

JOeSandbox Cloud BASIC



ID: 635071

Sample Name: 6gIL6GLh9R

Cookbook:

defaultlinuxfilecookbook.jbs

Time: 12:24:05

Date: 27/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Linux Analysis Report 6gIL6GLh9R	16
Overview	16
General Information	16
Detection	16
Signatures	16
Classification	16
Analysis Advice	16
General Information	16
Warnings	16
Runtime Messages	16
Process Tree	17
Yara Signatures	21
Initial Sample	21
Memory Dumps	21
Snort Signatures	22
Joe Sandbox Signatures	23
AV Detection	23
System Summary	23
Persistence and Installation Behavior	23
Language, Device and Operating System Detection	23
Stealing of Sensitive Information	23
Remote Access Functionality	23
Mitre Att&ck Matrix	23
Malware Configuration	24
Behavior Graph	24
Antivirus, Machine Learning and Genetic Malware Detection	24
Initial Sample	24
Dropped Files	24
Domains	24
URLs	24
Domains and IPs	25
Contacted Domains	25
URLs from Memory and Binaries	25
World Map of Contacted IPs	25
Public IPs	25
Joe Sandbox View / Context	28
IPs	28
Domains	28
ASNs	28
JA3 Fingerprints	28
Dropped Files	28
Created / dropped Files	28
/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	28
/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	28
/memfd:30-systemd-environment-d-generator (deleted)	28
/memfd:user-environment-generators (deleted)	28
/proc/6481/oom_score_adj	28
/proc/6752/oom_score_adj	28
/run/gdm3.pid	28
/run/systemd/journal/streams/.#9:74907KcTgBY	28
/run/systemd/journal/streams/.#9:74908YhXtMZ	28
/run/systemd/journal/streams/.#9:75603XHnZJ2	28
/run/systemd/journal/streams/.#9:7560854UGWY	28
/run/systemd/journal/streams/.#9:75648HSEZg1	28
/run/systemd/journal/streams/.#9:76282Q7faY0	28
/run/systemd/journal/streams/.#9:762936Rtbh0	28
/run/systemd/journal/streams/.#9:763065qKD00	28
/run/systemd/journal/streams/.#9:764607G7y91	28
/run/systemd/journal/streams/.#9:764661C4G2Z	29
/run/systemd/journal/streams/.#9:76483yHLTc2	29
/run/systemd/journal/streams/.#9:76734aHVBv1	29
/run/systemd/journal/streams/.#9:76816Eplxf0	29
/run/systemd/journal/streams/.#9:77222APHFD1	29
/run/systemd/journal/streams/.#9:77279rW8DKY	29
/run/systemd/journal/streams/.#9:77281dKkVj1	29
/run/systemd/journal/streams/.#9:77313ITXDsZ	29
/run/systemd/journal/streams/.#9:77318Ntn5G1	29
/run/systemd/journal/streams/.#9:78530WYHCsW	29
/run/systemd/journal/streams/.#9:78659QmgUCT	29
/run/systemd/journal/streams/.#9:79001nJ1kDW	29
/run/systemd/journal/streams/.#9:79003S5LcwW	29
/run/systemd/journal/streams/.#9:79018ws0pnV	29
/run/systemd/journal/streams/.#9:79019lZe3AV	29

/run/systemd/journal/streams/.#9:790217VV9sT	29
/run/systemd/journal/streams/.#9:79022JfbHJV	29
/run/systemd/journal/streams/.#9:79030m6EINU	29
/run/systemd/journal/streams/.#9:79564nzFwvb	29
/run/systemd/journal/streams/.#9:7956573XpT7	29
/run/systemd/journal/streams/.#9:79857UnSiRa	29
/run/systemd/journal/streams/.#9:80090sKzz08	29
/run/systemd/journal/streams/.#9:80198472PP9	29
/run/systemd/journal/streams/.#9:80199VfwKE7	29
/run/systemd/journal/streams/.#9:80200qaQNp8	29
/run/systemd/journal/streams/.#9:80209AuLRP7	29
/run/systemd/journal/streams/.#9:802193mvth7	29
/run/systemd/journal/streams/.#9:802203bqbDb	29
/run/systemd/journal/streams/.#9:802233Oj4f7	29
/run/systemd/journal/streams/.#9:80224CxNR98	29
/run/systemd/journal/streams/.#9:80267qBNDd8	29
/run/systemd/journal/streams/.#9:80268tMiLn8	29
/run/systemd/journal/streams/.#9:80302VjkqN8	30
/run/systemd/journal/streams/.#9:8030363hRo8	30
/run/systemd/journal/streams/.#9:80839bdrb2m	30
/run/systemd/journal/streams/.#9:80840LUNoBq	30
/run/systemd/journal/streams/.#9:80855OOJ4Dn	30
/run/systemd/journal/streams/.#9:80859HMYFwq	30
/run/systemd/journal/streams/.#9:808605vy5in	30
/run/systemd/journal/streams/.#9:80862wtapQo	30
/run/systemd/journal/streams/.#9:80883sZlffko	30
/run/systemd/journal/streams/.#9:827030qQjuG	30
/run/systemd/journal/streams/.#9:82718WqsSvl	30
/run/systemd/journal/streams/.#9:827193oflLI	30
/run/systemd/journal/streams/.#9:827207EgvPE	30
/run/systemd/journal/streams/.#9:82727hVCtjG	30
/run/systemd/journal/streams/.#9:82728h0VebH	30
/run/systemd/journal/streams/.#9:83247c0XgpF	30
/run/systemd/journal/streams/.#9:83253FjLj8H	30
/run/systemd/journal/streams/.#9:83261ZcxUvF	30
/run/systemd/journal/streams/.#9:83262gCngnG	30
/run/systemd/journal/streams/.#9:83266nuezcG	30
/run/systemd/journal/streams/.#9:83267NgGHuF	30
/run/systemd/journal/streams/.#9:83278jQCkRE	30
/run/systemd/journal/streams/.#9:83282jOZ5RF	30
/run/systemd/journal/streams/.#9:83283Xq186I	30
/run/systemd/journal/streams/.#9:83285dCfhGG	30
/run/systemd/journal/streams/.#9:83286ahPRol	30
/run/systemd/seats/.#seat0HzP17k	30
/run/systemd/seats/.#seat0K16fYl	30
/run/systemd/seats/.#seat0M9T2qZ	30
/run/systemd/seats/.#seat0YpYzkE	30
/run/systemd/seats/.#seat0i6qGpk	30
/run/systemd/seats/.#seat0xn76yi	30
/run/systemd/seats/.#seat0zs0y8u	31
/run/systemd/users/.#1279ZRaxm	31
/run/systemd/users/.#127LT7oLo	31
/run/systemd/users/.#127NKcwVk	31
/run/systemd/users/.#127TdX6Hj	31
/run/systemd/users/.#127TeLMik	31
/run/systemd/users/.#127Z4vyKh	31
/run/systemd/users/.#127pU3buh	31
/run/systemd/users/.#127qAetKk	31
/run/user/1000/pulse/pid	31
/run/utmp	31
/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/dbus.socket/cgroup.procs	31
/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/init.scope/cgroup.procs	31
/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	31
/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/dbus.socket/cgroup.procs	31
/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/init.scope/cgroup.procs	31
/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	31
/tmp/qemu-open.kCThj6 (deleted)	31
/var/crash/_usr_bin_light-locker.1000.uploaded	31
/var/lib/AccountsService/users/gdm.GDQ4M1	31
Static File Info	31
General	31
Static ELF Info	31
ELF header	32
Sections	32
Program Segments	32
Symbols	33
Network Behavior	51
Network Port Distribution	51
TCP Packets	51
DNS Queries	51
DNS Answers	51

System Behavior	51
Analysis Process: 6glL6GLh9R PID: 6234, Parent PID: 6129	51
General	51
File Activities	51
File Read	51
Analysis Process: 6glL6GLh9R PID: 6236, Parent PID: 6234	52
General	52
Analysis Process: 6glL6GLh9R PID: 6237, Parent PID: 6234	52
General	52
Analysis Process: 6glL6GLh9R PID: 6240, Parent PID: 6237	52
General	52
Analysis Process: 6glL6GLh9R PID: 6241, Parent PID: 6237	52
General	52
File Activities	52
File Deleted	52
File Read	52
File Written	52
Directory Enumerated	52
Analysis Process: 6glL6GLh9R PID: 6242, Parent PID: 6237	52
General	52
Analysis Process: systemd PID: 6249, Parent PID: 1	52
General	52
Analysis Process: journalctl PID: 6249, Parent PID: 1	53
General	53
File Activities	53
File Read	53
Analysis Process: systemd PID: 6266, Parent PID: 1	53
General	53
Analysis Process: systemd-journald PID: 6266, Parent PID: 1	53
General	53
File Activities	53
File Deleted	53
File Read	53
File Written	53
File Moved	53
Directory Enumerated	53
Directory Created	53
Analysis Process: systemd PID: 6270, Parent PID: 1	53
General	53
Analysis Process: journalctl PID: 6270, Parent PID: 1	53
General	54
File Activities	54
File Read	54
Analysis Process: systemd PID: 6323, Parent PID: 1	54
General	54
Analysis Process: whoopsie PID: 6323, Parent PID: 1	54
General	54
File Activities	54
File Created	54
File Read	54
File Written	54
File Moved	54
Directory Enumerated	54
Directory Created	54
Permission Modified	54
Analysis Process: systemd PID: 6327, Parent PID: 1	54
General	54
Analysis Process: dbus-daemon PID: 6327, Parent PID: 1	54
General	54
File Activities	55
File Read	55
Directory Enumerated	55
Analysis Process: systemd PID: 6328, Parent PID: 1860	55
General	55
Analysis Process: pulseaudio PID: 6328, Parent PID: 1860	55
General	55
File Activities	55
File Read	55
File Written	55
Directory Enumerated	55
Directory Created	55
Analysis Process: systemd PID: 6333, Parent PID: 1	55
General	55
Analysis Process: rtkit-daemon PID: 6333, Parent PID: 1	55
General	55
File Activities	55
File Read	55
Analysis Process: systemd PID: 6336, Parent PID: 1	55
General	55
Analysis Process: systemd-logind PID: 6336, Parent PID: 1	56
General	56
File Activities	56
File Deleted	56
File Read	56
File Written	56
File Moved	56
Directory Enumerated	56
Directory Created	56
Permission Modified	56
Analysis Process: systemd PID: 6399, Parent PID: 1	56
General	56
Analysis Process: polkitd PID: 6399, Parent PID: 1	56
General	56
File Activities	56
File Read	56
Directory Enumerated	56
Directory Created	56

Analysis Process: systemd PID: 6404, Parent PID: 1	56
General	56
Analysis Process: agetty PID: 6404, Parent PID: 1	56
General	57
File Activities	57
File Read	57
File Written	57
Owner / Group Modified	57
Permission Modified	57
Analysis Process: systemd PID: 6406, Parent PID: 1	57
General	57
Analysis Process: rsyslogd PID: 6406, Parent PID: 1	57
General	57
File Activities	57
File Read	57
File Written	57
Directory Enumerated	57
Analysis Process: gdm3 PID: 6408, Parent PID: 1320	57
General	57
Analysis Process: Default PID: 6408, Parent PID: 1320	57
General	57
File Activities	58
File Read	58
Analysis Process: systemd-udevd PID: 6409, Parent PID: 6306	58
General	58
Analysis Process: cached_setup_terminal.sh PID: 6409, Parent PID: 6306	58
General	58
File Activities	58
File Read	58
Analysis Process: gdm3 PID: 6410, Parent PID: 1320	58
General	58
Analysis Process: Default PID: 6410, Parent PID: 1320	58
General	58
File Activities	58
File Read	58
Analysis Process: gdm3 PID: 6411, Parent PID: 1320	58
General	58
Analysis Process: Default PID: 6411, Parent PID: 1320	59
General	59
File Activities	59
File Read	59
Analysis Process: systemd PID: 6417, Parent PID: 1	59
General	59
Analysis Process: gpu-manager PID: 6417, Parent PID: 1	59
General	59
File Activities	59
File Deleted	59
File Read	59
File Written	59
Directory Enumerated	59
Analysis Process: gpu-manager PID: 6418, Parent PID: 6417	59
General	59
Analysis Process: sh PID: 6418, Parent PID: 6417	59
General	59
File Activities	60
File Read	60
Directory Enumerated	60
Analysis Process: sh PID: 6419, Parent PID: 6418	60
General	60
Analysis Process: grep PID: 6419, Parent PID: 6418	60
General	60
File Activities	60
File Read	60
Analysis Process: gpu-manager PID: 6420, Parent PID: 6417	60
General	60
Analysis Process: sh PID: 6420, Parent PID: 6417	60
General	60
File Activities	60
File Read	60
Directory Enumerated	60
Analysis Process: sh PID: 6421, Parent PID: 6420	60
General	60
Analysis Process: grep PID: 6421, Parent PID: 6420	61
General	61
File Activities	61
File Read	61
Analysis Process: gpu-manager PID: 6422, Parent PID: 6417	61
General	61
Analysis Process: sh PID: 6422, Parent PID: 6417	61
General	61
File Activities	61
File Read	61
Directory Enumerated	61
Analysis Process: sh PID: 6423, Parent PID: 6422	61
General	61
Analysis Process: grep PID: 6423, Parent PID: 6422	61
General	61
File Activities	62
File Read	62
Analysis Process: gpu-manager PID: 6424, Parent PID: 6417	62
General	62
Analysis Process: sh PID: 6424, Parent PID: 6417	62
General	62
File Activities	62

