------------------|
| Start time: | 04:21:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/sshd |
| Arguments: | /usr/sbin/sshd -t |
| File size: | 876328 bytes |

| | |
|-----------|----------------------------------|
| MD5 hash: | dbca7a6bbf7bf57fedac243d4b2cb340 |
|-----------|----------------------------------|

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5309 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: sshd PID: 5309 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:16 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/sshd |
| Arguments: | /usr/sbin/sshd -D |
| File size: | 876328 bytes |
| MD5 hash: | dbca7a6bbf7bf57fedac243d4b2cb340 |

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm3 PID: 5314 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: Default PID: 5314 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:23 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gdm3 PID: 5318 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:23 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: Default PID: 5318 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:23 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: systemd PID: 5319 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: accounts-daemon PID: 5319 Parent PID: 1

General

| | |
|-------------|------------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/accountsservice/accounts-daemon |

| | |
|------------|------------------------------------------|
| Arguments: | /usr/lib/accountsservice/accounts-daemon |
| File size: | 203192 bytes |
| MD5 hash: | 01a899e3fb5e7e434bea1290255a1f30 |

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: accounts-daemon PID: 5334 Parent PID: 5319

General

| | |
|-------------|------------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/accountsservice/accounts-daemon |
| Arguments: | n/a |
| File size: | 203192 bytes |
| MD5 hash: | 01a899e3fb5e7e434bea1290255a1f30 |

File Activities

Directory Enumerated

Analysis Process: language-validate PID: 5334 Parent PID: 5319

General

| | |
|-------------|---------------------------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/share/language-tools/language-validate |
| Arguments: | /usr/share/language-tools/language-validate en_US.UTF-8 |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: language-validate PID: 5335 Parent PID: 5334

General

| | |
|-------------|---------------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/share/language-tools/language-validate |

| | |
|------------|----------------------------------|
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: language-options PID: 5335 Parent PID: 5334

General

| | |
|-------------|--------------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/share/language-tools/language-options |
| Arguments: | /usr/share/language-tools/language-options |
| File size: | 3478464 bytes |
| MD5 hash: | 16a21f464119ea7fad1d3660de963637 |

File Activities

File Read

Directory Enumerated

Analysis Process: language-options PID: 5336 Parent PID: 5335

General

| | |
|-------------|--------------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/share/language-tools/language-options |
| Arguments: | n/a |
| File size: | 3478464 bytes |
| MD5 hash: | 16a21f464119ea7fad1d3660de963637 |

Analysis Process: sh PID: 5336 Parent PID: 5335

General

| | |
|-------------|------------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | sh -c "locale -a grep -F .utf8 " |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: sh PID: 5337 Parent PID: 5336

General

| | |
|-------------|------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |

| | |
|------------|----------------------------------|
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: locale PID: 5337 Parent PID: 5336

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/locale |
| Arguments: | locale -a |
| File size: | 58944 bytes |
| MD5 hash: | c72a78792469db86d91369c9057f20d2 |

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5338 Parent PID: 5336

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: grep PID: 5338 Parent PID: 5336

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:24 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/grep |
| Arguments: | grep -F .utf8 |
| File size: | 199136 bytes |
| MD5 hash: | 1e6ebb9dd094f774478f72727bdba0f5 |

File Activities

File Read

Analysis Process: gdm3 PID: 5339 Parent PID: 1320

General

| | |
|-------------|----------------|
| Start time: | 04:21:26 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |

| | |
|------------|----------------------------------|
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: gdm-session-worker PID: 5339 Parent PID: 1320

General

| | |
|-------------|---------------------------------------------------|
| Start time: | 04:21:26 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | "gdm-session-worker [pam/gdm-launch-environment]" |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm-session-worker PID: 5343 Parent PID: 5339

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

Analysis Process: gdm-wayland-session PID: 5343 Parent PID: 5339

General

| | |
|-------------|--------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-wayland-session |
| Arguments: | /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart" |
| File size: | 76368 bytes |
| MD5 hash: | d3def63cf1e83f7fb8a0f13b1744ff7c |

