ID: 519722
Sample Name: iKuUJ0F8Du
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:36:00
Date: 11/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report iKuUJ0F8Du 12
Overview 12
General Information 12
Detection 12
Signatures 12
Classification 12
Analysis Advice 12
General Information 12
Process Tree 12
Yara Overview 15
PCAP (Network Traffic) 15
Jbx Signature Overview 15
AV Detection: 16
Networking: 16
System Summary: 16
Persistence and Installation Behavior: 16
Hooking and other Techniques for Hiding and Protection: 16
Language, Device and Operating System Detection: 16
Stealing of Sensitive Information: 16
Remote Access Functionality: 16
Mitre Att&ck Matrix 16
Malware Configuration 17
Behavior Graph 17
Antivirus, Machine Learning and Genetic Malware Detection 17
Initial Sample 17
Dropped Files 18
Domains 18
URLs 18
Domains and IPs 18
Contacted Domains 18
URLs from Memory and Binaries 18
Contacted IPs 18
Public 18
Joe Sandbox View / Context 20
IPs 20
Domains 20
ASN 21
JA3 Fingerprints 22
Dropped Files 22
Created / dropped Files 22
Static File Info 32
General 32
Static ELF Info 32
ELF header 32
Sections 32
Program Segments 32
Network Behavior 33
TCP Packets 33
DNS Queries 33
DNS Answers 33
System Behavior 33
Analysis Process: iKuUJ0F8Du PID: 5234 Parent PID: 5117 33
General 33
File Activities 33
File Read 33
Analysis Process: iKuUJ0F8Du PID: 5236 Parent PID: 5234 33
General 33
Analysis Process: iKuUJ0F8Du PID: 5237 Parent PID: 5234 34
General 34
Analysis Process: iKuUJ0F8Du PID: 5240 Parent PID: 5237 34
General 34
File Activities 34
File Read 34
Directory Enumerated 34
Analysis Process: iKuUJ0F8Du PID: 5242 Parent PID: 5237 34
General 34
Analysis Process: iKuUJ0F8Du PID: 5244 Parent PID: 5242 34
General 34
Analysis Process: systemd PID: 5286 Parent PID: 1 34
General 34
Analysis Process: whoopsie PID: 5286 Parent PID: 1 35
General 35
File Activities 35
File Read 35
File Written 35
File Moved 35
Directory Enumerated 35

Directory Created 35
Permission Modified 35
Analysis Process: systemd PID: 5293 Parent PID: 1 35
General 35
Analysis Process: sshd PID: 5293 Parent PID: 1 35
General 35
File Activities 35
File Read 36
Directory Enumerated 36
Analysis Process: systemd PID: 5294 Parent PID: 1 36
General 36
Analysis Process: sshd PID: 5294 Parent PID: 1 36
General 36
File Activities 36
File Read 36
File Written 36
Directory Enumerated 36
Analysis Process: gdm3 PID: 5303 Parent PID: 1320 36
General 36
Analysis Process: Default PID: 5303 Parent PID: 1320 36
General 36
File Activities 37
File Read 37
Analysis Process: gdm3 PID: 5306 Parent PID: 1320 37
General 37
Analysis Process: Default PID: 5306 Parent PID: 1320 37
General 37
File Activities 37
File Read 37
Analysis Process: systemd PID: 5307 Parent PID: 1 37
General 37
Analysis Process: accounts-daemon PID: 5307 Parent PID: 1 37
General 37
File Activities 37
File Read 38
File Written 38
File Moved 38
Directory Enumerated 38
Directory Created 38
Permission Modified 38
Analysis Process: accounts-daemon PID: 5322 Parent PID: 5307 38
General 38
File Activities 38
Directory Enumerated 38
Analysis Process: language-validate PID: 5322 Parent PID: 5307 38
General 38
File Activities 38
File Read 38
Analysis Process: language-validate PID: 5323 Parent PID: 5322 38
General 38
Analysis Process: language-options PID: 5323 Parent PID: 5322 39
General 39
File Activities 39
File Read 39
Directory Enumerated 39
Analysis Process: language-options PID: 5324 Parent PID: 5323 39
General 39
Analysis Process: sh PID: 5324 Parent PID: 5323 39
General 39
File Activities 39
File Read 39
Analysis Process: sh PID: 5325 Parent PID: 5324 39
General 39
Analysis Process: locale PID: 5325 Parent PID: 5324 40
General 40
File Activities 40
File Read 40
Directory Enumerated 40
Analysis Process: sh PID: 5326 Parent PID: 5324 40
General 40
Analysis Process: grep PID: 5326 Parent PID: 5324 40
General 40
File Activities 40
File Read 40
Analysis Process: gdm3 PID: 5327 Parent PID: 1320 40
General 40
Analysis Process: gdm-session-worker PID: 5327 Parent PID: 1320 41
General 41
File Activities 41
File Read 41
File Written 41
Directory Enumerated 41
Analysis Process: gdm-session-worker PID: 5333 Parent PID: 5327 41
General 41
Analysis Process: gdm-wayland-session PID: 5333 Parent PID: 5327 41
General 41
File Activities 41
File Read 41
Analysis Process: gdm-wayland-session PID: 5336 Parent PID: 5333 41
General 41
File Activities 42
Directory Enumerated 42
Analysis Process: dbus-run-session PID: 5336 Parent PID: 5333 42
General 42
File Activities 42
File Read 42

Analysis Process: dbus-run-session PID: 5337 Parent PID: 5336 42
General 42
Analysis Process: dbus-daemon PID: 5337 Parent PID: 5336 42
General 42
File Activities 42
File Read 42
Directory Enumerated 42
Directory Created 42
Analysis Process: dbus-daemon PID: 5341 Parent PID: 5337 42
General 42
Analysis Process: dbus-daemon PID: 5342 Parent PID: 5341 43
General 43
File Activities 43
File Written 43
Analysis Process: false PID: 5342 Parent PID: 5341 43
General 43
File Activities 43
File Read 43
Analysis Process: dbus-daemon PID: 5344 Parent PID: 5337 43
General 43
Analysis Process: dbus-daemon PID: 5345 Parent PID: 5344 43
General 43
File Activities 44
File Written 44
Analysis Process: false PID: 5345 Parent PID: 5344 44
General 44
File Activities 44
File Read 44
Analysis Process: dbus-daemon PID: 5346 Parent PID: 5337 44
General 44
Analysis Process: dbus-daemon PID: 5347 Parent PID: 5346 44
General 44
File Activities 44
File Written 44
Analysis Process: false PID: 5347 Parent PID: 5346 44
General 44
File Activities 45
File Read 45
Analysis Process: dbus-daemon PID: 5348 Parent PID: 5337 45
General 45
Analysis Process: dbus-daemon PID: 5349 Parent PID: 5348 45
General 45
File Activities 45
File Written 45
Analysis Process: false PID: 5349 Parent PID: 5348 45
General 45
File Activities 45
File Read 45
Analysis Process: dbus-daemon PID: 5350 Parent PID: 5337 45
General 45
Analysis Process: dbus-daemon PID: 5351 Parent PID: 5350 46
General 46
File Activities 46
File Written 46
Analysis Process: false PID: 5351 Parent PID: 5350 46
General 46
File Activities 46
File Read 46
Analysis Process: dbus-daemon PID: 5352 Parent PID: 5337 46
General 46
Analysis Process: dbus-daemon PID: 5353 Parent PID: 5352 46
General 46
File Activities 47
File Written 47
Analysis Process: false PID: 5353 Parent PID: 5352 47
General 47
File Activities 47
File Read 47
Analysis Process: dbus-daemon PID: 5355 Parent PID: 5337 47
General 47
Analysis Process: dbus-daemon PID: 5356 Parent PID: 5355 47
General 47
File Activities 47
File Written 47
Analysis Process: false PID: 5356 Parent PID: 5355 47
General 47
File Activities 48
File Read 48
Analysis Process: dbus-run-session PID: 5338 Parent PID: 5336 48
General 48
Analysis Process: gnome-session PID: 5338 Parent PID: 5336 48
General 48
File Activities 48
File Read 48
Analysis Process: gnome-session-binary PID: 5338 Parent PID: 5336 48
General 48
File Activities 48
File Created 48
File Deleted 48
File Read 48
File Written 48
Directory Enumerated 49
Directory Created 49
Link Created 49

Analysis Process: gnome-session-binary PID: 5357 Parent PID: 5338 49
General 49
File Activities 49
Directory Enumerated 49
Analysis Process: session-migration PID: 5357 Parent PID: 5338 49
General 49
File Activities 49
File Read 49
Analysis Process: gnome-session-binary PID: 5358 Parent PID: 5338 49
General 49
File Activities 49
Directory Enumerated 49
Analysis Process: sh PID: 5358 Parent PID: 5338 49
General 50
File Activities 50
File Read 50
Analysis Process: gnome-shell PID: 5358 Parent PID: 5338 50
General 50
File Activities 50
File Read 50
Directory Enumerated 50
Analysis Process: gdm3 PID: 5386 Parent PID: 1320 50
General 50
Analysis Process: gdm-session-worker PID: 5386 Parent PID: 1320 50
General 50
File Activities 50
File Read 50
File Written 50
Directory Enumerated 51
Analysis Process: gdm-session-worker PID: 5391 Parent PID: 5386 51
General 51
Analysis Process: gdm-x-session PID: 5391 Parent PID: 5386 51
General 51
File Activities 51
File Read 51
File Written 51
Directory Created 51
Analysis Process: gdm-x-session PID: 5393 Parent PID: 5391 51
General 51
File Activities 51
Directory Enumerated 51
Analysis Process: Xorg PID: 5393 Parent PID: 5391 51
General 51
File Activities 52
File Read 52
Analysis Process: Xorg.wrap PID: 5393 Parent PID: 5391 52
General 52
File Activities 52
File Read 52
Analysis Process: Xorg PID: 5393 Parent PID: 5391 52
General 52
File Activities 52
File Deleted 52
File Read 52
File Written 52
File Moved 52
Directory Enumerated 52
Analysis Process: Xorg PID: 5427 Parent PID: 5393 52
General 52
Analysis Process: sh PID: 5427 Parent PID: 5393 53
General 53
File Activities 53
File Read 53
Analysis Process: sh PID: 5428 Parent PID: 5427 53
General 53
Analysis Process: xkbcomp PID: 5428 Parent PID: 5427 53
General 53
File Activities 53
File Deleted 53
File Read 53
File Written 53
Analysis Process: Xorg PID: 5849 Parent PID: 5393 53
General 53
Analysis Process: sh PID: 5849 Parent PID: 5393 54
General 54
File Activities 54
File Read 54
Analysis Process: sh PID: 5850 Parent PID: 5849 54
General 54
Analysis Process: xkbcomp PID: 5850 Parent PID: 5849 54
General 54
File Activities 54
File Deleted 54
File Read 54
File Written 54
Analysis Process: gdm-x-session PID: 5437 Parent PID: 5391 54
General 54
File Activities 55
Directory Enumerated 55
Analysis Process: Default PID: 5437 Parent PID: 5391 55
General 55
File Activities 55
File Read 55
Analysis Process: gdm-x-session PID: 5438 Parent PID: 5391 55
General 55
File Activities 55