File Read	62
Directory Enumerated	62
Analysis Process: sh PID: 6425, Parent PID: 6424	62
General	62
Analysis Process: grep PID: 6425, Parent PID: 6424	62
General	62
File Activities	62
File Read	62
Analysis Process: gpu-manager PID: 6426, Parent PID: 6417	62
General	63
Analysis Process: sh PID: 6426, Parent PID: 6417	63
General	63
File Activities	63
File Read	63
Directory Enumerated	63
Analysis Process: sh PID: 6427, Parent PID: 6426	63
General	63
Analysis Process: grep PID: 6427, Parent PID: 6426	63
General	63
File Activities	63
File Read	63
Analysis Process: gpu-manager PID: 6428, Parent PID: 6417	63
General	63
Analysis Process: sh PID: 6428, Parent PID: 6417	63
General	64
File Activities	64
File Read	64
Directory Enumerated	64
Analysis Process: sh PID: 6429, Parent PID: 6428	64
General	64
Analysis Process: grep PID: 6429, Parent PID: 6428	64
General	64
File Activities	64
File Read	64
Analysis Process: gpu-manager PID: 6430, Parent PID: 6417	64
General	64
Analysis Process: sh PID: 6430, Parent PID: 6417	64
General	64
File Activities	64
File Read	64
Directory Enumerated	64
Analysis Process: sh PID: 6431, Parent PID: 6430	65
General	65
Analysis Process: grep PID: 6431, Parent PID: 6430	65
General	65
File Activities	65
File Read	65
Analysis Process: gpu-manager PID: 6433, Parent PID: 6417	65
General	65
Analysis Process: sh PID: 6433, Parent PID: 6417	65
General	65
File Activities	65
File Read	65
Directory Enumerated	65
Analysis Process: sh PID: 6435, Parent PID: 6433	65
General	65
Analysis Process: grep PID: 6435, Parent PID: 6433	66
General	66
File Activities	66
File Read	66
Analysis Process: systemd PID: 6439, Parent PID: 1	66
General	66
Analysis Process: generate-config PID: 6439, Parent PID: 1	66
General	66
File Activities	66
File Read	66
Directory Enumerated	66
Analysis Process: generate-config PID: 6440, Parent PID: 6439	66
General	66
Analysis Process: pkill PID: 6440, Parent PID: 6439	66
General	66
File Activities	66
File Read	66
Directory Enumerated	67
Analysis Process: systemd PID: 6441, Parent PID: 1	67
General	67
Analysis Process: gdm-wait-for-drm PID: 6441, Parent PID: 1	67
General	67
File Activities	67
File Read	67
Directory Enumerated	67
Analysis Process: systemd PID: 6446, Parent PID: 1	67
General	67
Analysis Process: gdm3 PID: 6446, Parent PID: 1	67
General	67
File Activities	67
File Deleted	67
File Read	67
File Written	67
Directory Created	67
Owner / Group Modified	67
Permission Modified	67
Analysis Process: gdm3 PID: 6451, Parent PID: 6446	67
General	67
File Activities	68

Directory Enumerated	68
Analysis Process: plymouth PID: 6451, Parent PID: 6446	68
General	68
File Activities	68
File Read	68
Analysis Process: gdm3 PID: 6470, Parent PID: 6446	68
General	68
File Activities	68
Directory Enumerated	68
Analysis Process: gdm-session-worker PID: 6470, Parent PID: 6446	68
General	68
File Activities	68
File Read	68
File Written	68
Directory Enumerated	68
Analysis Process: gdm-session-worker PID: 6474, Parent PID: 6470	68
General	68
Analysis Process: gdm-wayland-session PID: 6474, Parent PID: 6470	69
General	69
File Activities	69
File Read	69
Directory Created	69
Analysis Process: gdm-wayland-session PID: 6476, Parent PID: 6474	69
General	69
File Activities	69
Directory Enumerated	69
Analysis Process: dbus-daemon PID: 6476, Parent PID: 6474	69
General	69
File Activities	69
File Read	69
Directory Enumerated	69
Analysis Process: dbus-daemon PID: 6480, Parent PID: 6476	69
General	69
Analysis Process: dbus-daemon PID: 6481, Parent PID: 6480	69
General	69
File Activities	70
File Written	70
Analysis Process: false PID: 6481, Parent PID: 6480	70
General	70
File Activities	70
File Read	70
Analysis Process: gdm-wayland-session PID: 6482, Parent PID: 6474	70
General	70
File Activities	70
Directory Enumerated	70
Analysis Process: dbus-run-session PID: 6482, Parent PID: 6474	70
General	70
File Activities	70
File Read	70
Analysis Process: dbus-run-session PID: 6483, Parent PID: 6482	70
General	70
Analysis Process: dbus-daemon PID: 6483, Parent PID: 6482	70
General	70
File Activities	71
File Read	71
Directory Enumerated	71
Analysis Process: gdm3 PID: 6484, Parent PID: 6446	71
General	71
File Activities	71
Directory Enumerated	71
Analysis Process: Default PID: 6484, Parent PID: 6446	71
General	71
File Activities	71
File Read	71
Analysis Process: gdm3 PID: 6485, Parent PID: 6446	71
General	71
File Activities	71
Directory Enumerated	71
Analysis Process: Default PID: 6485, Parent PID: 6446	71
General	71
File Activities	71
File Read	71
Analysis Process: systemd PID: 6452, Parent PID: 1	72
General	72
Analysis Process: accounts-daemon PID: 6452, Parent PID: 1	72
General	72
File Activities	72
File Read	72
File Written	72
File Moved	72
Directory Enumerated	72
Directory Created	72
Permission Modified	72
Analysis Process: accounts-daemon PID: 6465, Parent PID: 6452	72
General	72
File Activities	72
Directory Enumerated	72
Analysis Process: language-validate PID: 6465, Parent PID: 6452	72
General	72
File Activities	72
File Read	72
Analysis Process: language-validate PID: 6466, Parent PID: 6465	72
General	72
Analysis Process: language-options PID: 6466, Parent PID: 6465	73
General	73
File Activities	73

File Read	73
Directory Enumerated	73
Analysis Process: language-options PID: 6467, Parent PID: 6466	73
General	73
Analysis Process: sh PID: 6467, Parent PID: 6466	73
General	73
File Activities	73
File Read	73
Analysis Process: sh PID: 6468, Parent PID: 6467	73
General	73
Analysis Process: locale PID: 6468, Parent PID: 6467	73
General	73
File Activities	74
File Read	74
Directory Enumerated	74
Analysis Process: sh PID: 6469, Parent PID: 6467	74
General	74
Analysis Process: grep PID: 6469, Parent PID: 6467	74
General	74
File Activities	74
File Read	74
Analysis Process: gvfsd-fuse PID: 6493, Parent PID: 2038	74
General	74
Analysis Process: fusemount PID: 6493, Parent PID: 2038	74
General	74
File Activities	74
File Read	74
Analysis Process: systemd PID: 6515, Parent PID: 1	74
General	74
Analysis Process: journalctl PID: 6515, Parent PID: 1	75
General	75
File Activities	75
File Read	75
Analysis Process: systemd PID: 6516, Parent PID: 1	75
General	75
Analysis Process: systemd-journald PID: 6516, Parent PID: 1	75
General	75
File Activities	75
File Deleted	75
File Read	75
File Written	75
File Moved	75
Directory Enumerated	75
Directory Created	75
Analysis Process: systemd PID: 6517, Parent PID: 1	75
General	75
Analysis Process: whoopsie PID: 6517, Parent PID: 1	75
General	75
File Activities	76
File Read	76
File Written	76
File Moved	76
Directory Enumerated	76
Directory Created	76
Permission Modified	76
Analysis Process: systemd PID: 6520, Parent PID: 1	76
General	76
Analysis Process: dbus-daemon PID: 6520, Parent PID: 1	76
General	76
File Activities	76
File Read	76
Directory Enumerated	76
Analysis Process: systemd PID: 6522, Parent PID: 1860	76
General	76
Analysis Process: pulseaudio PID: 6522, Parent PID: 1860	76
General	76
File Activities	76
File Read	76
File Written	76
Directory Enumerated	77
Directory Created	77
Analysis Process: systemd PID: 6526, Parent PID: 1	77
General	77
Analysis Process: systemd-logind PID: 6526, Parent PID: 1	77
General	77
File Activities	77
File Read	77
File Written	77
File Moved	77
Directory Enumerated	77
Directory Created	77
Permission Modified	77
Analysis Process: systemd PID: 6584, Parent PID: 1	77
General	77
Analysis Process: rtkit-daemon PID: 6584, Parent PID: 1	77
General	77
File Activities	77
File Read	77
Analysis Process: systemd PID: 6585, Parent PID: 1	77
General	77
Analysis Process: gpu-manager PID: 6585, Parent PID: 1	78
General	78
File Activities	78
File Deleted	78
File Read	78
File Written	78
Directory Enumerated	78

Analysis Process: gpu-manager PID: 6589, Parent PID: 6585	78
General	78
Analysis Process: sh PID: 6589, Parent PID: 6585	78
General	78
File Activities	78
File Read	78
Directory Enumerated	78
Analysis Process: sh PID: 6590, Parent PID: 6589	78
General	78
Analysis Process: grep PID: 6590, Parent PID: 6589	78
General	78
File Activities	79
File Read	79
Analysis Process: gpu-manager PID: 6596, Parent PID: 6585	79
General	79
Analysis Process: sh PID: 6596, Parent PID: 6585	79
General	79
File Activities	79
File Read	79
Directory Enumerated	79
Analysis Process: sh PID: 6597, Parent PID: 6596	79
General	79
Analysis Process: grep PID: 6597, Parent PID: 6596	79
General	79
File Activities	79
File Read	79
Analysis Process: gpu-manager PID: 6599, Parent PID: 6585	79
General	80
Analysis Process: sh PID: 6599, Parent PID: 6585	80
General	80
File Activities	80
File Read	80
Directory Enumerated	80
Analysis Process: sh PID: 6601, Parent PID: 6599	80
General	80
Analysis Process: grep PID: 6601, Parent PID: 6599	80
General	80
File Activities	80
File Read	80
Analysis Process: gpu-manager PID: 6602, Parent PID: 6585	80
General	80
Analysis Process: sh PID: 6602, Parent PID: 6585	80
General	81
File Activities	81
File Read	81
Directory Enumerated	81
Analysis Process: sh PID: 6604, Parent PID: 6602	81
General	81
Analysis Process: grep PID: 6604, Parent PID: 6602	81
General	81
File Activities	81
File Read	81
Analysis Process: gpu-manager PID: 6605, Parent PID: 6585	81
General	81
Analysis Process: sh PID: 6605, Parent PID: 6585	81
General	81
File Activities	81
File Read	81
Directory Enumerated	81
Analysis Process: sh PID: 6606, Parent PID: 6605	82
General	82
Analysis Process: grep PID: 6606, Parent PID: 6605	82
General	82
File Activities	82
File Read	82
Analysis Process: gpu-manager PID: 6607, Parent PID: 6585	82
General	82
Analysis Process: sh PID: 6607, Parent PID: 6585	82
General	82
File Activities	82
File Read	82
Directory Enumerated	82
Analysis Process: sh PID: 6608, Parent PID: 6607	82
General	82
Analysis Process: grep PID: 6608, Parent PID: 6607	83
General	83
File Activities	83
File Read	83
Analysis Process: gpu-manager PID: 6610, Parent PID: 6585	83
General	83
Analysis Process: sh PID: 6610, Parent PID: 6585	83
General	83
File Activities	83
File Read	83
Directory Enumerated	83
Analysis Process: sh PID: 6611, Parent PID: 6610	83
General	83
Analysis Process: grep PID: 6611, Parent PID: 6610	83
General	83
File Activities	84
File Read	84
Analysis Process: gpu-manager PID: 6615, Parent PID: 6585	84
General	84

Analysis Process: sh PID: 6615, Parent PID: 6585	84
General	84
File Activities	84
File Read	84
Directory Enumerated	84
Analysis Process: sh PID: 6616, Parent PID: 6615	84
General	84
Analysis Process: grep PID: 6616, Parent PID: 6615	84
General	84
File Activities	84
File Read	84
Analysis Process: systemd PID: 6588, Parent PID: 1	84
General	84
Analysis Process: polkitd PID: 6588, Parent PID: 1	85
General	85
File Activities	85
File Read	85
Directory Enumerated	85
Directory Created	85
Analysis Process: systemd PID: 6598, Parent PID: 1	85
General	85
Analysis Process: journalctl PID: 6598, Parent PID: 1	85
General	85
File Activities	85
File Read	85
Analysis Process: systemd PID: 6600, Parent PID: 1	85
General	85
Analysis Process:agetty PID: 6600, Parent PID: 1	85
General	85
File Activities	85
File Read	86
File Written	86
Owner / Group Modified	86
Permission Modified	86
Analysis Process: systemd PID: 6609, Parent PID: 1	86
General	86
Analysis Process: rsyslogd PID: 6609, Parent PID: 1	86
General	86
File Activities	86
File Read	86
File Written	86
Directory Enumerated	86
Analysis Process: systemd PID: 6620, Parent PID: 1	86
General	86
Analysis Process: generate-config PID: 6620, Parent PID: 1	86
General	86
File Activities	86
File Read	86
Directory Enumerated	86
Analysis Process: generate-config PID: 6623, Parent PID: 6620	86
General	86
Analysis Process: pkill PID: 6623, Parent PID: 6620	87
General	87
File Activities	87
File Read	87
Directory Enumerated	87
Analysis Process: systemd PID: 6622, Parent PID: 1	87
General	87
Analysis Process: journalctl PID: 6622, Parent PID: 1	87
General	87
File Activities	87
File Read	87
Analysis Process: systemd PID: 6624, Parent PID: 1860	87
General	87
Analysis Process: dbus-daemon PID: 6624, Parent PID: 1860	87
General	87
File Activities	88
File Read	88
Directory Enumerated	88
Directory Created	88
Analysis Process: systemd PID: 6625, Parent PID: 1	88
General	88
Analysis Process: systemd-journald PID: 6625, Parent PID: 1	88
General	88
File Activities	88
File Deleted	88
File Read	88
File Written	88
File Moved	88
Directory Enumerated	88
Directory Created	88
Analysis Process: systemd PID: 6628, Parent PID: 1	88
General	88
Analysis Process: gdm-wait-for-drm PID: 6628, Parent PID: 1	88
General	88
File Activities	88
File Read	88
Directory Enumerated	88
Analysis Process: systemd PID: 6629, Parent PID: 1	89
General	89
Analysis Process: whoopsie PID: 6629, Parent PID: 1	89
General	89
File Activities	89
File Read	89
File Written	89
File Moved	89
Directory Enumerated	89