File Activities

File Read

Analysis Process: gdm-wayland-session PID: 5348 Parent PID: 5343

General

| | |
|-------------|----------|
| Start time: | 04:21:28 |
|-------------|----------|

| | |
|-------------|-----------------------------------|
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-wayland-session |
| Arguments: | n/a |
| File size: | 76368 bytes |
| MD5 hash: | d3def63cf1e83f7fb8a0f13b1744ff7c |

File Activities

Directory Enumerated

Analysis Process: dbus-run-session PID: 5348 Parent PID: 5343

General

| | |
|-------------|--------------------------------------------------------------------------------|
| Start time: | 04:21:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

File Activities

File Read

Analysis Process: dbus-run-session PID: 5349 Parent PID: 5348

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

Analysis Process: dbus-daemon PID: 5349 Parent PID: 5348

General

| | |
|-------------|--------------------------------------------------|
| Start time: | 04:21:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | dbus-daemon --nofork --print-address 4 --session |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: dbus-daemon PID: 5353 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:30 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5354 Parent PID: 5353

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:30 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5354 Parent PID: 5353

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:30 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5356 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5357 Parent PID: 5356

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5357 Parent PID: 5356

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5358 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5359 Parent PID: 5358

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5359 Parent PID: 5358

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5360 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5361 Parent PID: 5360

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5361 Parent PID: 5360

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5362 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5363 Parent PID: 5362

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5363 Parent PID: 5362

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5364 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5365 Parent PID: 5364

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5365 Parent PID: 5364

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:31 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5367 Parent PID: 5349

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5368 Parent PID: 5367

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5368 Parent PID: 5367

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:32 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-run-session PID: 5350 Parent PID: 5348

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

Analysis Process: gnome-session PID: 5350 Parent PID: 5348

General

| | |
|-------------|------------------------------------------------------------|
| Start time: | 04:21:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/gnome-session |
| Arguments: | gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5350 Parent PID: 5348

General

| | |
|-------------|------------------------------------------------------------------------------------------|
| Start time: | 04:21:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

File Created

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Link Created

Analysis Process: gnome-session-binary PID: 5369 Parent PID: 5350

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:21:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: session-migration PID: 5369 Parent PID: 5350

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/session-migration |
| Arguments: | session-migration |
| File size: | 22680 bytes |
| MD5 hash: | 5227af42ebf14ac2fe2acddb002f68dc |

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5370 Parent PID: 5350

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:21:33 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 5370 Parent PID: 5350

General

| | |
|-------------|-----------------------------------------------------------------------------------------------------|
| Start time: | 04:21:33 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/bin/gnome-shell |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gnome-shell PID: 5370 Parent PID: 5350

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:33 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/gnome-shell |
| Arguments: | /usr/bin/gnome-shell |
| File size: | 23168 bytes |
| MD5 hash: | da7a257239677622fe4b3a65972c9e87 |

File Activities

File Read

Directory Enumerated

Analysis Process: gdm3 PID: 5398 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: gdm-session-worker PID: 5398 Parent PID: 1320

General

| | |
|-------------|---------------------------------------------------|
| Start time: | 04:21:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | "gdm-session-worker [pam/gdm-launch-environment]" |
| File size: | 293360 bytes |

| | |
|-----------|----------------------------------|
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |
|-----------|----------------------------------|

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm-session-worker PID: 5405 Parent PID: 5398

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

Analysis Process: gdm-x-session PID: 5405 Parent PID: 5398

General

| | |
|-------------|--------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | /usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart" |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

File Activities

File Read

File Written

Directory Created

Analysis Process: gdm-x-session PID: 5407 Parent PID: 5405

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | n/a |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

File Activities

Directory Enumerated

Analysis Process: Xorg PID: 5407 Parent PID: 5405

General

| | |
|-------------|-----------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/Xorg |
| Arguments: | /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeppty -verbose 3 |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: Xorg.wrap PID: 5407 Parent PID: 5405

General

| | |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/xorg/Xorg.wrap |
| Arguments: | /usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeppty -verbose 3 |
| File size: | 14488 bytes |
| MD5 hash: | 48993830888200ecf19dd7def0884dfd |