Directory Enumerated 55
Analysis Process: dbus-run-session PID: 5438 Parent PID: 5391 55
General 55
File Activities 55
File Read 56
Analysis Process: dbus-run-session PID: 5439 Parent PID: 5438 56
General 56
Analysis Process: dbus-daemon PID: 5439 Parent PID: 5438 56
General 56
File Activities 56
File Read 56
Directory Enumerated 56
Directory Created 56
Analysis Process: dbus-daemon PID: 5495 Parent PID: 5439 56
General 56
Analysis Process: dbus-daemon PID: 5496 Parent PID: 5495 56
General 56
File Activities 57
File Written 57
Analysis Process: at-spi-bus-launcher PID: 5496 Parent PID: 5495 57
General 57
File Activities 57
File Read 57
File Written 57
Directory Enumerated 57
Directory Created 57
Analysis Process: at-spi-bus-launcher PID: 5501 Parent PID: 5496 57
General 57
File Activities 57
Directory Enumerated 57
Analysis Process: dbus-daemon PID: 5501 Parent PID: 5496 57
General 57
File Activities 57
File Read 57
Directory Enumerated 58
Analysis Process: dbus-daemon PID: 5879 Parent PID: 5501 58
General 58
Analysis Process: dbus-daemon PID: 5883 Parent PID: 5879 58
General 58
File Activities 58
File Written 58
Analysis Process: at-spi2-registryd PID: 5883 Parent PID: 5879 58
General 58
File Activities 58
File Read 58
Analysis Process: dbus-daemon PID: 5525 Parent PID: 5439 58
General 58
Analysis Process: dbus-daemon PID: 5526 Parent PID: 5525 59
General 59
File Activities 59
File Written 59
Analysis Process: false PID: 5526 Parent PID: 5525 59
General 59
File Activities 59
File Read 59
Analysis Process: dbus-daemon PID: 5528 Parent PID: 5439 59
General 59
Analysis Process: dbus-daemon PID: 5529 Parent PID: 5528 59
General 59
File Activities 59
File Written 59
Analysis Process: false PID: 5529 Parent PID: 5528 60
General 60
File Activities 60
File Read 60
Analysis Process: dbus-daemon PID: 5530 Parent PID: 5439 60
General 60
Analysis Process: dbus-daemon PID: 5531 Parent PID: 5530 60
General 60
File Activities 60
File Written 60
Analysis Process: false PID: 5531 Parent PID: 5530 60
General 60
File Activities 60
File Read 61
Analysis Process: dbus-daemon PID: 5532 Parent PID: 5439 61
General 61
Analysis Process: dbus-daemon PID: 5533 Parent PID: 5532 61
General 61
File Activities 61
File Written 61
Analysis Process: false PID: 5533 Parent PID: 5532 61
General 61
File Activities 61
File Read 61
Analysis Process: dbus-daemon PID: 5534 Parent PID: 5439 61
General 61
Analysis Process: dbus-daemon PID: 5535 Parent PID: 5534 62
General 62
File Activities 62
File Written 62
Analysis Process: false PID: 5535 Parent PID: 5534 62
General 62
File Activities 62
File Read 62

Analysis Process: dbus-daemon PID: 5536 Parent PID: 5439 62
General 62
Analysis Process: dbus-daemon PID: 5537 Parent PID: 5536 62
General 62
File Activities 62
File Written 62
Analysis Process: false PID: 5537 Parent PID: 5536 63
General 63
File Activities 63
File Read 63
Analysis Process: dbus-daemon PID: 5539 Parent PID: 5439 63
General 63
Analysis Process: dbus-daemon PID: 5540 Parent PID: 5539 63
General 63
File Activities 63
File Written 63
Analysis Process: false PID: 5540 Parent PID: 5539 63
General 63
File Activities 63
File Read 64
Analysis Process: dbus-daemon PID: 5845 Parent PID: 5439 64
General 64
Analysis Process: dbus-daemon PID: 5846 Parent PID: 5845 64
General 64
File Activities 64
File Written 64
Analysis Process: ibus-portal PID: 5846 Parent PID: 5845 64
General 64
File Activities 64
File Read 64
Directory Enumerated 64
Directory Created 64
Analysis Process: dbus-daemon PID: 6079 Parent PID: 5439 64
General 64
Analysis Process: dbus-daemon PID: 6080 Parent PID: 6079 65
General 65
File Activities 65
File Written 65
Analysis Process: gjs PID: 6080 Parent PID: 6079 65
General 65
File Activities 65
File Read 65
Directory Enumerated 65
Analysis Process: dbus-daemon PID: 6142 Parent PID: 5439 65
General 65
Analysis Process: dbus-daemon PID: 6143 Parent PID: 6142 65
General 65
File Activities 66
File Written 66
Analysis Process: false PID: 6143 Parent PID: 6142 66
General 66
File Activities 66
File Read 66
Analysis Process: dbus-run-session PID: 5440 Parent PID: 5438 66
General 66
Analysis Process: gnome-session PID: 5440 Parent PID: 5438 66
General 66
File Activities 66
File Read 66
Analysis Process: gnome-session-binary PID: 5440 Parent PID: 5438 66
General 66
File Activities 67
File Created 67
File Deleted 67
File Read 67
File Written 67
Directory Enumerated 67
Directory Created 67
Link Created 67
Analysis Process: gnome-session-binary PID: 5441 Parent PID: 5440 67
General 67
File Activities 67
Directory Enumerated 67
Analysis Process: gnome-session-check-accelerated PID: 5441 Parent PID: 5440 67
General 67
File Activities 67
File Read 67
Directory Enumerated 67
Analysis Process: gnome-session-check-accelerated PID: 5502 Parent PID: 5441 67
General 68
File Activities 68
Directory Enumerated 68
Analysis Process: gnome-session-check-accelerated-gl-helper PID: 5502 Parent PID: 5441 68
General 68
File Activities 68
File Read 68
Directory Enumerated 68
Analysis Process: gnome-session-check-accelerated PID: 5512 Parent PID: 5441 68
General 68
File Activities 68
Directory Enumerated 68
Analysis Process: gnome-session-check-accelerated-gles-helper PID: 5512 Parent PID: 5441 68
General 68
File Activities 69
File Read 69
Directory Enumerated 69

Analysis Process: gnome-session-binary PID: 5541 Parent PID: 5440 69
General 69
File Activities 69
Directory Enumerated 69
Analysis Process: session-migration PID: 5541 Parent PID: 5440 69
General 69
File Activities 69
File Read 69
Analysis Process: gnome-session-binary PID: 5542 Parent PID: 5440 69
General 69
File Activities 69
Directory Enumerated 69
Analysis Process: sh PID: 5542 Parent PID: 5440 70
General 70
File Activities 70
File Read 70
Analysis Process: gnome-shell PID: 5542 Parent PID: 5440 70
General 70
File Activities 70
File Deleted 70
File Read 70
File Written 70
Directory Enumerated 70
Directory Created 70
Analysis Process: gnome-shell PID: 5797 Parent PID: 5542 70
General 70
File Activities 70
Directory Enumerated 70
Analysis Process: ibus-daemon PID: 5797 Parent PID: 5542 70
General 71
File Activities 71
File Deleted 71
File Read 71
File Written 71
Directory Enumerated 71
Directory Created 71
Analysis Process: ibus-daemon PID: 5841 Parent PID: 5797 71
General 71
File Activities 71
Directory Enumerated 71
Analysis Process: ibus-memconf PID: 5841 Parent PID: 5797 71
General 71
File Activities 71
File Read 71
Directory Enumerated 71
Directory Created 71
Analysis Process: ibus-daemon PID: 5843 Parent PID: 5797 72
General 72
Analysis Process: ibus-daemon PID: 5844 Parent PID: 5843 72
General 72
File Activities 72
Directory Enumerated 72
Analysis Process: ibus-x11 PID: 5844 Parent PID: 1 72
General 72
File Activities 72
File Read 72
Directory Enumerated 72
Directory Created 72
Analysis Process: ibus-daemon PID: 6114 Parent PID: 5797 72
General 72
File Activities 73
Directory Enumerated 73
Analysis Process: ibus-engine-simple PID: 6114 Parent PID: 5797 73
General 73
File Activities 73
File Read 73
Directory Enumerated 73
Directory Created 73
Analysis Process: gnome-session-binary PID: 6098 Parent PID: 5440 73
General 73
File Activities 73
Directory Enumerated 73
Analysis Process: sh PID: 6098 Parent PID: 5440 73
General 73
File Activities 73
File Read 73
Analysis Process: gsd-sharing PID: 6098 Parent PID: 5440 74
General 74
File Activities 74
File Read 74
File Written 74
Directory Enumerated 74
Directory Created 74
Analysis Process: gnome-session-binary PID: 6100 Parent PID: 5440 74
General 74
File Activities 74
Directory Enumerated 74
Analysis Process: sh PID: 6100 Parent PID: 5440 74
General 74
File Activities 74
File Read 74
Analysis Process: gsd-wacom PID: 6100 Parent PID: 5440 74
General 74
File Activities 75
File Read 75
Directory Enumerated 75
Analysis Process: gnome-session-binary PID: 6102 Parent PID: 5440 75
General 75

File Activities 75
Directory Enumerated 75
Analysis Process: sh PID: 6102 Parent PID: 5440 75
General 75
File Activities 75
File Read 75
Analysis Process: gsd-color PID: 6102 Parent PID: 5440 75
General 75
File Activities 75
File Read 76
File Written 76
Directory Enumerated 76
Directory Created 76
Analysis Process: gnome-session-binary PID: 6103 Parent PID: 5440 76
General 76
File Activities 76
Directory Enumerated 76
Analysis Process: sh PID: 6103 Parent PID: 5440 76
General 76
File Activities 76
File Read 76
Analysis Process: gsd-keyboard PID: 6103 Parent PID: 5440 76
General 76
File Activities 76
File Read 76
File Written 76
Directory Enumerated 77
Directory Created 77
Analysis Process: gnome-session-binary PID: 6105 Parent PID: 5440 77
General 77
File Activities 77
Directory Enumerated 77
Analysis Process: sh PID: 6105 Parent PID: 5440 77
General 77
File Activities 77
File Read 77
Analysis Process: gsd-print-notifications PID: 6105 Parent PID: 5440 77
General 77
File Activities 77
File Read 77
Analysis Process: gsd-print-notifications PID: 6421 Parent PID: 6105 77
General 77
Analysis Process: gsd-print-notifications PID: 6422 Parent PID: 6421 78
General 78
File Activities 78
Directory Enumerated 78
Analysis Process: gsd-printer PID: 6422 Parent PID: 1 78
General 78
File Activities 78
File Read 78
Analysis Process: gnome-session-binary PID: 6106 Parent PID: 5440 78
General 78
File Activities 78
Directory Enumerated 78
Analysis Process: sh PID: 6106 Parent PID: 5440 78
General 79
File Activities 79
File Read 79
Analysis Process: gsd-rfkill PID: 6106 Parent PID: 5440 79
General 79
File Activities 79
File Read 79
Analysis Process: gnome-session-binary PID: 6108 Parent PID: 5440 79
General 79
File Activities 79
Directory Enumerated 79
Analysis Process: sh PID: 6108 Parent PID: 5440 79
General 79
File Activities 79
File Read 80
Analysis Process: gsd-smartcard PID: 6108 Parent PID: 5440 80
General 80
File Activities 80
File Read 80
File Written 80
Directory Enumerated 80
Directory Created 80
Analysis Process: gnome-session-binary PID: 6111 Parent PID: 5440 80
General 80
File Activities 80
Directory Enumerated 80
Analysis Process: sh PID: 6111 Parent PID: 5440 80
General 80
File Activities 80
File Read 80
Analysis Process: gsd-datetime PID: 6111 Parent PID: 5440 81
General 81
File Activities 81
File Read 81
File Written 81
Directory Enumerated 81
Directory Created 81
Analysis Process: gnome-session-binary PID: 6112 Parent PID: 5440 81
General 81
File Activities 81
Directory Enumerated 81
Analysis Process: sh PID: 6112 Parent PID: 5440 81