Directory Created	89
Permission Modified	89
Analysis Process: systemd PID: 6634, Parent PID: 1	89
General	89
Analysis Process: dbus-daemon PID: 6634, Parent PID: 1	89
General	89
File Activities	89
File Read	89
Directory Enumerated	89
Analysis Process: systemd PID: 6635, Parent PID: 1860	89
General	89
Analysis Process: pulseaudio PID: 6635, Parent PID: 1860	90
General	90
File Activities	90
File Read	90
File Written	90
Directory Enumerated	90
Directory Created	90
Analysis Process: systemd PID: 6636, Parent PID: 1	90
General	90
Analysis Process: journalctl PID: 6636, Parent PID: 1	90
General	90
File Activities	90
File Read	90
Analysis Process: systemd PID: 6641, Parent PID: 1	90
General	90
Analysis Process: systemd-logind PID: 6641, Parent PID: 1	90
General	90
File Activities	91
File Deleted	91
File Read	91
File Written	91
File Moved	91
Directory Enumerated	91
Directory Created	91
Permission Modified	91
Analysis Process: systemd PID: 6698, Parent PID: 1	91
General	91
Analysis Process: rtkit-daemon PID: 6698, Parent PID: 1	91
General	91
File Activities	91
File Read	91
Analysis Process: systemd PID: 6703, Parent PID: 1	91
General	91
Analysis Process: polkitd PID: 6703, Parent PID: 1	91
General	91
File Activities	91
File Read	91
Directory Enumerated	91
Directory Created	91
Analysis Process: systemd PID: 6707, Parent PID: 1	92
General	92
Analysis Process: agetty PID: 6707, Parent PID: 1	92
General	92
Analysis Process: systemd PID: 6709, Parent PID: 1	92
General	92
Analysis Process: rsyslogd PID: 6709, Parent PID: 1	92
General	92
Analysis Process: systemd PID: 6716, Parent PID: 1	92
General	92
Analysis Process: gdm3 PID: 6716, Parent PID: 1	92
General	92
Analysis Process: gdm3 PID: 6719, Parent PID: 6716	93
General	93
Analysis Process: plymouth PID: 6719, Parent PID: 6716	93
General	93
Analysis Process: gdm3 PID: 6729, Parent PID: 6716	93
General	93
Analysis Process: gdm-session-worker PID: 6729, Parent PID: 6716	93
General	93
Analysis Process: gdm-session-worker PID: 6739, Parent PID: 6729	93
General	93
Analysis Process: gdm-wayland-session PID: 6739, Parent PID: 6729	93
General	93
Analysis Process: gdm-wayland-session PID: 6741, Parent PID: 6739	94
General	94
Analysis Process: dbus-daemon PID: 6741, Parent PID: 6739	94
General	94
Analysis Process: dbus-daemon PID: 6751, Parent PID: 6741	94
General	94
Analysis Process: dbus-daemon PID: 6752, Parent PID: 6751	94
General	94
Analysis Process: false PID: 6752, Parent PID: 6751	94
General	94
Analysis Process: gdm-wayland-session PID: 6753, Parent PID: 6739	94
General	94
Analysis Process: dbus-run-session PID: 6753, Parent PID: 6739	95
General	95
Analysis Process: gdm3 PID: 6754, Parent PID: 6716	95
General	95
Analysis Process: Default PID: 6754, Parent PID: 6716	95
General	95

Analysis Process: gdm3 PID: 6756, Parent PID: 6716	95
General	95
Analysis Process: Default PID: 6756, Parent PID: 6716	95
General	95
Analysis Process: systemd PID: 6720, Parent PID: 1	95
General	95
Analysis Process: accounts-daemon PID: 6720, Parent PID: 1	96
General	96
Analysis Process: accounts-daemon PID: 6724, Parent PID: 6720	96
General	96
Analysis Process: language-validate PID: 6724, Parent PID: 6720	96
General	96
Analysis Process: language-validate PID: 6725, Parent PID: 6724	96
General	96
Analysis Process: language-options PID: 6725, Parent PID: 6724	96
General	96
Analysis Process: language-options PID: 6726, Parent PID: 6725	96
General	96
Analysis Process: sh PID: 6726, Parent PID: 6725	97
General	97
Analysis Process: sh PID: 6727, Parent PID: 6726	97
General	97
Analysis Process: locale PID: 6727, Parent PID: 6726	97
General	97
Analysis Process: sh PID: 6728, Parent PID: 6726	97
General	97
Analysis Process: grep PID: 6728, Parent PID: 6726	97
General	97
Analysis Process: systemd PID: 6730, Parent PID: 1	97
General	97
Analysis Process: journalctl PID: 6730, Parent PID: 1	98
General	98
Analysis Process: systemd PID: 6734, Parent PID: 1	98
General	98
Analysis Process: systemd-journald PID: 6734, Parent PID: 1	98
General	98
Analysis Process: systemd PID: 6737, Parent PID: 1	98
General	98
Analysis Process: systemd PID: 6737, Parent PID: 1	98
General	98
Analysis Process: systemd PID: 6742, Parent PID: 6737	98
General	98
Analysis Process: systemd PID: 6743, Parent PID: 6742	99
General	99
Analysis Process: 30-systemd-environment-d-generator PID: 6743, Parent PID: 6742	99
General	99
Analysis Process: systemd PID: 6850, Parent PID: 6737	99
General	99
Analysis Process: systemctl PID: 6850, Parent PID: 6737	99
General	99
Analysis Process: systemd PID: 6855, Parent PID: 6737	99
General	99
Analysis Process: pulseaudio PID: 6855, Parent PID: 6737	99
General	99
Analysis Process: systemd PID: 6744, Parent PID: 1	100
General	100
Analysis Process: whoopsie PID: 6744, Parent PID: 1	100
General	100
Analysis Process: systemd PID: 6757, Parent PID: 1	100
General	100
Analysis Process: dbus-daemon PID: 6757, Parent PID: 1	100
General	100
Analysis Process: systemd PID: 6759, Parent PID: 1860	100
General	100
Analysis Process: pulseaudio PID: 6759, Parent PID: 1860	100
General	100
Analysis Process: systemd PID: 6762, Parent PID: 1	101
General	101
Analysis Process: systemd-logind PID: 6762, Parent PID: 1	101
General	101
Analysis Process: systemd PID: 6821, Parent PID: 1	101
General	101
Analysis Process: rtkit-daemon PID: 6821, Parent PID: 1	101
General	101
Analysis Process: systemd PID: 6824, Parent PID: 1	101
General	101
Analysis Process: polkitd PID: 6824, Parent PID: 1	101
General	101
Analysis Process: systemd PID: 6825, Parent PID: 1	102
General	102
Analysis Process: gpu-manager PID: 6825, Parent PID: 1	102
General	102
Analysis Process: gpu-manager PID: 6827, Parent PID: 6825	102
General	102
Analysis Process: sh PID: 6827, Parent PID: 6825	102
General	102
Analysis Process: sh PID: 6828, Parent PID: 6827	102

General	102
Analysis Process: grep PID: 6828, Parent PID: 6827	102
General	102
Analysis Process: gpu-manager PID: 6832, Parent PID: 6825	103
General	103
Analysis Process: sh PID: 6832, Parent PID: 6825	103
General	103
Analysis Process: sh PID: 6833, Parent PID: 6832	103
General	103
Analysis Process: grep PID: 6833, Parent PID: 6832	103
General	103
Analysis Process: gpu-manager PID: 6834, Parent PID: 6825	103
General	103
Analysis Process: sh PID: 6834, Parent PID: 6825	103
General	103
Analysis Process: sh PID: 6835, Parent PID: 6834	104
General	104
Analysis Process: grep PID: 6835, Parent PID: 6834	104
General	104
Analysis Process: gpu-manager PID: 6837, Parent PID: 6825	104
General	104
Analysis Process: sh PID: 6837, Parent PID: 6825	104
General	104
Analysis Process: sh PID: 6838, Parent PID: 6837	104
General	104
Analysis Process: grep PID: 6838, Parent PID: 6837	104
General	104
Analysis Process: gpu-manager PID: 6845, Parent PID: 6825	105
General	105
Analysis Process: sh PID: 6845, Parent PID: 6825	105
General	105
Analysis Process: sh PID: 6846, Parent PID: 6845	105
General	105
Analysis Process: grep PID: 6846, Parent PID: 6845	105
General	105
Analysis Process: gpu-manager PID: 6847, Parent PID: 6825	105
General	105
Analysis Process: sh PID: 6847, Parent PID: 6825	106
General	106
Analysis Process: sh PID: 6848, Parent PID: 6847	106
General	106
Analysis Process: grep PID: 6848, Parent PID: 6847	106
General	106
Analysis Process: gpu-manager PID: 6851, Parent PID: 6825	106
General	106
Analysis Process: sh PID: 6851, Parent PID: 6825	106
General	106
Analysis Process: sh PID: 6852, Parent PID: 6851	106
General	106
Analysis Process: grep PID: 6852, Parent PID: 6851	107
General	107
Analysis Process: gpu-manager PID: 6853, Parent PID: 6825	107
General	107
Analysis Process: sh PID: 6853, Parent PID: 6825	107
General	107
Analysis Process: sh PID: 6854, Parent PID: 6853	107
General	107
Analysis Process: grep PID: 6854, Parent PID: 6853	107
General	107
Analysis Process: systemd PID: 6826, Parent PID: 1	107
General	107
Analysis Process: agetty PID: 6826, Parent PID: 1	108
General	108
Analysis Process: systemd PID: 6836, Parent PID: 1	108
General	108
Analysis Process: rsyslogd PID: 6836, Parent PID: 1	108
General	108
Analysis Process: systemd PID: 6841, Parent PID: 1	108
General	108
Analysis Process: journalctl PID: 6841, Parent PID: 1	108
General	108
Analysis Process: systemd PID: 6856, Parent PID: 1	108
General	108
Analysis Process: journalctl PID: 6856, Parent PID: 1	109
General	109
Analysis Process: systemd PID: 6857, Parent PID: 1	109
General	109
Analysis Process: systemd-journald PID: 6857, Parent PID: 1	109
General	109
Analysis Process: systemd PID: 6862, Parent PID: 1860	109
General	109
Analysis Process: dbus-daemon PID: 6862, Parent PID: 1860	109
General	109
Analysis Process: systemd PID: 6863, Parent PID: 1	109
General	109
Analysis Process: generate-config PID: 6863, Parent PID: 1	110
General	110

Analysis Process: generate-config PID: 6864, Parent PID: 6863	110
General	110
Analysis Process: pkill PID: 6864, Parent PID: 6863	110
General	110
Analysis Process: systemd PID: 6867, Parent PID: 1	110
General	110
Analysis Process: whoopsie PID: 6867, Parent PID: 1	110
General	110
Analysis Process: systemd PID: 6868, Parent PID: 1	110
General	110
Analysis Process: gdm-wait-for-drm PID: 6868, Parent PID: 1	111
General	111
Analysis Process: systemd PID: 6870, Parent PID: 1	111
General	111
Analysis Process: dbus-daemon PID: 6870, Parent PID: 1	111
General	111
Analysis Process: systemd PID: 6871, Parent PID: 1860	111
General	111
Analysis Process: pulseaudio PID: 6871, Parent PID: 1860	111
General	111
Analysis Process: systemd PID: 6874, Parent PID: 1	111
General	111
Analysis Process: systemd-logind PID: 6874, Parent PID: 1	112
General	112
Analysis Process: systemd PID: 6932, Parent PID: 1	112
General	112
Analysis Process: rtkit-daemon PID: 6932, Parent PID: 1	112
General	112
Analysis Process: systemd PID: 6935, Parent PID: 1	112
General	112
Analysis Process: journalctl PID: 6935, Parent PID: 1	112
General	112
Analysis Process: systemd PID: 6939, Parent PID: 1	112
General	112
Analysis Process: polkitd PID: 6939, Parent PID: 1	113
General	113
Analysis Process: systemd PID: 6944, Parent PID: 1	113
General	113
Analysis Process: agetty PID: 6944, Parent PID: 1	113
General	113
Analysis Process: systemd PID: 6945, Parent PID: 1	113
General	113
Analysis Process: rsyslogd PID: 6945, Parent PID: 1	113
General	113
Analysis Process: systemd PID: 6952, Parent PID: 1	113
General	113
Analysis Process: journalctl PID: 6952, Parent PID: 1	114
General	114
Analysis Process: systemd PID: 6953, Parent PID: 1	114
General	114
Analysis Process: systemd-journald PID: 6953, Parent PID: 1	114
General	114
Analysis Process: systemd PID: 6954, Parent PID: 1	114
General	114
Analysis Process: gdm3 PID: 6954, Parent PID: 1	114
General	114
Analysis Process: gdm3 PID: 6957, Parent PID: 6954	114
General	114
Analysis Process: plymouth PID: 6957, Parent PID: 6954	115
General	115
Analysis Process: gdm3 PID: 6969, Parent PID: 6954	115
General	115
Analysis Process: gdm-session-worker PID: 6969, Parent PID: 6954	115
General	115
Analysis Process: systemd PID: 6958, Parent PID: 1	115
General	115
Analysis Process: accounts-daemon PID: 6958, Parent PID: 1	115
General	115
Analysis Process: accounts-daemon PID: 6964, Parent PID: 6958	115
General	115
Analysis Process: language-validate PID: 6964, Parent PID: 6958	116
General	116
Analysis Process: language-validate PID: 6965, Parent PID: 6964	116
General	116
Analysis Process: language-options PID: 6965, Parent PID: 6964	116
General	116
Analysis Process: language-options PID: 6966, Parent PID: 6965	116
General	116
Analysis Process: sh PID: 6966, Parent PID: 6965	116
General	116
Analysis Process: sh PID: 6967, Parent PID: 6966	116
General	116
Analysis Process: locale PID: 6967, Parent PID: 6966	117
General	117
Analysis Process: sh PID: 6968, Parent PID: 6966	117
General	117
Analysis Process: grep PID: 6968, Parent PID: 6966	117

General	117
Analysis Process: systemd PID: 6973, Parent PID: 1	117
General	117
Analysis Process: whoopsie PID: 6973, Parent PID: 1	117
General	117

Linux Analysis Report

6gIL6GLh9R

Overview

General Information

Sample Name:	6gIL6GLh9R
Analysis ID:	635071
MD5:	6dfcca37a6b146...
SHA1:	d96baef8427ad9..
SHA256:	eed19f89eba4f0c..
Tags:	32 arm elf gafgyt
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Mirai

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

Yara detected Mirai

Multi AV Scanner detection for subm...