File Activities

File Read

Analysis Process: Xorg PID: 5407 Parent PID: 5405

General

| | |
|-------------|----------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeppty -verbose 3 |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Analysis Process: Xorg PID: 5443 Parent PID: 5407

| General | |
|-------------|----------------------------------|
| Start time: | 04:21:49 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | n/a |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

Analysis Process: sh PID: 5443 Parent PID: 5407

| General | |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:49 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | sh -c "'/usr/bin/xkbcomp' -w 1 '-R/usr/share/X11/xkb' -xkm '-l' -em1 'The XKEYBOARD keymap compiler (xkbcomp) reports:' -emp ' > ' -eml 'Errors from xkbcomp are not fatal to the X server' '/tmp/server-0.xkm'" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: sh PID: 5444 Parent PID: 5443

| General | |
|-------------|----------------------------------|
| Start time: | 04:21:49 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: xkbcomp PID: 5444 Parent PID: 5443

| General | |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:21:49 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/xkbcomp |
| Arguments: | /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm |
| File size: | 217184 bytes |
| MD5 hash: | c5f953aec4c00d2a1cc27acb75d62c9b |

File Activities

File Deleted

File Read

File Written

Analysis Process: Xorg PID: 5866 Parent PID: 5407**General**

| | |
|-------------|----------------------------------|
| Start time: | 04:22:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | n/a |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

Analysis Process: sh PID: 5866 Parent PID: 5407**General**

| | |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:28 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | sh -c "'/usr/bin/xkbcomp' -w 1 '-R/usr/share/X11/xkb' -xkm '-l' -em1 'The XKEYBOARD keymap compiler (xkbcomp) reports:' -emp ' > ' -eml 'Errors from xkbcomp are not fatal to the X server' '/tmp/server-0.xkm'" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities**File Read****Analysis Process: sh PID: 5869 Parent PID: 5866****General**

| | |
|-------------|----------------------------------|
| Start time: | 04:22:28 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: xkbcomp PID: 5869 Parent PID: 5866**General**

| | |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:28 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/xkbcomp |
| Arguments: | /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm |
| File size: | 217184 bytes |
| MD5 hash: | c5f953aec4c00d2a1cc27acb75d62c9b |

File Activities**File Deleted****File Read****File Written**

Analysis Process: gdm-x-session PID: 5452 Parent PID: 5405

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:55 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | n/a |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

File Activities

Directory Enumerated

Analysis Process: Default PID: 5452 Parent PID: 5405

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:55 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/Prime/Default |
| Arguments: | /etc/gdm3/Prime/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gdm-x-session PID: 5453 Parent PID: 5405

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:55 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | n/a |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

File Activities

Directory Enumerated

Analysis Process: dbus-run-session PID: 5453 Parent PID: 5405

General

| | |
|-------------|--------------------------------------------------------------------------------|
| Start time: | 04:21:55 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart |

| | |
|------------|----------------------------------|
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

File Activities

File Read

Analysis Process: dbus-run-session PID: 5454 Parent PID: 5453

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:55 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

Analysis Process: dbus-daemon PID: 5454 Parent PID: 5453

General

| | |
|-------------|--------------------------------------------------|
| Start time: | 04:21:55 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | dbus-daemon --nofork --print-address 4 --session |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: dbus-daemon PID: 5509 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5510 Parent PID: 5509

General

| | |
|-------------|------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |

| | |
|------------|----------------------------------|
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: at-spi-bus-launcher PID: 5510 Parent PID: 5509

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/at-spi-bus-launcher |
| Arguments: | /usr/libexec/at-spi-bus-launcher |
| File size: | 27008 bytes |
| MD5 hash: | 1563f274acd4e7ba530a55bdc4c95682 |

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: at-spi-bus-launcher PID: 5515 Parent PID: 5510

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/at-spi-bus-launcher |
| Arguments: | n/a |
| File size: | 27008 bytes |
| MD5 hash: | 1563f274acd4e7ba530a55bdc4c95682 |

File Activities

Directory Enumerated

Analysis Process: dbus-daemon PID: 5515 Parent PID: 5510

General

| | |
|-------------|--------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3 |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 5931 Parent PID: 5515

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5934 Parent PID: 5931

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: at-spi2-registryd PID: 5934 Parent PID: 5931