General 81
File Activities 81
File Read 81
Analysis Process: gsd-media-keys PID: 6112 Parent PID: 5440 81
General 81
File Activities 82
File Read 82
File Written 82
Directory Enumerated 82
Directory Created 82
Analysis Process: gnome-session-binary PID: 6113 Parent PID: 5440 82
General 82
File Activities 82
Directory Enumerated 82
Analysis Process: sh PID: 6113 Parent PID: 5440 82
General 82
File Activities 82
File Read 82
Analysis Process: gsd-screensaver-proxy PID: 6113 Parent PID: 5440 82
General 82
File Activities 83
File Read 83
Analysis Process: gnome-session-binary PID: 6117 Parent PID: 5440 83
General 83
File Activities 83
Directory Enumerated 83
Analysis Process: sh PID: 6117 Parent PID: 5440 83
General 83
File Activities 83
File Read 83
Analysis Process: gsd-sound PID: 6117 Parent PID: 5440 83
General 83
File Activities 83
File Read 83
Analysis Process: gnome-session-binary PID: 6118 Parent PID: 5440 83
General 84
Analysis Process: sh PID: 6118 Parent PID: 5440 84
General 84
Analysis Process: gsd-a11y-settings PID: 6118 Parent PID: 5440 84
General 84
Analysis Process: gnome-session-binary PID: 6120 Parent PID: 5440 84
General 84
Analysis Process: sh PID: 6120 Parent PID: 5440 84
General 84
Analysis Process: gsd-housekeeping PID: 6120 Parent PID: 5440 85
General 85
Analysis Process: gnome-session-binary PID: 6123 Parent PID: 5440 85
General 85
Analysis Process: sh PID: 6123 Parent PID: 5440 85
General 85
Analysis Process: gsd-power PID: 6123 Parent PID: 5440 85
General 85
Analysis Process: gnome-session-binary PID: 6964 Parent PID: 5440 85
General 85
Analysis Process: sh PID: 6964 Parent PID: 5440 86
General 86
Analysis Process: spice-vdagent PID: 6964 Parent PID: 5440 86
General 86
Analysis Process: gnome-session-binary PID: 6971 Parent PID: 5440 86
General 86
Analysis Process: sh PID: 6971 Parent PID: 5440 86
General 86
Analysis Process: xbrlapi PID: 6971 Parent PID: 5440 86
General 86
Analysis Process: gdm3 PID: 5387 Parent PID: 1320 87
General 87
Analysis Process: Default PID: 5387 Parent PID: 1320 87
General 87
Analysis Process: gdm3 PID: 5388 Parent PID: 1320 87
General 87
Analysis Process: Default PID: 5388 Parent PID: 1320 87
General 87
Analysis Process: gdm3 PID: 5396 Parent PID: 1320 87
General 87
Analysis Process: Default PID: 5396 Parent PID: 1320 88
General 88
Analysis Process: systemd PID: 5422 Parent PID: 1860 88
General 88
Analysis Process: pulseaudio PID: 5422 Parent PID: 1860 88
General 88
Analysis Process: gvfsd-fuse PID: 5443 Parent PID: 2038 88
General 88
Analysis Process: fusermount PID: 5443 Parent PID: 2038 88
General 88
Analysis Process: systemd PID: 5458 Parent PID: 1 89
General 89
Analysis Process: systemd-user-runtime-dir PID: 5458 Parent PID: 1 89
General 89
Analysis Process: systemd PID: 5567 Parent PID: 1 89
General 89

Analysis Process: systemd-localed PID: 5567 Parent PID: 1 89
General 89
Analysis Process: systemd PID: 5856 Parent PID: 1334 89
General 89
Analysis Process: pulseaudio PID: 5856 Parent PID: 1334 90
General 90
Analysis Process: systemd PID: 5859 Parent PID: 1 90
General 90
Analysis Process: geoclue PID: 5859 Parent PID: 1 90
General 90
Analysis Process: systemd PID: 6148 Parent PID: 1 90
General 90
Analysis Process: systemd-hostnamed PID: 6148 Parent PID: 1 90
General 90
Analysis Process: systemd PID: 6484 Parent PID: 1 91
General 91
Analysis Process: systemd-localed PID: 6484 Parent PID: 1 91
General 91
Analysis Process: systemd PID: 6753 Parent PID: 1 91
General 91
Analysis Process: fprintd PID: 6753 Parent PID: 1 91
General 91

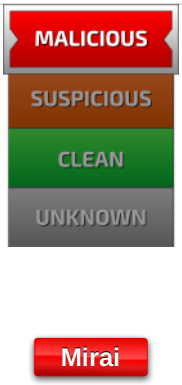
Linux Analysis Report iKuUJ0F8Du

Overview

General Information

Sample Name:	iKuUJ0F8Du
Analysis ID:	519722
MD5:	5d0d54974ca6c1..
SHA1:	00bdfd4f35dd30e..
SHA256:	8126a9a1a56257..
Tags:	32 elf mirai renesas
Infos:	

Detection

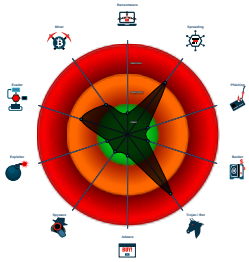


Score:	80
Range:	0 - 100
Whitelisted:	false

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...
- Uses known network protocols on no...
- Sample reads /proc/mounts (often u...
- Reads CPU information from /sys in...
- Executes the "grep" command used...
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Detected TCP or UDP traffic on non...

Classification



Analysis Advice

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:	519722
Start date:	11.11.2021
Start time:	04:36:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iKuUJ0F8Du
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:	mal80.spre.troj.lin@0/51@3/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- iKuUJ0F8Du (PID: 5234, Parent: 5117, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/iKuUJ0F8Du
  - iKuUJ0F8Du New Fork (PID: 5236, Parent: 5234)
  - iKuUJ0F8Du New Fork (PID: 5237, Parent: 5234)
    - iKuUJ0F8Du New Fork (PID: 5240, Parent: 5237)
    - iKuUJ0F8Du New Fork (PID: 5242, Parent: 5237)
      - iKuUJ0F8Du New Fork (PID: 5244, Parent: 5242)
- systemd New Fork (PID: 5286, Parent: 1)
  - whoopsie (PID: 5286, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5293, Parent: 1)
  - sshd (PID: 5293, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t

- systemd New Fork (PID: 5294, Parent: 1)
  - sshd (PID: 5294, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5303, Parent: 1320)
  - Default (PID: 5303, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5306, Parent: 1320)
  - Default (PID: 5306, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5307, Parent: 1)
  - accounts-daemon (PID: 5307, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5322, Parent: 5307)
    - language-validate (PID: 5322, Parent: 5307, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
      - language-validate New Fork (PID: 5323, Parent: 5322)
      - language-options (PID: 5323, Parent: 5322, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
        - language-options New Fork (PID: 5324, Parent: 5323)
        - sh (PID: 5324, Parent: 5323, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
          - sh New Fork (PID: 5325, Parent: 5324)
          - locale (PID: 5325, Parent: 5324, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
          - sh New Fork (PID: 5326, Parent: 5324)
          - grep (PID: 5326, Parent: 5324, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm3 New Fork (PID: 5327, Parent: 1320)
  - gdm-session-worker (PID: 5327, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5333, Parent: 5327)
    - gdm-wayland-session (PID: 5333, Parent: 5327, MD5: d3def63cf1e83f7fb8a0f13b1744ff7c) Arguments: /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
      - gdm-wayland-session New Fork (PID: 5336, Parent: 5333)
      - dbus-run-session (PID: 5336, Parent: 5333, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5337, Parent: 5336)
        - dbus-daemon (PID: 5337, Parent: 5336, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
          - dbus-daemon New Fork (PID: 5341, Parent: 5337)
            - dbus-daemon New Fork (PID: 5342, Parent: 5341)
            - false (PID: 5342, Parent: 5341, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5344, Parent: 5337)
            - dbus-daemon New Fork (PID: 5345, Parent: 5344)
            - false (PID: 5345, Parent: 5344, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5346, Parent: 5337)
            - dbus-daemon New Fork (PID: 5347, Parent: 5346)
            - false (PID: 5347, Parent: 5346, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5348, Parent: 5337)
            - dbus-daemon New Fork (PID: 5349, Parent: 5348)
            - false (PID: 5349, Parent: 5348, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5350, Parent: 5337)
            - dbus-daemon New Fork (PID: 5351, Parent: 5350)
            - false (PID: 5351, Parent: 5350, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5352, Parent: 5337)
            - dbus-daemon New Fork (PID: 5353, Parent: 5352)
            - false (PID: 5353, Parent: 5352, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5355, Parent: 5337)
            - dbus-daemon New Fork (PID: 5356, Parent: 5355)
            - false (PID: 5356, Parent: 5355, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-run-session New Fork (PID: 5338, Parent: 5336)
        - gnome-session (PID: 5338, Parent: 5336, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary (PID: 5338, Parent: 5336, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
          - gnome-session-binary New Fork (PID: 5357, Parent: 5338)
          - session-migration (PID: 5357, Parent: 5338, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
          - gnome-session-binary New Fork (PID: 5358, Parent: 5338)
          - sh (PID: 5358, Parent: 5338, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
          - gnome-shell (PID: 5358, Parent: 5338, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5386, Parent: 1320)
  - gdm-session-worker (PID: 5386, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5391, Parent: 5386)
    - gdm-x-session (PID: 5391, Parent: 5386, 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: 5393, Parent: 5391)
      - Xorg (PID: 5393, Parent: 5391, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg.wrap (PID: 5393, Parent: 5391, MD5: 48993830888200ecf19dd7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg (PID: 5393, Parent: 5391, MD5: 730cf4c45a7ee8bea88abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
        - Xorg New Fork (PID: 5427, Parent: 5393)
        - sh (PID: 5427, Parent: 5393, 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: 5428, Parent: 5427)
          - xkbcomp (PID: 5428, Parent: 5427, 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: 5849, Parent: 5393)
        - sh (PID: 5849, Parent: 5393, 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: 5850, Parent: 5849)
          - xkbcomp (PID: 5850, Parent: 5849, 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: 5437, Parent: 5391)
      - Default (PID: 5437, Parent: 5391, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
      - gdm-x-session New Fork (PID: 5438, Parent: 5391)
      - dbus-run-session (PID: 5438, Parent: 5391, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5439, Parent: 5438)
        - dbus-daemon (PID: 5439, Parent: 5438, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session