Reads system files that contain rec...

Contains symbols with names comm...

Sample tries to kill multiple process...

Sample reads /proc/mounts (often u...

Executes the "kill" or "pkill" comma...

Reads CPU information from /sys in...

Yara signature match

Executes the "grep" command used...

Reads system information from the ...

Classification

Analysis Advice

- Static ELF header machine description suggests that the sample might not execute correctly on this machine.
- Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635071
Start date and time: 27/05/202212:24:05	2022-05-27 12:24:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6gIL6GLh9R
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:	mal72.spre.troj.lin@0/161@7/0

Warnings

Runtime Messages

Command:	/tmp/6gIL6GLh9R
PID:	6234
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	VegaSec-KATANA001
Standard Error:	

Process Tree

- system is Inxubuntu20
 - 6gIL6GLh9R (PID: 6234, Parent: 6129, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/6gIL6GLh9R
 - 6gIL6GLh9R New Fork (PID: 6236, Parent: 6234)
 - 6gIL6GLh9R New Fork (PID: 6237, Parent: 6234)
 - 6gIL6GLh9R New Fork (PID: 6240, Parent: 6237)
 - 6gIL6GLh9R New Fork (PID: 6241, Parent: 6237)
 - 6gIL6GLh9R New Fork (PID: 6242, Parent: 6237)
 - systemd New Fork (PID: 6249, Parent: 1)
 - journalctl (PID: 6249, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
 - systemd New Fork (PID: 6266, Parent: 1)
 - systemd-journald (PID: 6266, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
 - systemd New Fork (PID: 6270, Parent: 1)
 - journalctl (PID: 6270, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
 - systemd New Fork (PID: 6323, Parent: 1)
 - whoopsie (PID: 6323, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
 - systemd New Fork (PID: 6327, Parent: 1)
 - dbus-daemon (PID: 6327, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
 - systemd New Fork (PID: 6328, Parent: 1860)
 - pulseaudio (PID: 6328, Parent: 1860, MD5: 0c3b4c789d8ffb12b5507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
 - systemd New Fork (PID: 6333, Parent: 1)
 - rtkit-daemon (PID: 6333, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
 - systemd New Fork (PID: 6336, Parent: 1)
 - systemd-logind (PID: 6336, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaef) Arguments: /lib/systemd/systemd-logind
 - systemd New Fork (PID: 6399, Parent: 1)
 - polkitd (PID: 6399, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
 - systemd New Fork (PID: 6404, Parent: 1)
 - agetty (PID: 6404, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\\u" --noclear tty2 linux
 - systemd New Fork (PID: 6406, Parent: 1)
 - rsyslogd (PID: 6406, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
 - gdm3 New Fork (PID: 6408, Parent: 1320)
 - Default (PID: 6408, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - systemd-udevd New Fork (PID: 6409, Parent: 6306)
 - cached_setup_terminal.sh (PID: 6409, Parent: 6306, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/console-setup/cached_setup_terminal.sh vcs2
 - gdm3 New Fork (PID: 6410, Parent: 1320)
 - Default (PID: 6410, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - gdm3 New Fork (PID: 6411, Parent: 1320)
 - Default (PID: 6411, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - systemd New Fork (PID: 6417, Parent: 1)
 - gpu-manager (PID: 6417, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
 - gpu-manager New Fork (PID: 6418, Parent: 6417)
 - sh (PID: 6418, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*nvidia[[:space:]]*\$\' /etc/modprobe.d/*.conf"
 - sh New Fork (PID: 6419, Parent: 6418)
 - grep (PID: 6419, Parent: 6418, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
 - gpu-manager New Fork (PID: 6420, Parent: 6417)
 - sh (PID: 6420, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*nvidia[[:space:]]*\$\' /lib/modprobe.d/*.conf"
 - sh New Fork (PID: 6421, Parent: 6420)
 - grep (PID: 6421, Parent: 6420, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
 - gpu-manager New Fork (PID: 6422, Parent: 6417)
 - sh (PID: 6422, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*radeon[[:space:]]*\$\' /etc/modprobe.d/*.conf"
 - sh New Fork (PID: 6423, Parent: 6422)
 - grep (PID: 6423, Parent: 6422, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
 - gpu-manager New Fork (PID: 6424, Parent: 6417)
 - sh (PID: 6424, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*radeon[[:space:]]*\$\' /lib/modprobe.d/*.conf"
 - sh New Fork (PID: 6425, Parent: 6424)
 - grep (PID: 6425, Parent: 6424, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
 - gpu-manager New Fork (PID: 6426, Parent: 6417)
 - sh (PID: 6426, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*amdgpu[[:space:]]*\$\' /etc/modprobe.d/*.conf"
 - sh New Fork (PID: 6427, Parent: 6426)
 - grep (PID: 6427, Parent: 6426, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
 - gpu-manager New Fork (PID: 6428, Parent: 6417)
 - sh (PID: 6428, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*amdgpu[[:space:]]*\$\' /lib/modprobe.d/*.conf"
 - sh New Fork (PID: 6429, Parent: 6428)
 - grep (PID: 6429, Parent: 6428, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
 - gpu-manager New Fork (PID: 6430, Parent: 6417)
 - sh (PID: 6430, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \\'^blacklist.*nouveau[[:space:]]*\$\' /etc/modprobe.d/*.conf"
 - sh New Fork (PID: 6431, Parent: 6430)
 - grep (PID: 6431, Parent: 6430, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf

- [gpu-manager](#) New Fork (PID: 6433, Parent: 6417)
- [sh](#) (PID: 6433, Parent: 6417, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /lib/modprobe.d/*conf"
 - [sh](#) New Fork (PID: 6435, Parent: 6433)
 - [grep](#) (PID: 6435, Parent: 6433, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- [systemd](#) New Fork (PID: 6439, Parent: 1)
- [generate-config](#) (PID: 6439, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
 - [generate-config](#) New Fork (PID: 6440, Parent: 6439)
 - [pkill](#) (PID: 6440, Parent: 6439, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- [systemd](#) New Fork (PID: 6441, Parent: 1)
- [gdm-wait-for-drm](#) (PID: 6441, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- [systemd](#) New Fork (PID: 6446, Parent: 1)
- [gdm3](#) (PID: 6446, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
 - [gdm3](#) New Fork (PID: 6451, Parent: 6446)
 - [plymouth](#) (PID: 6451, Parent: 6446, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
 - [gdm3](#) New Fork (PID: 6470, Parent: 6446)
 - [gdm-session-worker](#) (PID: 6470, Parent: 6446, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
 - [gdm-session-worker](#) New Fork (PID: 6474, Parent: 6470)
 - [gdm-wayland-session](#) (PID: 6474, Parent: 6470, 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: 6476, Parent: 6474)
 - [dbus-daemon](#) (PID: 6476, Parent: 6474, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 3 --session
 - [dbus-daemon](#) New Fork (PID: 6480, Parent: 6476)
 - [dbus-daemon](#) New Fork (PID: 6481, Parent: 6480)
 - [false](#) (PID: 6481, Parent: 6480, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - [gdm-wayland-session](#) New Fork (PID: 6482, Parent: 6474)
 - [dbus-run-session](#) (PID: 6482, Parent: 6474, MD5: 245f3ef6a268850b33b0225a8b753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
 - [dbus-run-session](#) New Fork (PID: 6483, Parent: 6482)
 - [dbus-daemon](#) (PID: 6483, Parent: 6482, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
 - [gdm3](#) New Fork (PID: 6484, Parent: 6446)
 - [Default](#) (PID: 6484, Parent: 6446, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - [gdm3](#) New Fork (PID: 6485, Parent: 6446)
 - [Default](#) (PID: 6485, Parent: 6446, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - [systemd](#) New Fork (PID: 6452, Parent: 1)
 - [accounts-daemon](#) (PID: 6452, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accounts-service/accounts-daemon
 - [accounts-daemon](#) New Fork (PID: 6465, Parent: 6452)
 - [language-validate](#) (PID: 6465, Parent: 6452, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
 - [language-validate](#) New Fork (PID: 6466, Parent: 6465)
 - [language-options](#) (PID: 6466, Parent: 6465, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
 - [language-options](#) New Fork (PID: 6467, Parent: 6466)
 - [sh](#) (PID: 6467, Parent: 6466, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
 - [sh](#) New Fork (PID: 6468, Parent: 6467)
 - [locale](#) (PID: 6468, Parent: 6467, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
 - [sh](#) New Fork (PID: 6469, Parent: 6467)
 - [grep](#) (PID: 6469, Parent: 6467, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
 - [gvfsd-fuse](#) New Fork (PID: 6493, Parent: 2038)
 - [fusermount](#) (PID: 6493, Parent: 2038, MD5: 576a1b135c82bdc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
 - [systemd](#) New Fork (PID: 6515, Parent: 1)
 - [journalctl](#) (PID: 6515, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
 - [systemd](#) New Fork (PID: 6516, Parent: 1)
 - [systemd-journald](#) (PID: 6516, Parent: 1, MD5: 474667ece6cecbe5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
 - [systemd](#) New Fork (PID: 6517, Parent: 1)
 - [whoopsie](#) (PID: 6517, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
 - [systemd](#) New Fork (PID: 6520, Parent: 1)
 - [dbus-daemon](#) (PID: 6520, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
 - [systemd](#) New Fork (PID: 6522, Parent: 1860)
 - [pulseaudio](#) (PID: 6522, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
 - [systemd](#) New Fork (PID: 6526, Parent: 1)
 - [systemd-logind](#) (PID: 6526, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeeef) Arguments: /lib/systemd/systemd-logind
 - [systemd](#) New Fork (PID: 6584, Parent: 1)
 - [rtkit-daemon](#) (PID: 6584, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ff7) Arguments: /usr/libexec/rtkit-daemon
 - [systemd](#) New Fork (PID: 6585, Parent: 1)
 - [gpu-manager](#) (PID: 6585, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
 - [gpu-manager](#) New Fork (PID: 6589, Parent: 6585)
 - [sh](#) (PID: 6589, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[:space:]]*\$\" /etc/modprobe.d/*conf"
 - [sh](#) New Fork (PID: 6590, Parent: 6589)
 - [grep](#) (PID: 6590, Parent: 6589, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
 - [gpu-manager](#) New Fork (PID: 6596, Parent: 6585)
 - [sh](#) (PID: 6596, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[:space:]]*\$\" /lib/modprobe.d/*conf"
 - [sh](#) New Fork (PID: 6597, Parent: 6596)
 - [grep](#) (PID: 6597, Parent: 6596, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
 - [gpu-manager](#) New Fork (PID: 6599, Parent: 6585)
 - [sh](#) (PID: 6599, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[:space:]]*\$\" /etc/modprobe.d/*conf"
 - [sh](#) New Fork (PID: 6601, Parent: 6599)
 - [grep](#) (PID: 6601, Parent: 6599, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
 - [gpu-manager](#) New Fork (PID: 6602, Parent: 6585)
 - [sh](#) (PID: 6602, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[:space:]]*\$\" /lib/modprobe.d/*conf"
 - [sh](#) New Fork (PID: 6604, Parent: 6602)
 - [grep](#) (PID: 6604, Parent: 6602, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
 - [gpu-manager](#) New Fork (PID: 6605, Parent: 6585)