General

| | |
|-------------|----------------------------------------------------|
| Start time: | 04:22:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/at-spi2-registryd |
| Arguments: | /usr/libexec/at-spi2-registryd --use-gnome-session |
| File size: | 100224 bytes |
| MD5 hash: | 1d904c2693452ede3a9e24d440 |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5539 Parent PID: 5454

General

| | |
|-------------|----------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |

| | |
|------------|----------------------------------|
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5540 Parent PID: 5539

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5540 Parent PID: 5539

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5542 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5543 Parent PID: 5542

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5543 Parent PID: 5542

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5544 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5545 Parent PID: 5544

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5545 Parent PID: 5544

General

| | |
|-------------|------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |

| | |
|------------|----------------------------------|
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5546 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5547 Parent PID: 5546

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5547 Parent PID: 5546

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:10 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5548 Parent PID: 5454

General

| | |
|-------------|------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |

| | |
|------------|----------------------------------|
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5549 Parent PID: 5548

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5549 Parent PID: 5548

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5550 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5551 Parent PID: 5550

General

| | |
|-------------|----------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |

| | |
|-----------|----------------------------------|
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |
|-----------|----------------------------------|

File Activities

File Written

Analysis Process: false PID: 5551 Parent PID: 5550

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5553 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5554 Parent PID: 5553

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 5554 Parent PID: 5553

General

| | |
|-------------|------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |

| | |
|------------|----------------------------------|
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-daemon PID: 5861 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 5862 Parent PID: 5861

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: ibus-portal PID: 5862 Parent PID: 5861

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/ibus-portal |
| Arguments: | /usr/libexec/ibus-portal |
| File size: | 92536 bytes |
| MD5 hash: | 562ad55bd9a4d54bd7b76746b01e37d3 |

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: dbus-daemon PID: 6095 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 6096 Parent PID: 6095

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: gjs PID: 6096 Parent PID: 6095

General

| | |
|-------------|-------------------------------------------------------------------|
| Start time: | 04:22:32 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/gjs |
| Arguments: | /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications |
| File size: | 23128 bytes |
| MD5 hash: | 5f3eceb792bb65c22f23d1efb4fde3ad |

File Activities

File Read

Directory Enumerated

Analysis Process: dbus-daemon PID: 6163 Parent PID: 5454

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

Analysis Process: dbus-daemon PID: 6165 Parent PID: 6163

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:47 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

File Activities

File Written

Analysis Process: false PID: 6165 Parent PID: 6163

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:47 |
| Start date: | 10/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

File Activities

File Read

Analysis Process: dbus-run-session PID: 5455 Parent PID: 5453

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:56 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

Analysis Process: gnome-session PID: 5455 Parent PID: 5453

General

| | |
|-------------|------------------------------------------------------------|
| Start time: | 04:21:56 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/gnome-session |
| Arguments: | gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5455 Parent PID: 5453

General

| | |
|-------------|------------------------------------------------------------------------------------------|
| Start time: | 04:21:56 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

File Created

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Link Created

Analysis Process: gnome-session-binary PID: 5456 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:21:56 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5456 Parent PID: 5455

General

| | |
|-------------|----------------------------------------------|
| Start time: | 04:21:56 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated |
| Arguments: | /usr/libexec/gnome-session-check-accelerated |
| File size: | 18752 bytes |
| MD5 hash: | a64839518af85b2b9de31aca27646396 |

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5516 Parent PID: 5456

General

| | |
|-------------|----------------------------------------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated |
| Arguments: | n/a |
| File size: | 18752 bytes |
| MD5 hash: | a64839518af85b2b9de31aca27646396 |

File Activities

Directory Enumerated

Analysis Process: gnome-session-check-accelerated-gi-helper PID: 5516 Parent PID: 5456

General

| | |
|-------------|-------------------------------------------------------------------------|
| Start time: | 04:22:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated-gi-helper |
| Arguments: | /usr/libexec/gnome-session-check-accelerated-gi-helper --print-renderer |
| File size: | 22920 bytes |
| MD5 hash: | b1ab9a384f9e98a39ae5c36037dd5e78 |