- dbus-daemon New Fork (PID: 5495, Parent: 5439)
  - dbus-daemon New Fork (PID: 5496, Parent: 5495)
  - at-spi-bus-launcher (PID: 5496, Parent: 5495, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
    - at-spi-bus-launcher New Fork (PID: 5501, Parent: 5496)
    - dbus-daemon (PID: 5501, Parent: 5496, 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: 5879, Parent: 5501)
        - dbus-daemon New Fork (PID: 5883, Parent: 5879)
        - at-spi2-registryd (PID: 5883, Parent: 5879, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
- dbus-daemon New Fork (PID: 5525, Parent: 5439)
  - dbus-daemon New Fork (PID: 5526, Parent: 5525)
  - false (PID: 5526, Parent: 5525, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5528, Parent: 5439)
  - dbus-daemon New Fork (PID: 5529, Parent: 5528)
  - false (PID: 5529, Parent: 5528, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5530, Parent: 5439)
  - dbus-daemon New Fork (PID: 5531, Parent: 5530)
  - false (PID: 5531, Parent: 5530, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5532, Parent: 5439)
  - dbus-daemon New Fork (PID: 5533, Parent: 5532)
  - false (PID: 5533, Parent: 5532, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5534, Parent: 5439)
  - dbus-daemon New Fork (PID: 5535, Parent: 5534)
  - false (PID: 5535, Parent: 5534, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5536, Parent: 5439)
  - dbus-daemon New Fork (PID: 5537, Parent: 5536)
  - false (PID: 5537, Parent: 5536, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5539, Parent: 5439)
  - dbus-daemon New Fork (PID: 5540, Parent: 5539)
  - false (PID: 5540, Parent: 5539, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
- dbus-daemon New Fork (PID: 5845, Parent: 5439)
  - dbus-daemon New Fork (PID: 5846, Parent: 5845)
  - ibus-portal (PID: 5846, Parent: 5845, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
- dbus-daemon New Fork (PID: 6079, Parent: 5439)
  - dbus-daemon New Fork (PID: 6080, Parent: 6079)
  - gjs (PID: 6080, Parent: 6079, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
- dbus-daemon New Fork (PID: 6142, Parent: 5439)
  - dbus-daemon New Fork (PID: 6143, Parent: 6142)
  - false (PID: 6143, Parent: 6142, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false

- dbus-run-session New Fork (PID: 5440, Parent: 5438)
- gnome-session (PID: 5440, Parent: 5438, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
- gnome-session-binary (PID: 5440, Parent: 5438, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
  - gnome-session-binary New Fork (PID: 5441, Parent: 5440)
  - gnome-session-check-accelerated (PID: 5441, Parent: 5440, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
    - gnome-session-check-accelerated New Fork (PID: 5502, Parent: 5441)
    - gnome-session-check-accelerated-gl-helper (PID: 5502, Parent: 5441, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
    - gnome-session-check-accelerated New Fork (PID: 5512, Parent: 5441)
    - gnome-session-check-accelerated-gles-helper (PID: 5512, Parent: 5441, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
  - gnome-session-binary New Fork (PID: 5541, Parent: 5440)
  - session-migration (PID: 5541, Parent: 5440, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
  - gnome-session-binary New Fork (PID: 5542, Parent: 5440)
  - sh (PID: 5542, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
  - gnome-shell (PID: 5542, Parent: 5440, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
    - gnome-shell New Fork (PID: 5797, Parent: 5542)
    - ibus-daemon (PID: 5797, Parent: 5542, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
      - ibus-daemon New Fork (PID: 5841, Parent: 5797)
      - ibus-memconf (PID: 5841, Parent: 5797, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
      - ibus-daemon New Fork (PID: 5843, Parent: 5797)
        - ibus-daemon New Fork (PID: 5844, Parent: 5843)
        - ibus-x11 (PID: 5844, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
      - ibus-daemon New Fork (PID: 6114, Parent: 5797)
      - ibus-engine-simple (PID: 6114, Parent: 5797, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
  - gnome-session-binary New Fork (PID: 6098, Parent: 5440)
  - sh (PID: 6098, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
  - gsd-sharing (PID: 6098, Parent: 5440, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
  - gnome-session-binary New Fork (PID: 6100, Parent: 5440)
  - sh (PID: 6100, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
  - gsd-wacom (PID: 6100, Parent: 5440, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
  - gnome-session-binary New Fork (PID: 6102, Parent: 5440)
  - sh (PID: 6102, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
  - gsd-color (PID: 6102, Parent: 5440, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
  - gnome-session-binary New Fork (PID: 6103, Parent: 5440)
  - sh (PID: 6103, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
  - gsd-keyboard (PID: 6103, Parent: 5440, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
  - gnome-session-binary New Fork (PID: 6105, Parent: 5440)
  - sh (PID: 6105, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6105, Parent: 5440, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6421, Parent: 6105)
      - gsd-print-notifications New Fork (PID: 6422, Parent: 6421)
      - gsd-printer (PID: 6422, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer

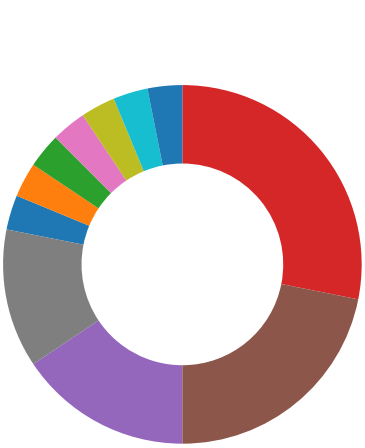
- gnome-session-binary New Fork (PID: 6106, Parent: 5440)
  - sh (PID: 6106, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
  - gsd-rfkill (PID: 6106, Parent: 5440, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6108, Parent: 5440)
  - sh (PID: 6108, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
  - gsd-smartcard (PID: 6108, Parent: 5440, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6111, Parent: 5440)
  - sh (PID: 6111, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
  - gsd-datetime (PID: 6111, Parent: 5440, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6112, Parent: 5440)
  - sh (PID: 6112, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
  - gsd-media-keys (PID: 6112, Parent: 5440, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6113, Parent: 5440)
  - sh (PID: 6113, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
  - gsd-screensaver-proxy (PID: 6113, Parent: 5440, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6117, Parent: 5440)
  - sh (PID: 6117, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
  - gsd-sound (PID: 6117, Parent: 5440, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6118, Parent: 5440)
  - sh (PID: 6118, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
  - gsd-a11y-settings (PID: 6118, Parent: 5440, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6120, Parent: 5440)
  - sh (PID: 6120, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
  - gsd-housekeeping (PID: 6120, Parent: 5440, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6123, Parent: 5440)
  - sh (PID: 6123, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
  - gsd-power (PID: 6123, Parent: 5440, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6964, Parent: 5440)
  - sh (PID: 6964, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
  - spice-vdagent (PID: 6964, Parent: 5440, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 6971, Parent: 5440)
  - sh (PID: 6971, Parent: 5440, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
  - xbrlapi (PID: 6971, Parent: 5440, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q
- gdm3 New Fork (PID: 5387, Parent: 1320)
  - Default (PID: 5387, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5388, Parent: 1320)
  - Default (PID: 5388, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5396, Parent: 1320)
  - Default (PID: 5396, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5422, Parent: 1860)
  - pulseaudio (PID: 5422, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- gvfsd-fuse New Fork (PID: 5443, Parent: 2038)
  - fusermount (PID: 5443, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5458, Parent: 1)
  - systemd-user-runtime-dir (PID: 5458, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5567, Parent: 1)
  - systemd-localed (PID: 5567, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5856, Parent: 1334)
  - pulseaudio (PID: 5856, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5859, Parent: 1)
  - geoclue (PID: 5859, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6148, Parent: 1)
  - systemd-hostnamed (PID: 6148, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6484, Parent: 1)
  - systemd-localed (PID: 6484, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 6753, Parent: 1)
  - fprintd (PID: 6753, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



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)