- o **sh** (PID: 6605, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -G \'^blacklist.*amdgpu[:space:]]*\$' /etc/modprobe.d/*.conf
 - **sh** New Fork (PID: 6606, Parent: 6605)
 - o **grep** (PID: 6606, Parent: 6605, MD5: 1e6bb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- **gpu-manager** New Fork (PID: 6607, Parent: 6585)
- o **sh** (PID: 6607, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \'^blacklist.*amdgpu[:space:]]*\$' /lib/modprobe.d/*.conf"
 - **sh** New Fork (PID: 6608, Parent: 6607)
 - o **grep** (PID: 6608, Parent: 6607, MD5: 1e6bb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- **gpu-manager** New Fork (PID: 6610, Parent: 6585)
- o **sh** (PID: 6610, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \'^blacklist.*nouveau[:space:]]*\$' /etc/modprobe.d/*.conf"
 - **sh** New Fork (PID: 6611, Parent: 6610)
 - o **grep** (PID: 6611, Parent: 6610, MD5: 1e6bb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- **gpu-manager** New Fork (PID: 6615, Parent: 6585)
- o **sh** (PID: 6615, Parent: 6585, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \'^blacklist.*nouveau[:space:]]*\$' /lib/modprobe.d/*.conf"
 - **sh** New Fork (PID: 6616, Parent: 6615)
 - o **grep** (PID: 6616, Parent: 6615, MD5: 1e6bb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- **systemd** New Fork (PID: 6588, Parent: 1)
- **polkitd** (PID: 6588, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- **systemd** New Fork (PID: 6598, Parent: 1)
- o **journalctl** (PID: 6598, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- **systemd** New Fork (PID: 6600, Parent: 1)
- o **agetty** (PID: 6600, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\\u" --noclear tty2 linux
- **systemd** New Fork (PID: 6609, Parent: 1)
- o **rsyslogd** (PID: 6609, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- **systemd** New Fork (PID: 6620, Parent: 1)
- o **generate-config** (PID: 6620, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
 - **generate-config** New Fork (PID: 6623, Parent: 6620)
 - o **pkll** (PID: 6623, Parent: 6620, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkll --signal HUP --uid gdm dconf-service
- **systemd** New Fork (PID: 6622, Parent: 1)
- o **journalctl** (PID: 6622, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- **systemd** New Fork (PID: 6624, Parent: 1860)
- o **dbus-daemon** (PID: 6624, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --noidfile --systemd-activation --syslog-only
- **systemd** New Fork (PID: 6625, Parent: 1)
- o **systemd-journald** (PID: 6625, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- **systemd** New Fork (PID: 6628, Parent: 1)
- o **gdm-wait-for-drm** (PID: 6628, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- **systemd** New Fork (PID: 6629, Parent: 1)
- o **whoopsie** (PID: 6629, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- **systemd** New Fork (PID: 6634, Parent: 1)
- o **dbus-daemon** (PID: 6634, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --noidfile --systemd-activation --syslog-only
- **systemd** New Fork (PID: 6635, Parent: 1860)
- o **pulseaudio** (PID: 6635, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- **systemd** New Fork (PID: 6636, Parent: 1)
- o **journalctl** (PID: 6636, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- **systemd** New Fork (PID: 6641, Parent: 1)
- o **systemd-logind** (PID: 6641, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeeef) Arguments: /lib/systemd/systemd-logind
- **systemd** New Fork (PID: 6698, Parent: 1)
- o **rtkit-daemon** (PID: 6698, Parent: 1, MD5: df0cac1db4ec95ac70f5b6e06b8ff7d) Arguments: /usr/libexec/rtkit-daemon
- **systemd** New Fork (PID: 6703, Parent: 1)
- o **polkitd** (PID: 6703, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- **systemd** New Fork (PID: 6707, Parent: 1)
- o **agetty** (PID: 6707, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\\u" --noclear tty2 linux
- **systemd** New Fork (PID: 6709, Parent: 1)
- o **rsyslogd** (PID: 6709, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- **systemd** New Fork (PID: 6716, Parent: 1)
- o **gdm3** (PID: 6716, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
 - **gdm3** New Fork (PID: 6719, Parent: 6716)
 - o **plymouth** (PID: 6719, Parent: 6716, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
 - **gdm3** New Fork (PID: 6729, Parent: 6716)
 - o **gdm-session-worker** (PID: 6729, Parent: 6716, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
 - **gdm-session-worker** New Fork (PID: 6739, Parent: 6729)
 - o **gdm-wayland-session** (PID: 6739, Parent: 6729, MD5: d3def63cf1e83f7b8a0f13b1744ff7c) Arguments: /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
 - **gdm-wayland-session** New Fork (PID: 6741, Parent: 6739)
 - o **dbus-daemon** (PID: 6741, Parent: 6739, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --print-address 3 --session
 - **dbus-daemon** New Fork (PID: 6751, Parent: 6741)
 - **dbus-daemon** New Fork (PID: 6752, Parent: 6751)
 - o **false** (PID: 6752, Parent: 6751, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
 - **gdm-wayland-session** New Fork (PID: 6753, Parent: 6739)
 - o **dbus-run-session** (PID: 6753, Parent: 6739, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
 - **gdm3** New Fork (PID: 6754, Parent: 6716)
 - o **Default** (PID: 6754, Parent: 6716, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - **gdm3** New Fork (PID: 6756, Parent: 6716)
 - o **Default** (PID: 6756, Parent: 6716, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
 - **systemd** New Fork (PID: 6720, Parent: 1)
 - o **accounts-daemon** (PID: 6720, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accounts-service/accounts-daemon
 - **accounts-daemon** New Fork (PID: 6724, Parent: 6720)
 - o **language-validate** (PID: 6724, Parent: 6720, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
 - **language-validate** New Fork (PID: 6725, Parent: 6724)
 - o **language-options** (PID: 6725, Parent: 6724, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options

- [language-options](#) New Fork (PID: 6726, Parent: 6725)
- [sh](#) (PID: 6726, Parent: 6725, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
 - [sh](#) New Fork (PID: 6727, Parent: 6726)
 - [locale](#) (PID: 6727, Parent: 6726, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
 - [sh](#) New Fork (PID: 6728, Parent: 6726)
 - [grep](#) (PID: 6728, Parent: 6726, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- [systemd](#) New Fork (PID: 6730, Parent: 1)
- [journalctl](#) (PID: 6730, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- [systemd](#) New Fork (PID: 6734, Parent: 1)
- [systemd-journald](#) (PID: 6734, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- [systemd](#) New Fork (PID: 6737, Parent: 1)
- [systemd](#) (PID: 6737, Parent: 1, MD5: 9b2bec7092a40488108543f9334aab75) Arguments: /lib/systemd/systemd --user
 - [systemd](#) New Fork (PID: 6742, Parent: 6737)
 - [systemd](#) New Fork (PID: 6743, Parent: 6742)
 - [30-systemd-environment-d-generator](#) (PID: 6743, Parent: 6742, MD5: 42417da8051ba8ee0eea7854c62d99ca) Arguments: /usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
 - [systemd](#) New Fork (PID: 6850, Parent: 6737)
 - [systemctl](#) (PID: 6850, Parent: 6737, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: /bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
 - [systemd](#) New Fork (PID: 6855, Parent: 6737)
 - [pulseaudio](#) (PID: 6855, Parent: 6737, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- [systemd](#) New Fork (PID: 6744, Parent: 1)
- [whoopsie](#) (PID: 6744, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- [systemd](#) New Fork (PID: 6757, Parent: 1)
- [dbus-daemon](#) (PID: 6757, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- [systemd](#) New Fork (PID: 6759, Parent: 1860)
- [pulseaudio](#) (PID: 6759, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- [systemd](#) New Fork (PID: 6762, Parent: 1)
- [systemd-logind](#) (PID: 6762, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeeef) Arguments: /lib/systemd/systemd-logind
- [systemd](#) New Fork (PID: 6821, Parent: 1)
- [rtkit-daemon](#) (PID: 6821, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ff7d) Arguments: /usr/libexec/rtkit-daemon
- [systemd](#) New Fork (PID: 6824, Parent: 1)
- [polkitd](#) (PID: 6824, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- [systemd](#) New Fork (PID: 6825, Parent: 1)
- [gpu-manager](#) (PID: 6825, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
 - [gpu-manager](#) New Fork (PID: 6827, Parent: 6825)
 - [sh](#) (PID: 6827, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[:space:]]*\$\" /etc/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6828, Parent: 6827)
 - [grep](#) (PID: 6828, Parent: 6827, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- [gpu-manager](#) New Fork (PID: 6832, Parent: 6825)
- [sh](#) (PID: 6832, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nvidia[:space:]]*\$\" /lib/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6833, Parent: 6832)
 - [grep](#) (PID: 6833, Parent: 6832, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nvidia[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- [gpu-manager](#) New Fork (PID: 6834, Parent: 6825)
- [sh](#) (PID: 6834, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[:space:]]*\$\" /etc/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6835, Parent: 6834)
 - [grep](#) (PID: 6835, Parent: 6834, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- [gpu-manager](#) New Fork (PID: 6837, Parent: 6825)
- [sh](#) (PID: 6837, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*radeon[:space:]]*\$\" /lib/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6838, Parent: 6837)
 - [grep](#) (PID: 6838, Parent: 6837, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*radeon[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- [gpu-manager](#) New Fork (PID: 6845, Parent: 6825)
- [sh](#) (PID: 6845, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[:space:]]*\$\" /etc/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6846, Parent: 6845)
 - [grep](#) (PID: 6846, Parent: 6845, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- [gpu-manager](#) New Fork (PID: 6847, Parent: 6825)
- [sh](#) (PID: 6847, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*amdgpu[:space:]]*\$\" /lib/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6848, Parent: 6847)
 - [grep](#) (PID: 6848, Parent: 6847, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*amdgpu[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- [gpu-manager](#) New Fork (PID: 6851, Parent: 6825)
- [sh](#) (PID: 6851, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /etc/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6852, Parent: 6851)
 - [grep](#) (PID: 6852, Parent: 6851, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
- [gpu-manager](#) New Fork (PID: 6853, Parent: 6825)
- [sh](#) (PID: 6853, Parent: 6825, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /lib/modprobe.d/*.conf"
 - [sh](#) New Fork (PID: 6854, Parent: 6853)
 - [grep](#) (PID: 6854, Parent: 6853, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -G ^blacklist.*nouveau[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
- [systemd](#) New Fork (PID: 6826, Parent: 1)
- [agetty](#) (PID: 6826, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "p -- \u" --noclear tty2 linux
- [systemd](#) New Fork (PID: 6836, Parent: 1)
- [rsyslogd](#) (PID: 6836, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- [systemd](#) New Fork (PID: 6841, Parent: 1)
- [journalctl](#) (PID: 6841, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush

- [systemd](#) New Fork (PID: 6856, Parent: 1)
- [journalctl](#) (PID: 6856, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- [systemd](#) New Fork (PID: 6857, Parent: 1)
- [systemd-journald](#) (PID: 6857, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- [systemd](#) New Fork (PID: 6862, Parent: 1860)
- [dbus-daemon](#) (PID: 6862, Parent: 1860, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- [systemd](#) New Fork (PID: 6863, Parent: 1)
- [generate-config](#) (PID: 6863, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
 - [generate-config](#) New Fork (PID: 6864, Parent: 6863)
 - [pkill](#) (PID: 6864, Parent: 6863, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill --signal HUP --uid gdm dconf-service
- [systemd](#) New Fork (PID: 6867, Parent: 1)
- [whoopsie](#) (PID: 6867, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- [systemd](#) New Fork (PID: 6868, Parent: 1)
- [gdm-wait-for-drm](#) (PID: 6868, Parent: 1, MD5: 82043ba752c6930b4e6aaea2f7747545) Arguments: /usr/lib/gdm3/gdm-wait-for-drm
- [systemd](#) New Fork (PID: 6870, Parent: 1)
- [dbus-daemon](#) (PID: 6870, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- [systemd](#) New Fork (PID: 6871, Parent: 1860)
- [pulseaudio](#) (PID: 6871, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- [systemd](#) New Fork (PID: 6874, Parent: 1)
- [systemd-logind](#) (PID: 6874, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeeef) Arguments: /lib/systemd/systemd-logind
- [systemd](#) New Fork (PID: 6932, Parent: 1)
- [rtkit-daemon](#) (PID: 6932, Parent: 1, MD5: df0cac1db4ec95ac70f5b6e06b8ffdf7) Arguments: /usr/libexec/rtkit-daemon
- [systemd](#) New Fork (PID: 6935, Parent: 1)
- [journalctl](#) (PID: 6935, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- [systemd](#) New Fork (PID: 6939, Parent: 1)
- [polkitd](#) (PID: 6939, Parent: 1, MD5: 8efc9b4b5b524210ad2ea1954a9d0e69) Arguments: /usr/lib/policykit-1/polkitd --no-debug
- [systemd](#) New Fork (PID: 6944, Parent: 1)
- [agetty](#) (PID: 6944, Parent: 1, MD5: 3a374724ba7e863768139bdd60ca36f7) Arguments: /sbin/agetty -o "-p -- \\\u" --noclear tty2 linux
- [systemd](#) New Fork (PID: 6945, Parent: 1)
- [rsyslogd](#) (PID: 6945, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- [systemd](#) New Fork (PID: 6952, Parent: 1)
- [journalctl](#) (PID: 6952, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- [systemd](#) New Fork (PID: 6953, Parent: 1)
- [systemd-journald](#) (PID: 6953, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- [systemd](#) New Fork (PID: 6954, Parent: 1)
- [gdm3](#) (PID: 6954, Parent: 1, MD5: 2492e2d8d34f9377e3e530a61a15674f) Arguments: /usr/sbin/gdm3
 - [gdm3](#) New Fork (PID: 6957, Parent: 6954)
 - [plymouth](#) (PID: 6957, Parent: 6954, MD5: 87003efd8dad470042f5e75360a8f49f) Arguments: plymouth --ping
 - [gdm3](#) New Fork (PID: 6969, Parent: 6954)
 - [gdm-session-worker](#) (PID: 6969, Parent: 6954, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
- [systemd](#) New Fork (PID: 6958, Parent: 1)
- [accounts-daemon](#) (PID: 6958, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accounts-service/accounts-daemon
 - [accounts-daemon](#) New Fork (PID: 6964, Parent: 6958)
 - [language-validate](#) (PID: 6964, Parent: 6958, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
 - [language-validate](#) New Fork (PID: 6965, Parent: 6964)
 - [language-options](#) (PID: 6965, Parent: 6964, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
 - [language-options](#) New Fork (PID: 6966, Parent: 6965)
 - [sh](#) (PID: 6966, Parent: 6965, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
 - [sh](#) New Fork (PID: 6967, Parent: 6966)
 - [locale](#) (PID: 6967, Parent: 6966, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
 - [sh](#) New Fork (PID: 6968, Parent: 6966)
 - [grep](#) (PID: 6968, Parent: 6966, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- [systemd](#) New Fork (PID: 6973, Parent: 1)
- [whoopsie](#) (PID: 6973, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- [cleanup](#)