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5528 Parent PID: 5456

General

| | |
|-------------|----------------------------------------------|
| Start time: | 04:22:08 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated |
| Arguments: | n/a |
| File size: | 18752 bytes |
| MD5 hash: | a64839518af85b2b9de31aca27646396 |

File Activities

Directory Enumerated

Analysis Process: gnome-session-check-accelerated-gles-helper PID: 5528 Parent PID: 5456

General

| | |
|-------------|---------------------------------------------------------------------------|
| Start time: | 04:22:08 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated-gles-helper |
| Arguments: | /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer |
| File size: | 14728 bytes |
| MD5 hash: | 1bd78885765a18e60c05ed1fb5fa3bf8 |

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: 5555 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: session-migration PID: 5555 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/session-migration |
| Arguments: | session-migration |
| File size: | 22680 bytes |
| MD5 hash: | 5227af42ebf14ac2fe2acddb002f68dc |

File Activities

File Read

Analysis Process: gnome-session-binary PID: 5558 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:12 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 5558 Parent PID: 5455

General

| | |
|-------------|-----------------------------------------------------------------------------------------------------|
| Start time: | 04:22:12 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/bin/gnome-shell |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gnome-shell PID: 5558 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:12 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/gnome-shell |
| Arguments: | /usr/bin/gnome-shell |
| File size: | 23168 bytes |
| MD5 hash: | da7a257239677622fe4b3a65972c9e87 |

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-shell PID: 5609 Parent PID: 5558

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:25 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/gnome-shell |
| Arguments: | n/a |
| File size: | 23168 bytes |
| MD5 hash: | da7a257239677622fe4b3a65972c9e87 |

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5609 Parent PID: 5558

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:26 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | ibus-daemon --panel disable --xim |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5857 Parent PID: 5609

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5857 Parent PID: 5609

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/ibus-memconf |
| Arguments: | /usr/libexec/ibus-memconf |
| File size: | 22904 bytes |
| MD5 hash: | 523e939905910d06598e66385761a822 |

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 5859 Parent PID: 5609

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

Analysis Process: ibus-daemon PID: 5860 Parent PID: 5859

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5860 Parent PID: 1

General

| | |
|-------------|-------------------------------------|
| Start time: | 04:22:27 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/ibus-x11 |
| Arguments: | /usr/libexec/ibus-x11 --kill-daemon |
| File size: | 100352 bytes |
| MD5 hash: | 2aa1e54666191243814c2733d6992dbd |

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: ibus-daemon PID: 6130 Parent PID: 5609

General

| | |
|-------------|----------|
| Start time: | 04:22:39 |
|-------------|----------|

| | |
|-------------|----------------------------------|
| Start date: | 10/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

File Activities

Directory Enumerated

Analysis Process: ibus-engine-simple PID: 6130 Parent PID: 5609

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/ibus-engine-simple |
| Arguments: | /usr/libexec/ibus-engine-simple |
| File size: | 14712 bytes |
| MD5 hash: | 0238866d5e8802a0ce1b1b9af8cb1376 |

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6116 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:36 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6116 Parent PID: 5455

General

| | |
|-------------|-------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:36 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-sharing |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-sharing PID: 6116 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:36 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-sharing |
| Arguments: | /usr/libexec/gsd-sharing |
| File size: | 35424 bytes |
| MD5 hash: | e29d9025d98590fbb69f89fdbd4438b3 |

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6118 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:36 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6118 Parent PID: 5455

General

| | |
|-------------|-------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-wacom |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-wacom PID: 6118 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-wacom |
| Arguments: | /usr/libexec/gsd-wacom |
| File size: | 39520 bytes |
| MD5 hash: | 13778dd1a23a4e94ddc17ac9caa4fcc1 |

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-binary PID: 6120 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6120 Parent PID: 5455

General

| | |
|-------------|-------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-color |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-color PID: 6120 Parent PID: 5455

General

| | |
|-------------|------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-color |
| Arguments: | /usr/libexec/gsd-color |
| File size: | 92832 bytes |

| | |
|-----------|--------------------------------|
| MD5 hash: | ac2861ad93ce047283e8e87cef9a19 |
|-----------|--------------------------------|