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

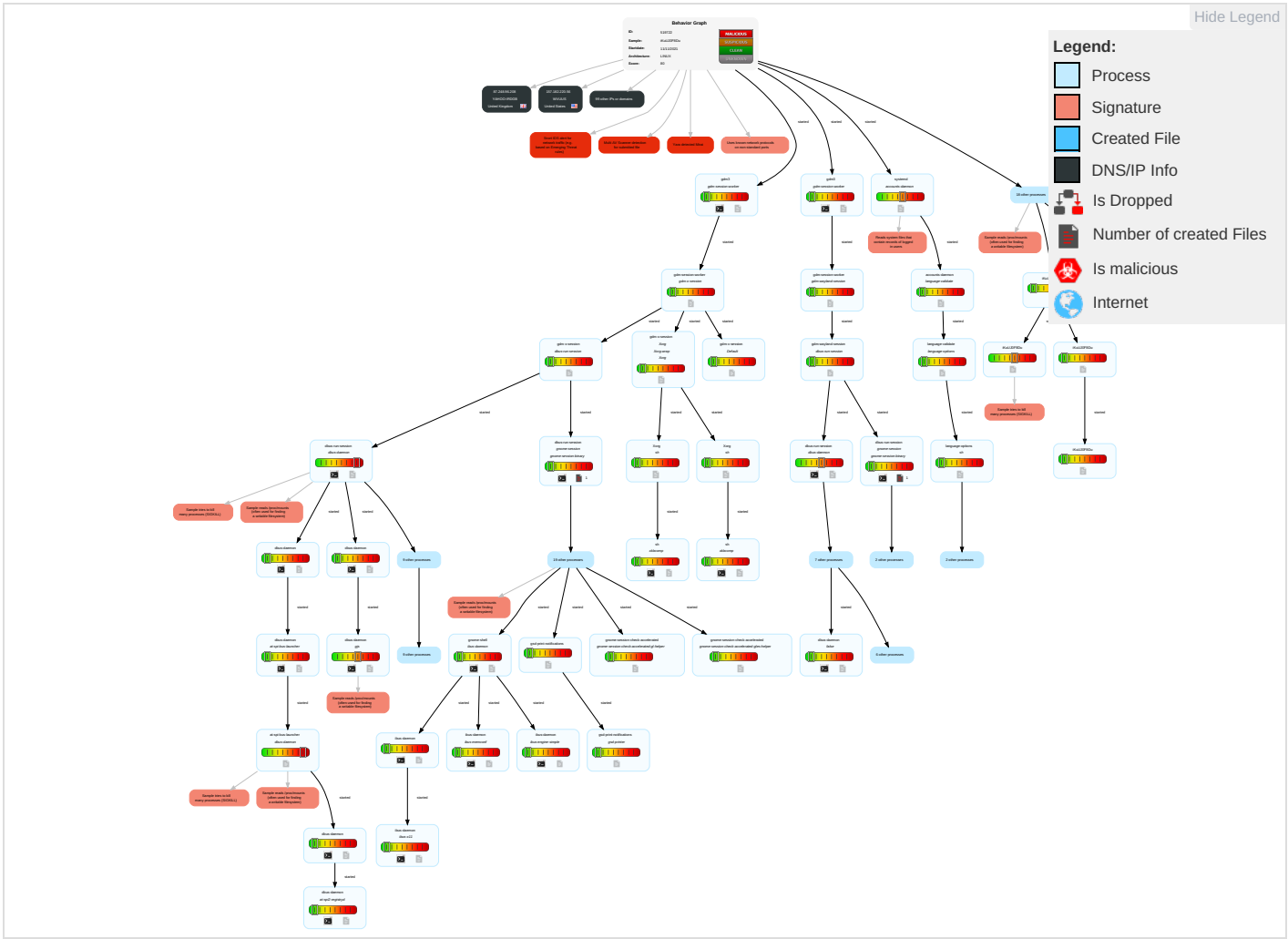
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	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	Modify System Partitio
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	Device Lockou
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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Indicator Removal on Host 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
iKuUJ0F8Du	37%	Virustotal		Browse
iKuUJ0F8Du	25%	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
113.20.79.14	unknown	Fiji		9241	FINTEL-FJFijiInternationalTelecomunicationsLtdFJ	false
114.19.7.216	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
95.56.132.187	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
101.83.192.210	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
132.118.40.110	unknown	United States		306	DNIC-ASBLK-00306-00371US	false
178.244.63.176	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
186.178.15.149	unknown	Ecuador		28006	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEPEC	false
4.250.17.37	unknown	United States		3356	LEVEL3US	false
220.142.93.152	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
20.167.89.117	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
5.144.113.94	unknown	Russian Federation		8359	MTSRU	false
103.203.177.190	unknown	Bangladesh		64074	ABS-AS-APAlphaBroadwaySystemBD	false
93.1.71.253	unknown	France		15557	LDCOMNETFR	false
155.106.187.199	unknown	United States		7018	ATT-INTERNET4US	false
2.202.212.208	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
125.70.125.254	unknown	China		38283	CHINANET-SCIDC-AS-APCHINANETSiChuanTelecomInternetData	false
27.231.70.48	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
172.175.150.76	unknown	United States		7018	ATT-INTERNET4US	false
163.199.10.38	unknown	South Africa		62355	NETWORKDEDICATEDCH	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.70.88.189	unknown	United Kingdom		16174	INTUITIV-ASIntuitivAutonomousSystemGB	false
203.220.124.122	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
211.92.196.254	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
150.94.230.212	unknown	Japan		6400	CompaniaDominicanadeTelefonosSADO	false
35.87.63.27	unknown	United States		237	MERIT-AS-14US	false
34.217.111.207	unknown	United States		16509	AMAZON-02US	false
79.117.211.246	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
138.106.222.182	unknown	Sweden		202116	SCANIA-ASSE	false
162.177.80.187	unknown	United States		21928	T-MOBILE-AS21928US	false
73.208.247.16	unknown	United States		7922	COMCAST-7922US	false
14.122.106.86	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
102.73.57.244	unknown	Morocco		6713	IAM-ASMA	false
94.99.157.11	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
217.156.238.227	unknown	United Kingdom		3549	LVLT-3549US	false
43.188.171.218	unknown	Japan		4249	LILLY-ASUS	false
95.218.217.74	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
27.126.160.205	unknown	Japan		18136	CTAJupiterTelecommunicationsCoLtdJP	false
77.183.61.140	unknown	Germany		6805	TDDE-ASN1DE	false
1.252.254.88	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
167.33.111.196	unknown	Canada		2665	CDAGOVNCA	false
107.210.249.239	unknown	United States		7018	ATT-INTERNET4US	false
148.185.5.243	unknown	European Union		3423	ATTIS-ASN3423US	false
65.171.81.59	unknown	United States		14574	RTCCOMUS	false
118.31.165.102	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
109.102.110.68	unknown	Romania		9050	RTDBucharestRomaniaRO	false
77.137.149.132	unknown	France		12849	HOTNET-ILAMS-IXAdminLANIL	false
87.160.4.220	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
46.220.227.113	unknown	Austria		25255	H3G-AUSTRIA-ASTELE2AUSTRIAAT	false
92.233.183.87	unknown	United Kingdom		5089	NTLGB	false
203.251.232.156	unknown	Korea Republic of		4670	HYUNDAI-KRShinbiroKR	false
168.54.241.222	unknown	United States		1761	TDIR-CAPNETUS	false
176.213.216.154	unknown	Russian Federation		51645	IRKUTSK-ASRU	false
87.248.96.208	unknown	United Kingdom		34010	YAHOO-IRDGB	false
186.148.170.212	unknown	Colombia		262186	TVAZTECASUCURSALCOLOMBIACO	false
95.42.34.111	unknown	Bulgaria		8866	BTC-ASBULGARIABG	false
34.137.212.25	unknown	United States		2686	ATGS-MMD-ASUS	false
133.74.84.34	unknown	Japan		3488	JAXANETInformationSystemsDepartmentJapanAerospaceExpl	false
151.156.34.66	unknown	Sweden		205664	VATTENFALL-ABSE	false
187.4.255.134	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
36.25.171.111	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
34.63.62.104	unknown	United States		2686	ATGS-MMD-ASUS	false
64.122.113.225	unknown	United States		7385	ALLSTREAMUS	false
194.144.206.241	unknown	Iceland		12969	VODAFONE_ICELANDIS	false
116.23.217.123	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
40.158.39.96	unknown	United States		4249	LILLY-ASUS	false
84.50.189.177	unknown	Estonia		3249	ESTPAKEE	false
189.35.34.46	unknown	Brazil		28573	CLAROSABR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
97.206.178.30	unknown	United States		6167	CELLCO-PARTUS	false
76.233.154.253	unknown	United States		7018	ATT-INTERNET4US	false
69.222.238.0	unknown	United States		7018	ATT-INTERNET4US	false
71.107.114.137	unknown	United States		701	UUNETUS	false
211.76.83.31	unknown	Taiwan; Republic of China (ROC)		9676	SAVECOM-TWSaveComInternationIncTW	false
173.72.114.191	unknown	United States		701	UUNETUS	false
88.116.83.42	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
148.38.9.227	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
208.41.137.87	unknown	United States		4565	MEGAPATH2-US	false
32.149.172.222	unknown	United States		2686	ATGS-MMD-ASUS	false
45.12.142.175	unknown	Latvia		35913	DEDIPATH-LLCUS	false
192.63.149.28	unknown	United States		unknown	unknown	false
40.128.249.36	unknown	United States		7029	WINDSTREAMUS	false
157.182.220.56	unknown	United States		12118	WVUUS	false
103.183.119.94	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
161.12.105.187	unknown	United Kingdom		61231	SSE-TELECOMSGB	false
38.123.47.200	unknown	United States		40166	DAEMEN-COLLEGEUS	false
157.77.88.7	unknown	Japan		4678	FINECanonITSolutionsIncJP	false
64.37.144.131	unknown	United States		13720	SONYONLINEUS	false
105.10.82.96	unknown	South Africa		37168	CELL-CZA	false
113.161.130.102	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
48.49.138.120	unknown	United States		2686	ATGS-MMD-ASUS	false
86.44.104.208	unknown	Ireland		5466	EIRCOMInternetHouseIE	false
19.161.5.47	unknown	United States		3	MIT-GATEWAYSUS	false
117.12.214.166	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
196.241.209.180	unknown	Seychelles		37518	FIBERGRIDSC	false
164.9.224.4	unknown	Sweden		29217	WM-DATASE	false
58.81.27.74	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
77.182.11.56	unknown	Germany		6805	TDDE-ASN1DE	false
37.24.114.121	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
213.83.85.152	unknown	United Kingdom		8586	OBSL-ASTalkTalk-BusinessdivisionGB	false
177.72.156.107	unknown	Brazil		52821	TorreseAnselmiLtdaBR	false
204.140.211.89	unknown	United States		226	LOS-NETTOS-ASUS	false
105.11.128.173	unknown	South Africa		37168	CELL-CZA	false

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
daisy.ubuntu.com	arm7	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.108
	x86	Get hash	malicious	Browse	• 162.213.33.108
	arm	Get hash	malicious	Browse	• 162.213.33.108
	arm7	Get hash	malicious	Browse	• 162.213.33.132
	x86	Get hash	malicious	Browse	• 162.213.33.132

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KAZTELECOM-ASKZ	z0x3n.arm-20211110-2150	Get hash	malicious	Browse	• 2.133.122.113
	DVHEnaPp2d	Get hash	malicious	Browse	• 95.58.131.4
	qgxgn5fQU1	Get hash	malicious	Browse	• 37.150.27.46
	jyTZMJKPD2	Get hash	malicious	Browse	• 5.76.170.94
	P8NtIPe7f0	Get hash	malicious	Browse	• 2.135.7.136
	FAuA0G2obM	Get hash	malicious	Browse	• 92.47.16.107
	7L38cWaJpW	Get hash	malicious	Browse	• 2.134.69.178
	nY0UOuOPzI	Get hash	malicious	Browse	• 5.63.77.104
	arm7-20211103-0152	Get hash	malicious	Browse	• 31.169.197.101
	sora.arm	Get hash	malicious	Browse	• 178.91.19.34
	zJk9UEOnQ7	Get hash	malicious	Browse	• 2.135.247.91
	wt5i2fAcF0	Get hash	malicious	Browse	• 95.57.233.60
	izTs48VpFZ	Get hash	malicious	Browse	• 178.91.19.33
	Yoshi.x86	Get hash	malicious	Browse	• 37.151.123.198
	Antisocial.x86	Get hash	malicious	Browse	• 5.251.149.225
	QtNnZoNz75	Get hash	malicious	Browse	• 95.58.131.8
	S13B4aCa4E	Get hash	malicious	Browse	• 95.56.47.28
	Tsunami.x86	Get hash	malicious	Browse	• 5.251.149.212
	9QPGr9LMaq	Get hash	malicious	Browse	• 95.56.23.109
	32UX3eB2m0	Get hash	malicious	Browse	• 95.57.49.132
KDDIKDDICORPORATIONJP	arm7	Get hash	malicious	Browse	• 106.141.201.52
	TFiqcmldz5	Get hash	malicious	Browse	• 175.128.12 2.198
	mF0Mqdkjfz	Get hash	malicious	Browse	• 59.239.123.55
	sora.arm7	Get hash	malicious	Browse	• 106.148.78.193
	z0x3n.arm7-20211110-2150	Get hash	malicious	Browse	• 118.152.12 0.101
	sora.mpsl	Get hash	malicious	Browse	• 222.226.56.23
	l0vNaPgd6f	Get hash	malicious	Browse	• 111.98.134.48
	8fVDxGRR8S	Get hash	malicious	Browse	• 106.191.145.9
	63BjZ1IcIh	Get hash	malicious	Browse	• 210.199.22 8.130
	QXFOZ3Cshc	Get hash	malicious	Browse	• 59.228.127.121
	sora.x86	Get hash	malicious	Browse	• 113.155.217.53
	sora.arm	Get hash	malicious	Browse	• 118.157.14.103
	HwcNrhNfZg	Get hash	malicious	Browse	• 59.250.167.249
	e9e6i5D2gK	Get hash	malicious	Browse	• 106.142.62.27
	ecuuS2WNmQ	Get hash	malicious	Browse	• 106.132.15 6.115
	0LuSWzDmJG	Get hash	malicious	Browse	• 163.48.92.243
	Yoshi.arm-20211110-0350	Get hash	malicious	Browse	• 111.106.90.136
	pt7DJSPfna	Get hash	malicious	Browse	• 106.176.10 4.203
	sora.x86	Get hash	malicious	Browse	• 106.158.254.0
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 210.168.19 2.200
FINTEL-FJFijiInternationalTelecomunicationsLtdFJ	sora.arm	Get hash	malicious	Browse	• 113.20.79.29
	TJpN4pn0l7	Get hash	malicious	Browse	• 202.62.5.149