Yara Signatures				
Initial Sample				
Source	Rule	Description	Author	Strings
6glL6GLh9R	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \Mozilla/5.0\ - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x171d8:\$xo1: \x18:/<994z`{e</li> <li>• 0x17250:\$xo1: \x18:/<994z`{e • 0x172c8:\$xo1: \x18:/<994z`{e</li> <li>• 0x1731c:\$xo1: \x18:/<994z`{e • 0x17394:\$xo1: \x18:/<994z`{e</li> <li>• 0x1740c:\$xo1: \x18:/<994z`{e • 0x17484:\$xo1: \x18:/<994z`{e</li> <li>• 0x174f4:\$xo1: \x18:/<994z`{e • 0x17570:\$xo1: \x18:/<994z`{e</li> <li>• 0x175c0:\$xo1: \x18:/<994z`{e
6glL6GLh9R	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6237.1.0000000024c9a23c.00000000c094cd33.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword 'Mozilla/5.0' - it uses yara's XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x3f00:\$xo1: \x18:/<994z`{e</li> <li>0x3f78:\$xo1: \x18:/<994z`{e 0x3ff0:\$xo1: \x18:/<994z`{e</li> <li>0x4048:\$xo1: \x18:/<994z`{e 0x40c0:\$xo1: \x18:/<994z`{e</li> <li>0x4138:\$xo1: \x18:/<994z`{e 0x41b8:\$xo1: \x18:/<994z`{e</li> <li>0x4230:\$xo1: \x18:/<994z`{e 0x42b0:\$xo1: \x18:/<994z`{e</li> <li>0x4308:\$xo1: \x18:/<994z`{e
6240.1.0000000065830d93.00000000a6543536.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword 'Mozilla/5.0' - it uses yara's XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x171d8:\$xo1: \x18:/<994z`{e</li> <li>0x17250:\$xo1: \x18:/<994z`{e 0x172c8:\$xo1: \x18:/<994z`{e</li> <li>0x1731c:\$xo1: \x18:/<994z`{e 0x17394:\$xo1: \x18:/<994z`{e</li> <li>0x1740c:\$xo1: \x18:/<994z`{e 0x17484:\$xo1: \x18:/<994z`{e</li> <li>0x174f4:\$xo1: \x18:/<994z`{e 0x17570:\$xo1: \x18:/<994z`{e</li> <li>0x175c0:\$xo1: \x18:/<994z`{e
6237.1.0000000065830d93.00000000a6543536.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword 'Mozilla/5.0' - it uses yara's XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x171d8:\$xo1: \x18:/<994z`{e</li> <li>0x17250:\$xo1: \x18:/<994z`{e 0x172c8:\$xo1: \x18:/<994z`{e</li> <li>0x1731c:\$xo1: \x18:/<994z`{e 0x17394:\$xo1: \x18:/<994z`{e</li> <li>0x1740c:\$xo1: \x18:/<994z`{e 0x17484:\$xo1: \x18:/<994z`{e</li> <li>0x174f4:\$xo1: \x18:/<994z`{e 0x17570:\$xo1: \x18:/<994z`{e</li> <li>0x175c0:\$xo1: \x18:/<994z`{e
6240.1.0000000024c9a23c.00000000c094cd33.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword 'Mozilla/5.0' - it uses yara's XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x3f00:\$xo1: \x18:/<994z`{e</li> <li>0x3f78:\$xo1: \x18:/<994z`{e 0x3ff0:\$xo1: \x18:/<994z`{e</li> <li>0x4048:\$xo1: \x18:/<994z`{e 0x40c0:\$xo1: \x18:/<994z`{e</li> <li>0x4138:\$xo1: \x18:/<994z`{e 0x41b8:\$xo1: \x18:/<994z`{e</li> <li>0x4230:\$xo1: \x18:/<994z`{e 0x42b0:\$xo1: \x18:/<994z`{e</li> <li>0x4308:\$xo1: \x18:/<994z`{e
6234.1.0000000024c9a23c.00000000c094cd33.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword 'Mozilla/5.0' - it uses yara's XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x3f00:\$xo1: \x18:/<994z`{e</li> <li>0x3f78:\$xo1: \x18:/<994z`{e 0x3ff0:\$xo1: \x18:/<994z`{e</li> <li>0x4048:\$xo1: \x18:/<994z`{e 0x40c0:\$xo1: \x18:/<994z`{e</li> <li>0x4138:\$xo1: \x18:/<994z`{e 0x41b8:\$xo1: \x18:/<994z`{e</li> <li>0x4230:\$xo1: \x18:/<994z`{e 0x42b0:\$xo1: \x18:/<994z`{e</li> <li>0x4308:\$xo1: \x18:/<994z`{e

Click to see the 5 entries

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

System Summary



Contains symbols with names commonly found in malware

Sample tries to kill multiple processes (SIGKILL)

Persistence and Installation Behavior



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

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
Valid Accounts	1 Scripting	1 Systemd Service	1 Systemd Service	1 Masquerading	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	LSASS Memory	1 System Owner/User Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Scripting	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Indicator Removal on Host	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

—

—



—

—

Source	Detection	Scanner	Label	Link
6glL6GLh9R	55%	Virustotal		Browse

—

—

①

—

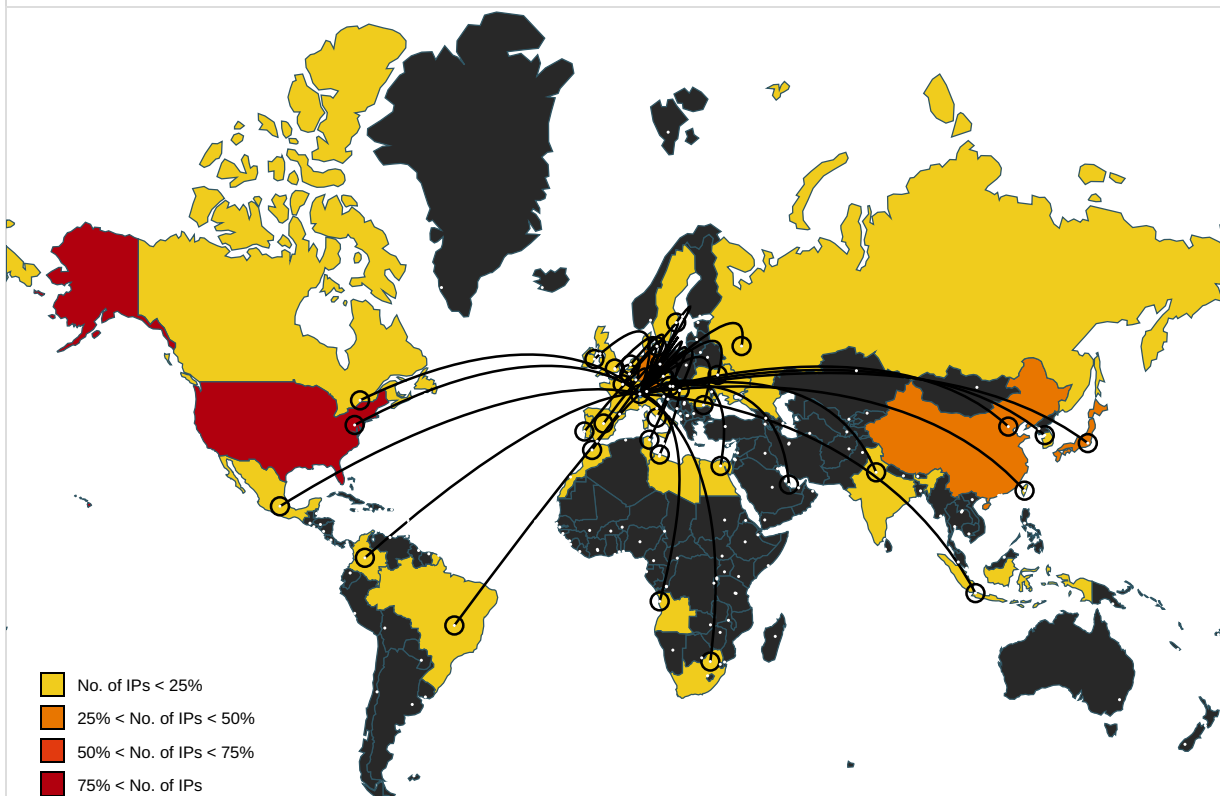
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	185.125.188.137	true	false		high

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
180.102.235.37	unknown	China		134756	CHINANET-NANJING-IDCCHINANETNanjingIDCnetworkCN	false
118.218.75.33	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
183.43.249.222	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
53.59.63.35	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
85.239.107.103	unknown	Germany		16097	HLKOMM04107LeipzigDE	false
180.38.220.68	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
160.218.230.61	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
110.46.44.140	unknown	Korea Republic of		9845	CJCKN-AS-KRLGHHelloVisionCorpKR	false
195.77.52.159	unknown	Spain		60493	FICOSA-ASES	false
117.248.227.5	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
168.224.103.243	unknown	United States		27435	OPSOURCE-INCUS	false
185.114.163.50	unknown	Ireland		34912	IFN-ASIE	false
66.142.12.181	unknown	United States		7018	ATT-INTERNET4US	false
164.69.149.11	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.37.22.59	unknown	Egypt		8452	TE-ASTE-ASEG	false
150.38.242.139	unknown	Japan		10010	TOKAITOKAICommunicationsCorporationJP	false
197.241.226.183	unknown	Angola		37081	movicel-asAO	false
77.197.0.249	unknown	France		15557	LDCOMNETFR	false
73.63.4.69	unknown	United States		7922	COMCAST-7922US	false
171.83.195.89	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
193.224.142.169	unknown	Hungary		1955	HBONE-ASHUNGARNETHU	false
149.119.66.93	unknown	United States		11872	SYRACUSE-UNIVERSITYUS	false
211.46.47.245	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
79.194.218.46	unknown	Germany		3320	DTAGInternetServiceprovideroptionsDE	false
86.36.155.182	unknown	Qatar		47901	MEEZAQA	false
59.11.110.116	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
89.154.120.125	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
196.82.255.189	unknown	Morocco		6713	IAM-ASMA	false
106.116.197.74	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
219.199.62.193	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
202.249.240.98	unknown	Japan		2506	SUPERCSINTTWESTCHUGOKUCORPORATIONJP	false
81.87.79.174	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
161.236.138.122	unknown	United States		396269	BPL-ASNUS	false
113.40.35.231	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
97.155.23.40	unknown	United States		6167	CELLCO-PARTUS	false
8.124.12.147	unknown	United States		3356	LEVEL3US	false
109.193.92.64	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
159.6.65.194	unknown	Canada		1906	NORTHROP-GRUMMANUS	false
27.242.146.18	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
72.8.160.227	unknown	United States		25761	STAMINUS-COMMUS	false
162.178.41.108	unknown	United States		21928	T-MOBILE-AS21928US	false
118.243.102.216	unknown	Japan		4685	ASAHI-NETAsahiNetJP	false
87.58.15.119	unknown	Denmark		3292	TDCTDCASDK	false
48.221.53.130	unknown	United States		2686	ATGS-MMD-ASUS	false
96.112.179.205	unknown	United States		7922	COMCAST-7922US	false
205.223.57.76	unknown	United States		32073	MCPS-K12-MD-US	false
41.169.50.109	unknown	South Africa		36937	Neotel-ASZA	false
73.74.56.155	unknown	United States		7922	COMCAST-7922US	false
1.34.218.58	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
75.156.126.48	unknown	Canada		852	ASN852CA	false
139.237.140.198	unknown	United States		1462	DNIC-ASBLK-01462-01463US	false
40.86.60.220	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
79.242.191.254	unknown	Germany		3320	DTAGInternetServiceprovideroptionsDE	false
157.69.228.108	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
24.249.185.198	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
108.124.109.216	unknown	United States		10507	SPCSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
124.25.151.81	unknown	Japan		2510	INFOWEBFUJITSULIMITE DJP	false
118.118.129.108	unknown	China		139220	CHINANET-SICHUAN- CHUANXI- IDCSichuanChuanxnIDCCN	false
165.161.203.135	unknown	United States		2381	WISCNET1-ASUS	false
17.152.116.13	unknown	United States		714	APPLE-ENGINEERINGUS	false
154.52.99.81	unknown	United States		174	COGENT-174US	false
178.165.242.98	unknown	Austria		25255	H3G-AUSTRIA- ASTELE2AUSTRIAAT	false
113.228.66.169	unknown	China		4837	CHINA169- BACKBONECHINAUNICO MChina169BackboneCN	false
41.119.232.127	unknown	South Africa		16637	MTNNS-ASZA	false
41.254.158.144	unknown	Libyan Arab Jamahiriya		21003	GPTC-ASLY	false
63.10.95.67	unknown	United States		701	UUNETUS	false
119.18.52.5	unknown	India		394695	PUBLIC-DOMAIN- REGISTRYUS	false
204.187.191.249	unknown	Canada		27396	ASSOCI-BR-AS1US	false
84.46.116.225	unknown	Germany		15943	WTNET- ASwilhelmtelGmbHDE	false
164.205.168.226	unknown	United States		3303	SWISSCOMSwisscomSwitz erlandLtdCH	false
85.192.163.6	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
141.79.250.229	unknown	Germany		553	BELWUEBelWue- KoordinationEU	false
201.63.26.127	unknown	Brazil		10429	TELEFONICABRASILSAB R	false
101.255.113.22	unknown	Indonesia		38511	TACHYON-AS- IDPTRemalaAbadiID	false
185.227.197.197	unknown	United Kingdom		207789	SUPERNET-ASPL	false
191.152.78.188	unknown	Colombia		26611	COMCELSACO	false
178.136.126.22	unknown	Ukraine		6703	ALKAR-ASUA	false
119.39.14.214	unknown	China		4837	CHINA169- BACKBONECHINAUNICO MChina169BackboneCN	false
71.233.106.104	unknown	United States		7922	COMCAST-7922US	false
93.71.108.188	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
23.119.46.253	unknown	United States		7018	ATT-INTERNET4US	false
219.135.58.124	unknown	China		134764	CT-FOSHAN- IDCCHINANETGuangdongp rovincenetworkCN	false
164.19.161.193	unknown	Germany		29355	KCELL-ASKZ	false
57.159.115.221	unknown	Belgium		2686	ATGS-MMD-ASUS	false
216.61.127.70	unknown	United States		7018	ATT-INTERNET4US	false
41.225.247.253	unknown	Tunisia		37671	GLOBALNET-ASTN	false
70.134.116.5	unknown	United States		7018	ATT-INTERNET4US	false
213.65.121.58	unknown	Sweden		3301	TELIANET- SWEDENTeliaCompanySE	false
157.97.102.158	unknown	Netherlands		207161	US-PHXCH	false
57.37.31.230	unknown	Belgium		2686	ATGS-MMD-ASUS	false
110.57.233.194	unknown	China		9394	CTTNETChinaTieTongTele communicationsCorporation CN	false
153.210.55.36	unknown	Japan		4713	OCNNTTCommunicationsC orporationJP	false
99.70.156.74	unknown	United States		7018	ATT-INTERNET4US	false
78.51.203.229	unknown	Germany		6805	TDDE-ASN1DE	false
199.70.171.32	unknown	United States		7018	ATT-INTERNET4US	false
180.132.154.152	unknown	Korea Republic of		9644	SKTELECOM-NET- ASSKTelecomKR	false
148.226.199.223	unknown	Mexico		7184	UniversidadVeracruzanaMX	false
31.47.209.241	unknown	Romania		49800	GNC- ALFAGNCAIfaCJSCRostele comArmeniaAM	false
219.61.62.110	unknown	Japan		17676	GIGAINFRASoftbankBBCor pJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.19.90.2	unknown	United States		206	CSC-IGN-AMERUS	false