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6121 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6121 Parent PID: 5455

General

| | |
|-------------|----------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-keyboard |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-keyboard PID: 6121 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-keyboard |
| Arguments: | /usr/libexec/gsd-keyboard |
| File size: | 39760 bytes |
| MD5 hash: | 8e288fd17c80bb0a1148b964b2ac2279 |

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6122 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6122 Parent PID: 5455

General

| | |
|-------------|---------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-print-notifications |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-print-notifications PID: 6122 Parent PID: 5455

General

| | |
|-------------|--------------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | /usr/libexec/gsd-print-notifications |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

File Activities

File Read

Analysis Process: gsd-print-notifications PID: 6442 Parent PID: 6122

| General | |
|-------------|--------------------------------------|
| Start time: | 04:22:49 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | n/a |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

Analysis Process: gsd-print-notifications PID: 6443 Parent PID: 6442

| General | |
|-------------|--------------------------------------|
| Start time: | 04:22:49 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | n/a |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

File Activities

Directory Enumerated

Analysis Process: gsd-printer PID: 6443 Parent PID: 1

| General | |
|-------------|----------------------------------|
| Start time: | 04:22:49 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-printer |
| Arguments: | /usr/libexec/gsd-printer |
| File size: | 31120 bytes |
| MD5 hash: | 7995828cf98c315fd55f2ffb3b22384d |

File Activities

File Read

Analysis Process: gnome-session-binary PID: 6123 Parent PID: 5455

| General | |
|-------------|-----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6123 Parent PID: 5455

General

| | |
|-------------|--------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-rfkill |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-rfkill PID: 6123 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-rfkill |
| Arguments: | /usr/libexec/gsd-rfkill |
| File size: | 51808 bytes |
| MD5 hash: | 88a16a3c0aba1759358c06215ecfb5cc |

File Activities

File Read

Analysis Process: gnome-session-binary PID: 6124 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6124 Parent PID: 5455

General

| | |
|-------------|-----------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:38 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-smartcard |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-smartcard PID: 6124 Parent PID: 5455

General

| | |
|-------------|---------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-smartcard |
| Arguments: | /usr/libexec/gsd-smartcard |
| File size: | 109152 bytes |
| MD5 hash: | ea1fd7f62e4cd0331eae2ef754ee605 |

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6128 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:38 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6128 Parent PID: 5455

General

| | |
|-------------|----------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-datetime |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-datetime PID: 6128 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-datetime |
| Arguments: | /usr/libexec/gsd-datetime |
| File size: | 76736 bytes |
| MD5 hash: | d80d39745740de37d6634d36e344d4bc |

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6129 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6129 Parent PID: 5455

General

| | |
|-------------|----------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\$@\" sh /usr/libexec/gsd-media-keys |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-media-keys PID: 6129 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-media-keys |
| Arguments: | /usr/libexec/gsd-media-keys |
| File size: | 232936 bytes |
| MD5 hash: | a425448c135afb4b8bfd79cc0b6b74da |

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6131 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

File Activities

Directory Enumerated

Analysis Process: sh PID: 6131 Parent PID: 5455

General

| | |
|-------------|------------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:39 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"@\$@\" sh /usr/libexec/gsd-screensaver-proxy |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

File Activities

File Read

Analysis Process: gsd-screensaver-proxy PID: 6131 Parent PID: 5455

General

| | |
|-------------|------------------------------------|
| Start time: | 04:22:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-screensaver-proxy |
| Arguments: | /usr/libexec/gsd-screensaver-proxy |
| File size: | 27232 bytes |

| | |
|-----------|----------------------------------|
| MD5 hash: | 77e309450c87dceee43f1a9e50cc0d02 |
|-----------|----------------------------------|

File Activities

File Read

Analysis Process: gnome-session-binary PID: 6134 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:40 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

Analysis Process: sh PID: 6134 Parent PID: 5455

General

| | |
|-------------|-------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-sound |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: gsd-sound PID: 6134 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-sound |
| Arguments: | /usr/libexec/gsd-sound |
| File size: | 31248 bytes |
| MD5 hash: | 4c7d3fb993463337b4a0eb5c80c760ee |