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
	vq0sPlNJDK	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
	0bqzNIp9PV	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
	KSzA1ujvlV	Get hash	malicious	Browse	• 162.213.33.108
	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:	C54830B41ECFA1B6FBDC30397188DDA86B7B200E62AEAC21AE694A6192DCC38A
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:	3:5bkrIZsXvn:pkckv
MD5:	28FE6435F34B3367707BB1C5D5F6B430
SHA1:	EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6
SHA-256:	721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0
SHA-512:	6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919
Malicious:	false
Reputation:	moderate, very likely benign file

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Preview:	auto_null.monitor.

/proc/5294/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:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/proc/5342/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0

/proc/5345/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0

/proc/5347/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/5347/oom_score_adj	
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5349/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5351/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5353/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5356/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/5356/oom_score_adj	
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5496/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5526/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5529/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5531/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

/proc/5531/oom_score_adj	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5533/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5535/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5537/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5540/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)
Category:	dropped

/proc/5540/oom_score_adj	
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5846/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/5883/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/6080/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:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/proc/6143/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)

/proc/6143/oom_score_adj	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
Preview:	 0

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Cgvn:Cq
MD5:	6241802DCBEB7C5908456B924444BB89
SHA1:	6A5ACBBE3C16030790F8986FC4D3F260C54D6F85
SHA-256:	C20721BC2D0E1AC3B2DE5B79934895327A12A807206D6A5B1DA934930039491F
SHA-512:	2586333D03E5C8D84816CBD9E22AF84F9249F0725A4FEA77BF0F0594DAE407A83FEFF40B2C7BF9C6DE29595A358190763AF0B4EC1F0506232D33D9056E53CA9F
Malicious:	false
Preview:	 5294.

/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:EHvn:EHv
MD5:	4516DC9CF0F93B2D127A8649FA91487F
SHA1:	39DFD4ADAB3BAFFC730B164AE3B95F434A716DBE
SHA-256:	4A9FF2D3B76A3A6E1E4487B909539E14D55E3265E0678B582C5976846C42C1E9
SHA-512:	79804BAFCA62C90DE63FA2C0CB8494C4EC1F3F8DB4F722B35ADCE0F25282F303913ACA63B180AFE2D671A6AD31909876077D49400BAADCDBAC881C8A07D55 CB
Malicious:	false
Preview:	 5422.

/run/user/127/ICEauthority	
Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	6.00103512134652
Encrypted:	false
SSDEEP:	12:OxPG3+DfKUf2veY+G3+Q2xPNwveY+NqxP5mhijveY+5tWmxPwWoveY+wcZVveY+S:SyG8wqrccBzK
MD5:	2FA0FBCE75C1D6701C9E2039A853071A
SHA1:	EB3CB5C8A550AD7F9803F35D807ADA6CF2DFF05C
SHA-256:	B04B4DBE3ED80C87D45A47D0BCDC6215D44B74D56756D3E3DDCBD7B4B4AC1C9F
SHA-512:	7CADA7637EBCE8F10CF8CA8B0235DE11D96002B27E7F019FCFCA93A3B326F4A3F09CB3DC04F757D35145362115947AF93B24E67A810D64BB1F1BFEE106668C7 C
Malicious:	false

/run/user/127/ICEauthority	
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5440..MIT-MAGIC-COOKIE-1..!<.. .d..w.....z..XSMP...#local/galassia:@/tmp/.ICE-unix/5440..MIT-MAGIC-COOKIE-1...i....]7.... .K}...ICE...!unix/galassia:/tmp/.ICE-unix/5338..MIT-MAGIC-COOKIE-1...=.S.B.M.d....'...ICE...#local/galassia:@/tmp/.ICE-unix/5338..MIT-MAGIC-COOKIE-1..K.....B.0. 9\!....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$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f..... E..c..XSMP...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... .....Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,: B.o.....ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte\|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN.. ...N+..$..XSMP...#local/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):	4.903826878482618
Encrypted:	false
SSDEEP:	3:rg/WFllasO93JSm5qoTwgWFllasO93JSm5qoX:rg/WFl21TTHWFl21TX
MD5:	04ACDFC76BC762CBD5D80806B686A14D
SHA1:	B70D3DCAE8B5C8C0BD338938D876E4994C5BEAA6
SHA-256:	DA9EEA71445CE097F87A13F4EC0705652B012C44524EA788E8AE9FB5C65F4E2E
SHA-512:	59AFBC7E4EF881369E3081B7D76C46E6776E1DDD277107D3A58230EE857380740DE6D45B4513CD8E791B1BEFB0D14D51B008186A0FBE55F6338A8B2BB42BADD C
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1..$^o..\|C..!..(.\|.....galassia....MIT-MAGIC-COOKIE-1..$^o..|C..!..(.|.

/run/user/127/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:IGv:I4
MD5:	7230424E7D3E372FC3B7652A32CA23EA
SHA1:	ACE4182875EF90D5C3E88BDAE9FD0ACB22565BF2
SHA-256:	2BCD075A0755DD77FC0D81B5AEDB64D33F5E81AF6938603334559F7F07271213
SHA-512:	F14D19C686155140C8912CD3E080713DCD4646CF04B33F42ED37222479D38D455988E61CE58238F1EBE6EFF9481C3A6ABB4FFF3C7036AFB9396AC138F6C9AAF
Malicious:	false
Preview:	5856.

/tmp/server-0.xkm	
Process:	/usr/bin/xkbcomp
File Type:	Compiled XKB Keymap: lsb, version 15
Category:	dropped
Size (bytes):	12060
Entropy (8bit):	4.8492493153178975
Encrypted:	false
SSDEEP:	192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ
MD5:	B4E3EB0B8B6B0FC1F46740C573E18D86
SHA1:	7D35426357695EBA77850757E8939A62DCEFF2D1

/tmp/server-0.xkm	
SHA-256:	7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91
SHA-512:	8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE0 1
Malicious:	false
Preview:	.mkx.....D.....h.....<.....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta ....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD 06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB 08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP 3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWN PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181 I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18

/var/lib/AccountsService/users/gdm.G1IGC1	
Process:	/usr/lib/accountsservice/accounts-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.66214589518167
Encrypted:	false
SSDEEP:	3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M
MD5:	542BA3FB41206AE43928AF1C5E61FEBC
SHA1:	F56F574DAF50D609526B36B5B54FDD59EA4D6A26
SHA-256:	730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A
SHA-512:	D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F AEA
Malicious:	false
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/AccountsService/users/gdm.W1YOC1	
Process:	/usr/lib/accountsservice/accounts-daemon
File Type:	ASCII text
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.66214589518167
Encrypted:	false
SSDEEP:	3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M
MD5:	542BA3FB41206AE43928AF1C5E61FEBC
SHA1:	F56F574DAF50D609526B36B5B54FDD59EA4D6A26
SHA-256:	730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A
SHA-512:	D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F AEA
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):	5.133298357510428
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWvTXHtBSAem:q5sU3LWfLUDmQymqSFbfomSRTLZZ1fzn
MD5:	9A1A12B1FB2DC1E55780138634D3EB76
SHA1:	D80BC27D0C0037419A0FB18746B9FDC44D248DA6
SHA-256:	855CF73D95E573A3175EF919B082CDF8151653DCED564B6F84447548DF92A1CD
SHA-512:	2BD1C113438D84A2C9721164CA9C92421C0008255FB9BBB6D899DAC4B8E57312FCFB1A18D7711966B3434402B44638D0850E09C06068A2EB867F789078615DC7
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-t5L6Rr9i,guid=f41 9f9dc2281b89c1781a9d3618c9e44.IBUS_DAEMON_PID=5797.

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Process:	/usr/bin/pulseaudio
File Type:	very short file (no magic)

/var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:v:v
MD5:	68B329DA9893E34099C7D8AD5CB9C940
SHA1:	ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC
SHA-256:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE(9
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:	01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B
SHA-512:	BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE(9
Malicious:	false
Preview:	.

/var/lib/whoopsie/whoopsie-id.2ZXHC1	
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:3y6BlVEfQXU8djCZd40
MD5:	D2B5AAF22916F8D6665CF9E835EAD5E7
SHA1:	AAEF3CE527B8F1E3733BCD03EF7A6C0F30881E15
SHA-256:	FEB925D4465BF6D30A42B19112406AD1B59BA90673DC4F91B25005A90FEFEB36
SHA-512:	B55A45FA0DECE5A3B0348BC3F3031A7329590E57BAD5013690AFEAA9825C0DE4B75D27057A56C33800F1626935840DA2262AAF14E795C75F39362B728D95F18A
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):	5.28868875123975
Encrypted:	false
SSDEEP:	384:yGOLNc9JMRdkdsdXdDdfdedOdXdzdYdjdVd3dddhdydGd1dpdldC7d7jdWod+dKq:POLO8echQY5pQBBfqZsyJlY0C
MD5:	FD693E30205B537968E11D507E598149
SHA1:	94705675CFB3ED098C26F12F06B86BF9465CC8B7
SHA-256:	F9CB2A2D3802FCF116E135CEF588F7108DD351F3AB6614DAB285FE9170D06EE7
SHA-512:	B52F201D34AFB862CB859DE1AC723477346C675475CA3BC405631830987D67D10BF55320F7D76A015AC08D67A6BF13FCCAFF19D6B5F8CC91E1D80BF1565E746
Malicious:	false
Preview:	[479.631] (--) Log file renamed from "/var/log/Xorg.pid-5393.log" to "/var/log/Xorg.0.log".[479.655] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[479.674] Build Operating System: linux Ubuntu.[479.689] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[479.699] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[479.714] Build Date: 06 July 2021 10:17:51AM.[479.719] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[479.724] Current version of pixman: 0.38.4.[479.730] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[479.734] 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, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.827240147591348
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	iKuUJ0F8Du
File size:	71832
MD5:	5d0d54974ca6c1262372b7292ff1eb70
SHA1:	00bdfd4f35dd30e1c049648cf5d8cffaf70cddd0
SHA256:	8126a9a1a5625761574346 56d620574ce14b6db55b8c37bc6341c0bf1664820e
SHA512:	201ec2de315e35cadb68a0f45cf95490d68d76e9d7f4ef6ace49b83841241e750fb94dfaf7ad7d9803a257ab7c325e38076b00c5e76e644ae3273f98caa2b1ac
SSDEEP:	1536:ZR2ni8I7eNtxLcyTd4DR3mNZi3K/feul5YcCsRoqtfK:PRiNtqyTd48Nt/F5YcTC
File Content Preview:	.ELF.....*.....@.4.....4. ...(.....@...@.....B...B.....h.....Q.td....././/"O.n.....#.*@.....#.*@.....o&O.n...l....././../../a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71432
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xee00	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40eee0	0xeee0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40ef04	0xef04	0x23f8	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x421300	0x11300	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x421308	0x11308	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x421314	0x11314	0x3b4	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x4216c8	0x116c8	0x64e0	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x116c8	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x112fc	0x112fc	4.6922	0x5	R E	0x10000		.init .text .fini .rodata