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

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

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

/memfd:30-systemd-environment-d-generator (deleted) 

/memfd:user-environment-generators (deleted) 

/proc/6481/oom_score_adj 

/proc/6752/oom_score_adj 

/run/gdm3.pid 

/run/systemd/journal/streams/.#9:74907KcTgBY 

/run/systemd/journal/streams/.#9:74908YhXtMZ 

/run/systemd/journal/streams/.#9:75603XHnZJ2 

/run/systemd/journal/streams/.#9:7560854UGWY 

/run/systemd/journal/streams/.#9:75648HSEZg1 

/run/systemd/journal/streams/.#9:76282Q7faY0 

/run/systemd/journal/streams/.#9:762936Rtbh0 

/run/systemd/journal/streams/.#9:763065qKD00 

/run/systemd/journal/streams/.#9:764607G7y91 

/run/systemd/journal/streams/.#9:764661C4G2Z	▼
/run/systemd/journal/streams/.#9:76483yHLTc2	▼
/run/systemd/journal/streams/.#9:76734aHVBv1	▼
/run/systemd/journal/streams/.#9:76816Eplx0	▼
/run/systemd/journal/streams/.#9:77222APHFD1	▼
/run/systemd/journal/streams/.#9:77279rW8DKY	▼
/run/systemd/journal/streams/.#9:77281dKkVj1	▼
/run/systemd/journal/streams/.#9:77313lTXDsZ	▼
/run/systemd/journal/streams/.#9:77318Ntn5G1	▼
/run/systemd/journal/streams/.#9:78530WYHCsW	▼
/run/systemd/journal/streams/.#9:78659QmgUCT	▼
/run/systemd/journal/streams/.#9:79001nJ1kDW	▼
/run/systemd/journal/streams/.#9:79003S5LcwW	▼
/run/systemd/journal/streams/.#9:79018ws0pnV	▼
/run/systemd/journal/streams/.#9:79019lZe3AV	▼
/run/systemd/journal/streams/.#9:790217VV9sT	▼
/run/systemd/journal/streams/.#9:79022JfbHJV	▼
/run/systemd/journal/streams/.#9:79030m6EINU	▼
/run/systemd/journal/streams/.#9:79564nzFwvb	▼
/run/systemd/journal/streams/.#9:7956573XpT7	▼
/run/systemd/journal/streams/.#9:79857UnSIRa	▼
/run/systemd/journal/streams/.#9:80090sKzz08	▼
/run/systemd/journal/streams/.#9:80198472PP9	▼
/run/systemd/journal/streams/.#9:80199VfwKE7	▼
/run/systemd/journal/streams/.#9:80200qaQNp8	▼
/run/systemd/journal/streams/.#9:80209AuLRP7	▼
/run/systemd/journal/streams/.#9:802193mvth7	▼
/run/systemd/journal/streams/.#9:802203bqbDb	▼
/run/systemd/journal/streams/.#9:8022330j4f7	▼
/run/systemd/journal/streams/.#9:80224CxNR98	▼
/run/systemd/journal/streams/.#9:80267qBNDd8	▼
/run/systemd/journal/streams/.#9:80268tMiLn8	▼

/run/systemd/journal/streams/.#9:80302VjkqN8	▼
/run/systemd/journal/streams/.#9:8030363hRo8	▼
/run/systemd/journal/streams/.#9:80839bdrb2m	▼
/run/systemd/journal/streams/.#9:80840LUNoBq	▼
/run/systemd/journal/streams/.#9:8085500J4Dn	▼
/run/systemd/journal/streams/.#9:80859HMYFwq	▼
/run/systemd/journal/streams/.#9:808605vy5in	▼
/run/systemd/journal/streams/.#9:80862wtapQo	▼
/run/systemd/journal/streams/.#9:80883sZlfko	▼
/run/systemd/journal/streams/.#9:827030qQjuG	▼
/run/systemd/journal/streams/.#9:82718WqsSvl	▼
/run/systemd/journal/streams/.#9:827193oflLI	▼
/run/systemd/journal/streams/.#9:827207EgvPE	▼
/run/systemd/journal/streams/.#9:82727hvCtjG	▼
/run/systemd/journal/streams/.#9:82728h0VebH	▼
/run/systemd/journal/streams/.#9:83247c0XgpF	▼
/run/systemd/journal/streams/.#9:83253FjLj8H	▼
/run/systemd/journal/streams/.#9:83261ZcxUvF	▼
/run/systemd/journal/streams/.#9:83262gCngnG	▼
/run/systemd/journal/streams/.#9:83266nuezcG	▼
/run/systemd/journal/streams/.#9:83267NgGHuF	▼
/run/systemd/journal/streams/.#9:83278jQCkRE	▼
/run/systemd/journal/streams/.#9:83282jOZ5RF	▼
/run/systemd/journal/streams/.#9:83283Xq186I	▼
/run/systemd/journal/streams/.#9:83285dCfHGG	▼
/run/systemd/journal/streams/.#9:83286ahPRol	▼
/run/systemd/seats/.#seat0HzP17k	▼
/run/systemd/seats/.#seat0K16fYL	▼
/run/systemd/seats/.#seat0M9T2qZ	▼
/run/systemd/seats/.#seat0YpYzkE	▼
/run/systemd/seats/.#seat0i6qGpk	▼
/run/systemd/seats/.#seat0xn76yi	▼

/run/systemd/seats/.#seat0zs0y8u	▼
/run/systemd/users/.#1279ZRaxm	▼
/run/systemd/users/.#127LT7oLo	▼
/run/systemd/users/.#127NKcwVk	▼
/run/systemd/users/.#127TdX6Hj	▼
/run/systemd/users/.#127TeLMik	▼
/run/systemd/users/.#127Z4vyKh	▼
/run/systemd/users/.#127pU3buh	▼
/run/systemd/users/.#127qAetKk	▼
/run/user/1000/pulse/pid	▼
/run/utmp	▼
/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/dbus.socket/cgroup.procs	▼
/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/init.scope/cgroup.procs	▼
/sys/fs/cgroup/systemd/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	▼
/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/dbus.socket/cgroup.procs	▼
/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/init.scope/cgroup.procs	▼
/sys/fs/cgroup/unified/user.slice/user-127.slice/user@127.service/pulseaudio.service/cgroup.procs	▼
/tmp/qemu-open.kCThj6 (deleted)	▼
/var/crash/_usr_bin_light-locker.1000.uploaded	▼
/var/lib/AccountsService/users/gdm.GDQ4M1	▼

Static File Info		—
General		—
File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, with debug_info, not stripped	
Entropy (8bit):	6.0065312398450255	
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%	
File name:	6glL6GLh9R	
File size:	150354	
MD5:	6dfcca37a6b1468fcdf3addab827b850	
SHA1:	d96baef8427ad98a42e418e49fbcf440b173fc3a	
SHA256:	eed19f89eba4f0ca0b1f7ef5f02080b5839f076652aeb277c59e3b6e85f18c4a	
SHA512:	ebddf8a3dce7866e86cd188e492ed143dc1e7ab7cf6adfc5d8cc5b3eb47a1779b06f81f08e759e918c8f5868e467558a7b7d6a81cd2ba17a792d38ddb1860229	
SSDEEP:	3072:0rMrjDKMLbid2wnVMD021MzcdTcLdVaTneYxbhAGpWyfa90tM/9V3Jnr:04rjDKybid2wnKbVUdVaTn7phAMfa9a4	
TLSH:	3BE33B86FA409E13C0C61776BAAF014A3322E755E3DB73068D185FF43F8AA5E4E57606	
File Content Preview:	.ELF.....(.....4.....4. ...{.....p.}.....\$~..\$~.....5.....Q.td.....-..L.....@-.. .,@...0....S	

Static ELF Info	—
-----------------	---

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8194
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	122776
Section Header Size:	40
Number of Section Headers:	29
Header String Table Index:	26

Sections										
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80d4	0xd4	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80f0	0xf0	0x168d8	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1e9c8	0x169c8	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e9d8	0x169d8	0x131c	0x0	0x2	A	0	0	4
.ARM.extab	PROGBITS	0x1fcf4	0x17cf4	0x18	0x0	0x2	A	0	0	4
.ARM.exidx	ARM_EXIDX	0x1fd0c	0x17d0c	0x118	0x0	0x82	AL	2	0	4
.eh_frame	PROGBITS	0x20000	0x18000	0x4	0x0	0x3	WA	0	0	4
.tbss	NOBITS	0x20004	0x18004	0x8	0x0	0x403	WAT	0	0	4
.init_array	INIT_ARRAY	0x20004	0x18004	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x20008	0x18008	0x4	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x2000c	0x1800c	0x4	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x20010	0x18010	0xa8	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x200b8	0x180b8	0x204	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x202bc	0x182bc	0x32ec	0x0	0x3	WA	0	0	4
.comment	PROGBITS	0x0	0x182bc	0x8f2	0x0	0x0		0	0	1
.debug_aranges	PROGBITS	0x0	0x18bb0	0xc0	0x0	0x0		0	0	8
.debug_pubnames	PROGBITS	0x0	0x18c70	0x213	0x0	0x0		0	0	1
.debug_info	PROGBITS	0x0	0x18e83	0x1d23	0x0	0x0		0	0	1
.debug_abbrev	PROGBITS	0x0	0x1aba6	0x692	0x0	0x0		0	0	1
.debug_line	PROGBITS	0x0	0x1b238	0x9c7	0x0	0x0		0	0	1
.debug_frame	PROGBITS	0x0	0x1bc00	0x2b8	0x0	0x0		0	0	4
.debug_str	PROGBITS	0x0	0x1beb8	0x8ca	0x1	0x30	MS	0	0	1
.debug_loc	PROGBITS	0x0	0x1c782	0x118f	0x0	0x0		0	0	1
.debug_ranges	PROGBITS	0x0	0x1d911	0x558	0x0	0x0		0	0	1
.ARM.attributes	ARM_ATTRIBUTES	0x0	0x1de69	0x16	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x1de7f	0x117	0x0	0x0		0	0	1
.symtab	SYMTAB	0x0	0x1e420	0x4540	0x10	0x0		28	642	4
.strtab	STRTAB	0x0	0x22960	0x21f2	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
EXIDX	0x17d0c	0x1fd0c	0x1fd0c	0x118	0x118	1.5788	0x4	R	0x4		.ARM.exidx

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x17e24	0x17e24	3.3231	0x5	R E	0x8000		.init .text .fini .rodata .ARM.extab .ARM.exidx
LOAD	0x18000	0x20000	0x20000	0x2bc	0x35a8	2.3220	0x6	RW	0x8000		.eh_frame .init_array .fini_array .jcr .got .data .bss
TLS	0x18004	0x20004	0x20004	0x0	0x8	0.0000	0x4	R	0x4		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Symbols