Analysis Process: gnome-session-binary PID: 6137 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

Analysis Process: sh PID: 6137 Parent PID: 5455

General

| | |
|-------------|---------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:41 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-a11y-settings |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: gsd-a11y-settings PID: 6137 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:42 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-a11y-settings |
| Arguments: | /usr/libexec/gsd-a11y-settings |
| File size: | 23056 bytes |
| MD5 hash: | 18e243d2cf30ecee7ea89d1462725c5c |

Analysis Process: gnome-session-binary PID: 6139 Parent PID: 5455

General

| | |
|-------------|-----------------------------------|
| Start time: | 04:22:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

Analysis Process: sh PID: 6139 Parent PID: 5455

General

| | |
|-------------|--------------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:42 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-housekeeping |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: gsd-housekeeping PID: 6139 Parent PID: 5455

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:43 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-housekeeping |
| Arguments: | /usr/libexec/gsd-housekeeping |
| File size: | 51840 bytes |
| MD5 hash: | b55f3394a84976ddb92a2915e5d76914 |

Analysis Process: gnome-session-binary PID: 6144 Parent PID: 5455

| General | |
|-------------|-----------------------------------|
| Start time: | 04:22:42 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

Analysis Process: sh PID: 6144 Parent PID: 5455

| General | |
|-------------|-------------------------------------------------------------------------------------------------------|
| Start time: | 04:22:43 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/libexec/gsd-power |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: gsd-power PID: 6144 Parent PID: 5455

| General | |
|-------------|----------------------------------|
| Start time: | 04:22:43 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gsd-power |
| Arguments: | /usr/libexec/gsd-power |
| File size: | 88672 bytes |
| MD5 hash: | 28b8e1b43c3e7f1db6741ea1ecd978b7 |

Analysis Process: gnome-session-binary PID: 6995 Parent PID: 5455

| General | |
|-------------|-----------------------------------|
| Start time: | 04:23:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

Analysis Process: sh PID: 6995 Parent PID: 5455

| General | |
|-------------|-------------------------------------------------------------------------------------------------------|
| Start time: | 04:23:07 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh /usr/bin/spice-vdagent |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: spice-vdagent PID: 6995 Parent PID: 5455**General**

| | |
|-------------|----------------------------------|
| Start time: | 04:23:07 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/spice-vdagent |
| Arguments: | /usr/bin/spice-vdagent |
| File size: | 80664 bytes |
| MD5 hash: | 80fb7f613aa78d1b8a229dbcf4577a9d |

Analysis Process: gnome-session-binary PID: 7018 Parent PID: 5455**General**

| | |
|-------------|-----------------------------------|
| Start time: | 04:23:10 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

Analysis Process: sh PID: 7018 Parent PID: 5455**General**

| | |
|-------------|-------------------------------------------------------------------------------------------|
| Start time: | 04:23:10 |
| Start date: | 10/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=\$\$; exec \"\${@}\" sh xbrlapi -q |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: xbrlapi PID: 7018 Parent PID: 5455**General**

| | |
|-------------|----------------------------------|
| Start time: | 04:23:11 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/xbrlapi |
| Arguments: | xbrlapi -q |
| File size: | 166384 bytes |
| MD5 hash: | 0cfe25df39d38af32d6265ed947ca5b9 |

Analysis Process: gdm3 PID: 5399 Parent PID: 1320**General**

| | |
|-------------|----------------------------------|
| Start time: | 04:21:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: Default PID: 5399 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:37 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: gdm3 PID: 5400 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:37 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: Default PID: 5400 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:37 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: gdm3 PID: 5408 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:41 |
| Start date: | 10/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

Analysis Process: Default PID: 5408 Parent PID: 1320

General

| | |
|-------------|----------------------------------|
| Start time: | 04:21:41 |
| Start date: | 10/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

Analysis Process: systemd PID: 5414 Parent PID: 1860**General**

| | |
|-------------|----------------------------------|
| Start time: | 04:21:46 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: pulseaudio PID: 5414 Parent PID: 1860**General**

| | |
|-------------|---------------------------------------------------------|
| Start time: | 04:21:46 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/pulseaudio |
| Arguments: | /usr/bin/pulseaudio --daemonize=no --log-target=journal |
| File size: | 100832 bytes |
| MD5 hash: | 0c3b4c789d8ffb12b25507f27e14c186 |