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x11300	0x421300	0x421300	0x3c8	0x68a8	1.8435	0x6	RW	0x10000		.ctors .dtors .data .bss
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 11, 2021 04:37:25.751020908 CET	192.168.2.23	1.1.1.1	0x62a6	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)
Nov 11, 2021 04:37:25.751169920 CET	192.168.2.23	1.1.1.1	0x4ba	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)
Nov 11, 2021 04:37:25.851524115 CET	192.168.2.23	1.1.1.1	0x5a8e	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 11, 2021 04:37:25.767560005 CET	1.1.1.1	192.168.2.23	0x62a6	No error (0)	daisy.ubuntu.com		162.213.33.132	A (IP address)	IN (0x0001)
Nov 11, 2021 04:37:25.767560005 CET	1.1.1.1	192.168.2.23	0x62a6	No error (0)	daisy.ubuntu.com		162.213.33.108	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: iKuUJ0F8Du PID: 5234 Parent PID: 5117

General

Start time:	04:36:40
Start date:	11/11/2021
Path:	/tmp/iKuUJ0F8Du
Arguments:	/tmp/iKuUJ0F8Du
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: iKuUJ0F8Du PID: 5236 Parent PID: 5234

General

Start time:	04:36:40
Start date:	11/11/2021
Path:	/tmp/iKuUJ0F8Du
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: iKuUJ0F8Du PID: 5237 Parent PID: 5234

General

Start time:	04:36:40
Start date:	11/11/2021
Path:	/tmp/iKuUJ0F8Du
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: iKuUJ0F8Du PID: 5240 Parent PID: 5237

General

Start time:	04:36:40
Start date:	11/11/2021
Path:	/tmp/iKuUJ0F8Du
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: iKuUJ0F8Du PID: 5242 Parent PID: 5237

General

Start time:	04:36:40
Start date:	11/11/2021
Path:	/tmp/iKuUJ0F8Du
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: iKuUJ0F8Du PID: 5244 Parent PID: 5242

General

Start time:	04:36:40
Start date:	11/11/2021
Path:	/tmp/iKuUJ0F8Du
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: systemd PID: 5286 Parent PID: 1

General

Start time:	04:37:24
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5286 Parent PID: 1

General

Start time:	04:37:24
Start date:	11/11/2021
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: 5293 Parent PID: 1

General

Start time:	04:37:28
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5293 Parent PID: 1

General

Start time:	04:37:28
Start date:	11/11/2021
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: 5294 Parent PID: 1

General

Start time:	04:37:28
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5294 Parent PID: 1

General

Start time:	04:37:28
Start date:	11/11/2021
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: 5303 Parent PID: 1320

General

Start time:	04:37:35
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5303 Parent PID: 1320

General

Start time:	04:37:35
Start date:	11/11/2021
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: 5306 Parent PID: 1320

General

Start time:	04:37:35
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5306 Parent PID: 1320

General

Start time:	04:37:35
Start date:	11/11/2021
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: 5307 Parent PID: 1

General

Start time:	04:37:35
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5307 Parent PID: 1

General

Start time:	04:37:35
Start date:	11/11/2021
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: 5322 Parent PID: 5307

General

Start time:	04:37:35
Start date:	11/11/2021
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: 5322 Parent PID: 5307

General

Start time:	04:37:35
Start date:	11/11/2021
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: 5323 Parent PID: 5322

General

Start time:	04:37:35
Start date:	11/11/2021
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5323 Parent PID: 5322

General

Start time:	04:37:35
Start date:	11/11/2021
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: 5324 Parent PID: 5323

General

Start time:	04:37:36
Start date:	11/11/2021
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5324 Parent PID: 5323

General

Start time:	04:37:36
Start date:	11/11/2021
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: 5325 Parent PID: 5324

General

Start time:	04:37:36
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5325 Parent PID: 5324

General

Start time:	04:37:36
Start date:	11/11/2021
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5326 Parent PID: 5324

General

Start time:	04:37:36
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5326 Parent PID: 5324

General

Start time:	04:37:36
Start date:	11/11/2021
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gdm3 PID: 5327 Parent PID: 1320

General

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

Analysis Process: gdm-session-worker PID: 5327 Parent PID: 1320

General

Start time:	04:37:37
Start date:	11/11/2021
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: 5333 Parent PID: 5327

General

Start time:	04:37:39
Start date:	11/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 5333 Parent PID: 5327

General

Start time:	04:37:39
Start date:	11/11/2021
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: 5336 Parent PID: 5333

General

Start time:	04:37:39
Start date:	11/11/2021
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: 5336 Parent PID: 5333

General

Start time:	04:37:39
Start date:	11/11/2021
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: 5337 Parent PID: 5336

General

Start time:	04:37:39
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5337 Parent PID: 5336

General

Start time:	04:37:39
Start date:	11/11/2021
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: 5341 Parent PID: 5337

General

Start time:	04:37:40
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5342 Parent PID: 5341

General

Start time:	04:37:40
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5342 Parent PID: 5341

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5344 Parent PID: 5337

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5345 Parent PID: 5344

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon

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

File Activities

File Written

Analysis Process: false PID: 5345 Parent PID: 5344

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5346 Parent PID: 5337

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5347 Parent PID: 5346

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5347 Parent PID: 5346

General

Start time:	04:37:41

Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5348 Parent PID: 5337

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

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

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5349 Parent PID: 5348

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5350 Parent PID: 5337

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5351 Parent PID: 5350

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5351 Parent PID: 5350

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5352 Parent PID: 5337

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5353 Parent PID: 5352

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon

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

File Activities

File Written

Analysis Process: false PID: 5353 Parent PID: 5352

General

Start time:	04:37:41
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5355 Parent PID: 5337

General

Start time:	04:37:42
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5356 Parent PID: 5355

General

Start time:	04:37:42
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5356 Parent PID: 5355

General

Start time:	04:37:42

Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5338 Parent PID: 5336

General

Start time:	04:37:39
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5338 Parent PID: 5336

General

Start time:	04:37:40
Start date:	11/11/2021
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: 5338 Parent PID: 5336

General

Start time:	04:37:40
Start date:	11/11/2021
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: 5357 Parent PID: 5338

General

Start time:	04:37:43
Start date:	11/11/2021
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: 5357 Parent PID: 5338

General

Start time:	04:37:43
Start date:	11/11/2021
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: 5358 Parent PID: 5338

General

Start time:	04:37:43
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5358 Parent PID: 5338

General

Start time:	04:37:43
Start date:	11/11/2021
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: 5358 Parent PID: 5338

General

Start time:	04:37:43
Start date:	11/11/2021
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: 5386 Parent PID: 1320

General

Start time:	04:37:47
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5386 Parent PID: 1320

General

Start time:	04:37:47
Start date:	11/11/2021
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: 5391 Parent PID: 5386

General

Start time:	04:37:48
Start date:	11/11/2021
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 5391 Parent PID: 5386

General

Start time:	04:37:48
Start date:	11/11/2021
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: 5393 Parent PID: 5391

General

Start time:	04:37:48
Start date:	11/11/2021
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: 5393 Parent PID: 5391

General

Start time:	04:37:48
Start date:	11/11/2021

Path:	/usr/bin/Xorg
Arguments:	/usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: Xorg.wrap PID: 5393 Parent PID: 5391

General

Start time:	04:37:48
Start date:	11/11/2021
Path:	/usr/lib/xorg/Xorg.wrap
Arguments:	/usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
File size:	14488 bytes
MD5 hash:	48993830888200ecf19dd7def0884dfd

File Activities

File Read

Analysis Process: Xorg PID: 5393 Parent PID: 5391

General

Start time:	04:37:48
Start date:	11/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	/usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -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: 5427 Parent PID: 5393

General

Start time:	04:37:57
Start date:	11/11/2021
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes

MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5427 Parent PID: 5393

General

Start time:	04:37:57
Start date:	11/11/2021
Path:	/bin/sh
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\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5428 Parent PID: 5427

General

Start time:	04:37:57
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5428 Parent PID: 5427

General

Start time:	04:37:57
Start date:	11/11/2021
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: 5849 Parent PID: 5393

General

Start time:	04:38:30
Start date:	11/11/2021

Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5849 Parent PID: 5393

General

Start time:	04:38:30
Start date:	11/11/2021
Path:	/bin/sh
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\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5850 Parent PID: 5849

General

Start time:	04:38:30
Start date:	11/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5850 Parent PID: 5849

General

Start time:	04:38:30
Start date:	11/11/2021
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: 5437 Parent PID: 5391

General

General

Start time:	04:38:04
Start date:	11/11/2021
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: 5437 Parent PID: 5391

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5438 Parent PID: 5391

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5438 Parent PID: 5391

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5439 Parent PID: 5438

General

Start time:	04:38:05
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5439 Parent PID: 5438

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5495 Parent PID: 5439

General

Start time:	04:38:11
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5496 Parent PID: 5495

General

Start time:	04:38:11
Start date:	11/11/2021
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: 5496 Parent PID: 5495

General

Start time:	04:38:11
Start date:	11/11/2021
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: 5501 Parent PID: 5496

General

Start time:	04:38:11
Start date:	11/11/2021
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: 5501 Parent PID: 5496

General

Start time:	04:38:11
Start date:	11/11/2021
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: 5879 Parent PID: 5501

General

Start time:	04:38:32
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5883 Parent PID: 5879

General

Start time:	04:38:32
Start date:	11/11/2021
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: 5883 Parent PID: 5879

General

Start time:	04:38:32
Start date:	11/11/2021
Path:	/usr/libexec/at-spi2-registryd
Arguments:	/usr/libexec/at-spi2-registryd --use-gnome-session
File size:	100224 bytes
MD5 hash:	1d904c2693452edebc7ede3a9e24d440

File Activities

File Read

Analysis Process: dbus-daemon PID: 5525 Parent PID: 5439

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5526 Parent PID: 5525

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5526 Parent PID: 5525

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5528 Parent PID: 5439

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5529 Parent PID: 5528

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5529 Parent PID: 5528

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5530 Parent PID: 5439

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5531 Parent PID: 5530

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5531 Parent PID: 5530

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5532 Parent PID: 5439

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5533 Parent PID: 5532

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5533 Parent PID: 5532

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5534 Parent PID: 5439

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5535 Parent PID: 5534

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5535 Parent PID: 5534

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5536 Parent PID: 5439

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5537 Parent PID: 5536

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5537 Parent PID: 5536

General

Start time:	04:38:14
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5539 Parent PID: 5439

General

Start time:	04:38:15
Start date:	11/11/2021
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:	04:38:15
Start date:	11/11/2021
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:	04:38:15
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5845 Parent PID: 5439

General

Start time:	04:38:28
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5846 Parent PID: 5845

General

Start time:	04:38:28
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: ibus-portal PID: 5846 Parent PID: 5845

General

Start time:	04:38:28
Start date:	11/11/2021
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: 6079 Parent PID: 5439

General

Start time:	04:38:33
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon

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

Analysis Process: dbus-daemon PID: 6080 Parent PID: 6079

General

Start time:	04:38:33
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: gjs PID: 6080 Parent PID: 6079

General

Start time:	04:38:34
Start date:	11/11/2021
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: 6142 Parent PID: 5439

General

Start time:	04:38:46
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 6143 Parent PID: 6142

General

Start time:	04:38:46
Start date:	11/11/2021
Path:	/usr/bin/dbus-daemon

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

File Activities

File Written

Analysis Process: false PID: 6143 Parent PID: 6142

General

Start time:	04:38:46
Start date:	11/11/2021
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5440 Parent PID: 5438

General

Start time:	04:38:05
Start date:	11/11/2021
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5440 Parent PID: 5438

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5440 Parent PID: 5438

General

Start time:	04:38:05

Start date:	11/11/2021
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: 5441 Parent PID: 5440

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5441 Parent PID: 5440

General

Start time:	04:38:05
Start date:	11/11/2021
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: 5502 Parent PID: 5441

General

Start time:	04:38:12
Start date:	11/11/2021
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-gl-helper PID: 5502 Parent PID: 5441

General

Start time:	04:38:12
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-check-accelerated-gl-helper
Arguments:	/usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
File size:	22920 bytes
MD5 hash:	b1ab9a384f9e98a39ae5c36037dd5e78

File Activities

File Read

Directory Enumerated

Analysis Process: gnome-session-check-accelerated PID: 5512 Parent PID: 5441

General

Start time:	04:38:12
Start date:	11/11/2021
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: 5512 Parent PID: 5441

General

Start time:	04:38:12
Start date:	11/11/2021
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: 5541 Parent PID: 5440

General

Start time:	04:38:15
Start date:	11/11/2021
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: 5541 Parent PID: 5440

General

Start time:	04:38:15
Start date:	11/11/2021
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: 5542 Parent PID: 5440

General

Start time:	04:38:16
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5542 Parent PID: 5440

General

Start time:	04:38:16
Start date:	11/11/2021
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: 5542 Parent PID: 5440

General

Start time:	04:38:16
Start date:	11/11/2021
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: 5797 Parent PID: 5542

General

Start time:	04:38:27
Start date:	11/11/2021
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5797 Parent PID: 5542

General

Start time:	04:38:28
Start date:	11/11/2021
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: 5841 Parent PID: 5797

General

Start time:	04:38:28
Start date:	11/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5841 Parent PID: 5797

General

Start time:	04:38:28
Start date:	11/11/2021
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: 5843 Parent PID: 5797

General

Start time:	04:38:28
Start date:	11/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5844 Parent PID: 5843

General

Start time:	04:38:28
Start date:	11/11/2021
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5844 Parent PID: 1

General

Start time:	04:38:28
Start date:	11/11/2021
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: 6114 Parent PID: 5797

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6114 Parent PID: 5797

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6098 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6098 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
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: 6098 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
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: 6100 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6100 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
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: 6100 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
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: 6102 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6102 Parent PID: 5440

General

Start time:	04:38:37
Start date:	11/11/2021
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: 6102 Parent PID: 5440

General

Start time:	04:38:38
Start date:	11/11/2021
Path:	/usr/libexec/gsd-color
Arguments:	/usr/libexec/gsd-color
File size:	92832 bytes
MD5 hash:	ac2861ad93ce047283e8e87cefef9a19

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6103 Parent PID: 5440

General

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

File Activities

Directory Enumerated

Analysis Process: sh PID: 6103 Parent PID: 5440

General

Start time:	04:38:38
Start date:	11/11/2021
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: 6103 Parent PID: 5440

General

Start time:	04:38:38
Start date:	11/11/2021
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: 6105 Parent PID: 5440

General

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

File Activities

Directory Enumerated

Analysis Process: sh PID: 6105 Parent PID: 5440

General

Start time:	04:38:38
Start date:	11/11/2021
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: 6105 Parent PID: 5440

General

Start time:	04:38:38
Start date:	11/11/2021
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: 6421 Parent PID: 6105

General

Start time:	04:38:48
Start date:	11/11/2021
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6422 Parent PID: 6421

General

Start time:	04:38:48
Start date:	11/11/2021
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: 6422 Parent PID: 1

General

Start time:	04:38:49
Start date:	11/11/2021
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: 6106 Parent PID: 5440

General

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

File Activities

Directory Enumerated

Analysis Process: sh PID: 6106 Parent PID: 5440

General

Start time:	04:38:38
Start date:	11/11/2021
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: 6106 Parent PID: 5440

General

Start time:	04:38:39
Start date:	11/11/2021
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: 6108 Parent PID: 5440

General

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

File Activities

Directory Enumerated

Analysis Process: sh PID: 6108 Parent PID: 5440

General

Start time:	04:38:39
Start date:	11/11/2021
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: 6108 Parent PID: 5440

General

Start time:	04:38:39
Start date:	11/11/2021
Path:	/usr/libexec/gsd-smartcard
Arguments:	/usr/libexec/gsd-smartcard
File size:	109152 bytes
MD5 hash:	ea1fbd7f62e4cd0331eae2ef754ee605

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 6111 Parent PID: 5440

General

Start time:	04:38:39
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6111 Parent PID: 5440

General

Start time:	04:38:39
Start date:	11/11/2021
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: 6111 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6112 Parent PID: 5440

General

Start time:	04:38:39
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6112 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6112 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6113 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6113 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6113 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
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: 6117 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 6117 Parent PID: 5440

General

Start time:	04:38:40
Start date:	11/11/2021
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

File Activities

File Read

Analysis Process: gsd-sound PID: 6117 Parent PID: 5440

General

Start time:	04:38:41
Start date:	11/11/2021
Path:	/usr/libexec/gsd-sound
Arguments:	/usr/libexec/gsd-sound
File size:	31248 bytes
MD5 hash:	4c7d3fb993463337b4a0eb5c80c760ee

File Activities

File Read

Analysis Process: gnome-session-binary PID: 6118 Parent PID: 5440

General

Start time:	04:38:41
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6118 Parent PID: 5440

General

Start time:	04:38:41
Start date:	11/11/2021
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: 6118 Parent PID: 5440

General

Start time:	04:38:41
Start date:	11/11/2021
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: 6120 Parent PID: 5440

General

Start time:	04:38:41
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6120 Parent PID: 5440

General

Start time:	04:38:41
Start date:	11/11/2021
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: 6120 Parent PID: 5440

General

Start time:	04:38:42
Start date:	11/11/2021
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

Analysis Process: gnome-session-binary PID: 6123 Parent PID: 5440

General

Start time:	04:38:42
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6123 Parent PID: 5440

General

Start time:	04:38:42
Start date:	11/11/2021
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: 6123 Parent PID: 5440

General

Start time:	04:38:43
Start date:	11/11/2021
Path:	/usr/libexec/gsd-power
Arguments:	/usr/libexec/gsd-power
File size:	88672 bytes
MD5 hash:	28b8e1b43c3e7f1db6741ea1ecd978b7

Analysis Process: gnome-session-binary PID: 6964 Parent PID: 5440

General

Start time:	04:39:05
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6964 Parent PID: 5440

General

Start time:	04:39:05
Start date:	11/11/2021
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: 6964 Parent PID: 5440

General

Start time:	04:39:05
Start date:	11/11/2021
Path:	/usr/bin/spice-vdagent
Arguments:	/usr/bin/spice-vdagent
File size:	80664 bytes
MD5 hash:	80fb7f613aa78d1b8a229dbcf4577a9d

Analysis Process: gnome-session-binary PID: 6971 Parent PID: 5440

General

Start time:	04:39:07
Start date:	11/11/2021
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6971 Parent PID: 5440

General

Start time:	04:39:07
Start date:	11/11/2021
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: 6971 Parent PID: 5440

General

Start time:	04:39:07
Start date:	11/11/2021
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5387 Parent PID: 1320

General

Start time:	04:37:47
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5387 Parent PID: 1320

General

Start time:	04:37:47
Start date:	11/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5388 Parent PID: 1320

General

Start time:	04:37:47
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5388 Parent PID: 1320

General

Start time:	04:37:47
Start date:	11/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5396 Parent PID: 1320

General

Start time:	04:37:52
Start date:	11/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes

MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5396 Parent PID: 1320

General

Start time:	04:37:52
Start date:	11/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemd PID: 5422 Parent PID: 1860

General

Start time:	04:37:57
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5422 Parent PID: 1860

General

Start time:	04:37:57
Start date:	11/11/2021
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: 5443 Parent PID: 2038

General

Start time:	04:38:07
Start date:	11/11/2021
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5443 Parent PID: 2038

General

Start time:	04:38:07
Start date:	11/11/2021
Path:	/bin/fusermount

Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

Analysis Process: systemd PID: 5458 Parent PID: 1

General

Start time:	04:38:07
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5458 Parent PID: 1

General

Start time:	04:38:07
Start date:	11/11/2021
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: 5567 Parent PID: 1

General

Start time:	04:38:27
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5567 Parent PID: 1

General

Start time:	04:38:27
Start date:	11/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 5856 Parent PID: 1334

General

Start time:	04:38:31

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

Analysis Process: pulseaudio PID: 5856 Parent PID: 1334

General

Start time:	04:38:31
Start date:	11/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5859 Parent PID: 1

General

Start time:	04:38:33
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5859 Parent PID: 1

General

Start time:	04:38:33
Start date:	11/11/2021
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 6148 Parent PID: 1

General

Start time:	04:38:48
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-hostnamed PID: 6148 Parent PID: 1

General

Start time:	04:38:48
Start date:	11/11/2021
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	35040 bytes
MD5 hash:	2cc8a5576629a2d5bd98e49a4b8bef65

Analysis Process: systemd PID: 6484 Parent PID: 1

General

Start time:	04:38:59
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 6484 Parent PID: 1

General

Start time:	04:38:59
Start date:	11/11/2021
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 6753 Parent PID: 1

General

Start time:	04:39:04
Start date:	11/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6753 Parent PID: 1

General

Start time:	04:39:04
Start date:	11/11/2021
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84