Analysis Process: gvfsd-fuse PID: 5460 Parent PID: 2038**General**

| | |
|-------------|----------------------------------|
| Start time: | 04:21:59 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/gvfsd-fuse |
| Arguments: | n/a |
| File size: | 47632 bytes |
| MD5 hash: | d18fbf1cbf8eb57b17fac48b7b4be933 |

Analysis Process: fusermount PID: 5460 Parent PID: 2038**General**

| | |
|-------------|--------------------------------------------|
| Start time: | 04:21:59 |
| Start date: | 10/11/2021 |
| Path: | /bin/fusermount |
| Arguments: | fusermount -u -q -z -- /run/user/1000/gvfs |
| File size: | 39144 bytes |
| MD5 hash: | 576a1b135c82bdcbc97a91acea900566 |

Analysis Process: systemd PID: 5475 Parent PID: 1**General**

| | |
|-------------|--------------------------|
| Start time: | 04:22:01 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |

| | |
|-----------|----------------------------------|
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |
|-----------|----------------------------------|

Analysis Process: systemd-user-runtime-dir PID: 5475 Parent PID: 1

General

| | |
|-------------|-------------------------------------------------|
| Start time: | 04:22:01 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-user-runtime-dir |
| Arguments: | /lib/systemd/systemd-user-runtime-dir stop 1000 |
| File size: | 22672 bytes |
| MD5 hash: | d55f4b0847f88131dbcfb07435178e54 |

Analysis Process: systemd PID: 5583 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:26 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: systemd-localed PID: 5583 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:26 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-localed |
| Arguments: | /lib/systemd/systemd-localed |
| File size: | 43232 bytes |
| MD5 hash: | 1244af9646256d49594f2a8203329aa9 |

Analysis Process: systemd PID: 5873 Parent PID: 1334

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: pulseaudio PID: 5873 Parent PID: 1334

General

| | |
|-------------|---------------------|
| Start time: | 04:22:29 |
| Start date: | 10/11/2021 |
| Path: | /usr/bin/pulseaudio |

| | |
|------------|---------------------------------------------------------|
| Arguments: | /usr/bin/pulseaudio --daemonize=no --log-target=journal |
| File size: | 100832 bytes |
| MD5 hash: | 0c3b4c789d8ffb12b25507f27e14c186 |

Analysis Process: systemd PID: 5876 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: geoclue PID: 5876 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:31 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/geoclue |
| Arguments: | /usr/libexec/geoclue |
| File size: | 301544 bytes |
| MD5 hash: | 30ac5455f3c598dde91dc87477fb19f7 |

Analysis Process: systemd PID: 6169 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:48 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: systemd-hostnamed PID: 6169 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:22:48 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-hostnamed |
| Arguments: | /lib/systemd/systemd-hostnamed |
| File size: | 35040 bytes |
| MD5 hash: | 2cc8a5576629a2d5bd98e49a4b8bef65 |

Analysis Process: systemd PID: 6497 Parent PID: 1

General

| | |
|-------------|----------|
| Start time: | 04:23:01 |
|-------------|----------|

| | |
|-------------|----------------------------------|
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: systemd-locale PID: 6497 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:23:01 |
| Start date: | 10/11/2021 |
| Path: | /lib/systemd/systemd-locale |
| Arguments: | /lib/systemd/systemd-locale |
| File size: | 43232 bytes |
| MD5 hash: | 1244af9646256d49594f2a8203329aa9 |

Analysis Process: systemd PID: 6783 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:23:05 |
| Start date: | 10/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

Analysis Process: fprintd PID: 6783 Parent PID: 1

General

| | |
|-------------|----------------------------------|
| Start time: | 04:23:05 |
| Start date: | 10/11/2021 |
| Path: | /usr/libexec/fprintd |
| Arguments: | /usr/libexec/fprintd |
| File size: | 125312 bytes |
| MD5 hash: | b0d8829f05cd028529b84b061b660e84 |