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
			.symtab	0x80d4	0	SECTION	<unknown>	DEFAULT	1
			.symtab	0x80f0	0	SECTION	<unknown>	DEFAULT	2
			.symtab	0x1e9c8	0	SECTION	<unknown>	DEFAULT	3
			.symtab	0x1e9d8	0	SECTION	<unknown>	DEFAULT	4
			.symtab	0x1fcf4	0	SECTION	<unknown>	DEFAULT	5
			.symtab	0x1fd0c	0	SECTION	<unknown>	DEFAULT	6
			.symtab	0x20000	0	SECTION	<unknown>	DEFAULT	7
			.symtab	0x20004	0	SECTION	<unknown>	DEFAULT	8
			.symtab	0x20004	0	SECTION	<unknown>	DEFAULT	9
			.symtab	0x20008	0	SECTION	<unknown>	DEFAULT	10
			.symtab	0x2000c	0	SECTION	<unknown>	DEFAULT	11
			.symtab	0x20010	0	SECTION	<unknown>	DEFAULT	12
			.symtab	0x200b8	0	SECTION	<unknown>	DEFAULT	13
			.symtab	0x202bc	0	SECTION	<unknown>	DEFAULT	14
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	15
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	16
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	17
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	18
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	19
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	20
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	21
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	22
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	23
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	24
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	25
\$a			.symtab	0x80d4	0	NOTYPE	<unknown>	DEFAULT	1
\$a			.symtab	0x1e9c8	0	NOTYPE	<unknown>	DEFAULT	3
\$a			.symtab	0x80e0	0	NOTYPE	<unknown>	DEFAULT	1
\$a			.symtab	0x1e9d4	0	NOTYPE	<unknown>	DEFAULT	3
\$a			.symtab	0x80f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x8134	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x8194	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x81d0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x8514	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x9148	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa1f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa24c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa348	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa564	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa5d0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa640	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xa9d4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xb068	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xb684	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xbd7c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xc428	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xc6c8	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$a			.symtab	0xcbb4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xcfec	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xd658	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xd6ac	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xdd60	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xe008	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xe058	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xe0fc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xe124	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xe6a0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xf684	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xfc30	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xfc48	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xfd4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0xfe3c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1009c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10848	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x108a4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1090c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10a48	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10b24	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10b4c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10c14	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10d74	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x10f00	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x135b0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x13fe4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x14200	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x14224	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x142c4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x14364	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15524	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15544	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1556c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x155b4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x155d8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x155fc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15668	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x157a4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15800	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15894	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15924	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x159a4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15a38	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15b34	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15c48	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15d8c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15da0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15e38	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15f2c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x15f40	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16020	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16058	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1609c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x160dc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16120	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x161a4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x161e4	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$a			.symtab	0x16270	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x162a0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x163b0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16480	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16544	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x165f4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x166dc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x166fc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16730	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16740	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16750	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x167f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16818	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1685c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x168d0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16914	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16958	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x169cc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16a10	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16a58	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16a98	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16adc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16b4c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16b94	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16c1c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16c60	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16cd0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16d1c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16da4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16dec	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16e30	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16e80	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16e94	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16f58	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x16fc4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x17974	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x17ab4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x17e74	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18314	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18354	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1847c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18494	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18538	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x185f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x186b0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18754	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x187e4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x188bc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x189b4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18aa0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18b64	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x18cb0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x192d4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x196a0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19738	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19780	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19870	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x199a4	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$a			.symtab	0x199fc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19a04	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19a34	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19a8c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19a94	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19ac4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19b1c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19b24	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19b54	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19bac	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19bb4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19be0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19c68	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19d44	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19e04	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19e58	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x19eb0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a29c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a318	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a344	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a3cc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a3d4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a3e0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a3f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a400	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a440	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a4a8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a50c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a5ac	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a5d8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a5ec	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a600	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a614	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a63c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a674	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a6b4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a6c8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a70c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a74c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a78c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a7ec	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a858	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a86c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1a9e4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1aad0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1ae74	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b1a4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b1c4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b624	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b6a4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b808	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b838	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1b97c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1ba98	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1bd48	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c0f4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c220	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c2c0	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$a			.symtab	0x1c750	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c770	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c7d0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c8c0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c9ac	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1c9f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1ca40	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1ca8c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cab0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cb2c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cc24	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cc9c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cd04	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cf58	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cf64	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cf9c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1cff4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d04c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d058	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d1a0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d1f8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d2d4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d304	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d3a8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d3cc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d40c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d47c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d4c8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d514	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d51c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d520	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d54c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d558	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d564	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d784	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d8d4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d8f0	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d950	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1d9bc	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1da74	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1da94	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1dbd8	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e120	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e128	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e130	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e138	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e1f4	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e238	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e94c	0	NOTYPE	<unknown>	DEFAULT	2
\$a			.symtab	0x1e994	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x8128	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x20008	0	NOTYPE	<unknown>	DEFAULT	10
\$d			.symtab	0x8180	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x20004	0	NOTYPE	<unknown>	DEFAULT	9
\$d			.symtab	0x81c4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x84ec	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x9120	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xa340	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$d			.symtab	0xa9a0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xb064	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xb680	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xbd78	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xc424	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xcbb0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xcfe8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xd648	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xd6a4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xdd5c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xe120	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xe69c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xf674	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xfc40	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xfde4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0xfe34	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10098	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1080c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x200b8	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x200bc	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x200c0	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x200c4	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x10894	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x108fc	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10a30	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10b14	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10b48	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10c10	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10d68	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x10dbc	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1358c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x13fac	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1ed10	0	NOTYPE	<unknown>	DEFAULT	4
\$d			.symtab	0x1ed19	0	NOTYPE	<unknown>	DEFAULT	4
\$d			.symtab	0x14220	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x142bc	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1435c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x15374	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x200c8	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x20	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x26	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x2c	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x4c	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x53	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x15e30	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x15f1c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16010	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16054	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16098	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x160d8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1611c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1619c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x161e0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1626c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16394	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16478	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16538	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$d			.symtab	0x165ec	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1f91c	0	NOTYPE	<unknown>	DEFAULT	4
\$d			.symtab	0x166c8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x166f8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1672c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16854	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x168c8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1690c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16950	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x169c4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16a08	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16a50	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16a94	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16ad4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16b44	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16b90	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16c14	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16c58	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16cc8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16d14	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16d9c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16de4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16e28	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16e7c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x16f4c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x17950	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x200cc	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x17a98	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x17e54	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x182f8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1834c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x18468	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x200e4	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x1851c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x185d4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x18694	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x18738	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x200fc	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x20194	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x187e0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x188b0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x189a4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x18a94	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1f934	0	NOTYPE	<unknown>	DEFAULT	4
\$d			.symtab	0x18b44	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x201a8	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x18c8c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x192a8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19678	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19864	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19990	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x199a0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19a30	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19ac0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19b50	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19d3c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19df0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x19e50	0	NOTYPE	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
\$d			.symtab	0x19ea4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a250	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x201c0	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x1a310	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a340	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a3c0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a43c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a4a0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a508	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a5a8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a634	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a670	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a6b0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a708	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a748	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a788	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a7e4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1a850	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1aabc	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1ae6c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1b194	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1b5f0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1b694	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1b7ec	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x201d8	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x201d4	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x1bd2c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1c0dc	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1c218	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1c8b8	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1c9a4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1cb28	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1cc1c	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1cc84	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1ccf4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1cf30	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1cf90	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1d040	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1d198	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1d2d0	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1d3a4	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1d478	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1d768	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x1e110	0	NOTYPE	<unknown>	DEFAULT	2
\$d			.symtab	0x58	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	23
\$d			.symtab	0x23c	0	NOTYPE	<unknown>	DEFAULT	21
\$d			.symtab	0xe39	0	NOTYPE	<unknown>	DEFAULT	23
\$d			.symtab	0x201cc	0	NOTYPE	<unknown>	DEFAULT	13
\$d			.symtab	0x1f9c2	0	NOTYPE	<unknown>	DEFAULT	4
C.11.5548			.symtab	0x1f9a0	12	OBJECT	<unknown>	DEFAULT	4
C.43.5768			.symtab	0x1ed19	3	OBJECT	<unknown>	DEFAULT	4
C.44.5769			.symtab	0x1ed10	9	OBJECT	<unknown>	DEFAULT	4
C.5.5083			.symtab	0x1f91c	24	OBJECT	<unknown>	DEFAULT	4
C.7.5370			.symtab	0x1f9ac	12	OBJECT	<unknown>	DEFAULT	4
C.7.6109			.symtab	0x1fce8	12	OBJECT	<unknown>	DEFAULT	4
C.7.6182			.symtab	0x1fcc4	12	OBJECT	<unknown>	DEFAULT	4
C.8.6110			.symtab	0x1fcdc	12	OBJECT	<unknown>	DEFAULT	4

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
C.9.6119			.symtab	0x1fcd0	12	OBJECT	<unknown>	DEFAULT	4
LOCAL_ADDR			.symtab	0x22dfc	4	OBJECT	<unknown>	DEFAULT	14
Laligned			.symtab	0x1c798	0	NOTYPE	<unknown>	DEFAULT	2
Llastword			.symtab	0x1c7b4	0	NOTYPE	<unknown>	DEFAULT	2
_Exit			.symtab	0x1a440	104	FUNC	<unknown>	DEFAULT	2
_GLOBAL_OFFSET_TABLE_			.symtab	0x20010	0	OBJECT	<unknown>	HIDDEN	12
_Jv_RegisterClasses			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_READ.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_Unwind_Complete			.symtab	0x1d51c	4	FUNC	<unknown>	HIDDEN	2
_Unwind_DeleteException			.symtab	0x1d520	44	FUNC	<unknown>	HIDDEN	2
_Unwind_ForcedUnwind			.symtab	0x1e1d0	36	FUNC	<unknown>	HIDDEN	2
_Unwind_GetCFA			.symtab	0x1d514	8	FUNC	<unknown>	HIDDEN	2
_Unwind_GetDataRelBase			.symtab	0x1d558	12	FUNC	<unknown>	HIDDEN	2
_Unwind_GetLanguageSpecificData			.symtab	0x1e1f4	68	FUNC	<unknown>	HIDDEN	2
_Unwind_GetRegionStart			.symtab	0x1e994	52	FUNC	<unknown>	HIDDEN	2
_Unwind_GetTextRelBase			.symtab	0x1d54c	12	FUNC	<unknown>	HIDDEN	2
_Unwind_RaiseException			.symtab	0x1e164	36	FUNC	<unknown>	HIDDEN	2
_Unwind_Resume			.symtab	0x1e188	36	FUNC	<unknown>	HIDDEN	2
_Unwind_Resume_or_Rethrow			.symtab	0x1e1ac	36	FUNC	<unknown>	HIDDEN	2
_Unwind_VRS_Get			.symtab	0x1d47c	76	FUNC	<unknown>	HIDDEN	2
_Unwind_VRS_Pop			.symtab	0x1da94	324	FUNC	<unknown>	HIDDEN	2
_Unwind_VRS_Set			.symtab	0x1d4c8	76	FUNC	<unknown>	HIDDEN	2
_WRITE.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__C_ctype_b			.symtab	0x201cc	4	OBJECT	<unknown>	DEFAULT	13
__C_ctype_b.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__C_ctype_b_data			.symtab	0x1f9c2	768	OBJECT	<unknown>	DEFAULT	4
__EH_FRAME_BEGIN__			.symtab	0x20000	0	OBJECT	<unknown>	DEFAULT	7
__FRAME_END__			.symtab	0x20000	0	OBJECT	<unknown>	DEFAULT	7
__Gl__C_ctype_b			.symtab	0x201cc	4	OBJECT	<unknown>	HIDDEN	13
__Gl__close			.symtab	0x199c0	100	FUNC	<unknown>	HIDDEN	2
__Gl__close_nocancel			.symtab	0x199a4	24	FUNC	<unknown>	HIDDEN	2
__Gl__ctype_b			.symtab	0x201d0	4	OBJECT	<unknown>	HIDDEN	13
__Gl__errno_location			.symtab	0x166dc	32	FUNC	<unknown>	HIDDEN	2
__Gl__fcntl_nocancel			.symtab	0x15da0	152	FUNC	<unknown>	HIDDEN	2
__Gl__fgetc_unlocked			.symtab	0x1c0f4	300	FUNC	<unknown>	HIDDEN	2
__Gl__libc_close			.symtab	0x199c0	100	FUNC	<unknown>	HIDDEN	2
__Gl__libc_fcntl			.symtab	0x15e38	244	FUNC	<unknown>	HIDDEN	2
__Gl__libc_open			.symtab	0x19a50	100	FUNC	<unknown>	HIDDEN	2
__Gl__libc_read			.symtab	0x19b70	100	FUNC	<unknown>	HIDDEN	2
__Gl__libc_write			.symtab	0x19ae0	100	FUNC	<unknown>	HIDDEN	2
__Gl__open			.symtab	0x19a50	100	FUNC	<unknown>	HIDDEN	2
__Gl__open_nocancel			.symtab	0x19a34	24	FUNC	<unknown>	HIDDEN	2
__Gl__read			.symtab	0x19b70	100	FUNC	<unknown>	HIDDEN	2
__Gl__read_nocancel			.symtab	0x19b54	24	FUNC	<unknown>	HIDDEN	2
__Gl__sigaddset			.symtab	0x16f7c	36	FUNC	<unknown>	HIDDEN	2
__Gl__sigdelset			.symtab	0x16fa0	36	FUNC	<unknown>	HIDDEN	2
__Gl__sigismember			.symtab	0x16f58	36	FUNC	<unknown>	HIDDEN	2
__Gl__uClibc_fini			.symtab	0x19d88	124	FUNC	<unknown>	HIDDEN	2
__Gl__uClibc_init			.symtab	0x19e58	88	FUNC	<unknown>	HIDDEN	2
__Gl__write			.symtab	0x19ae0	100	FUNC	<unknown>	HIDDEN	2
__Gl__write_nocancel			.symtab	0x19ac4	24	FUNC	<unknown>	HIDDEN	2
__Gl__exit			.symtab	0x1a440	104	FUNC	<unknown>	HIDDEN	2
__Gl__abort			.symtab	0x18354	296	FUNC	<unknown>	HIDDEN	2
__Gl__accept			.symtab	0x1685c	116	FUNC	<unknown>	HIDDEN	2
__Gl__bind			.symtab	0x168d0	68	FUNC	<unknown>	HIDDEN	2
__Gl__brk			.symtab	0x1cff4	88	FUNC	<unknown>	HIDDEN	2
__Gl__close			.symtab	0x199c0	100	FUNC	<unknown>	HIDDEN	2
__Gl__closedir			.symtab	0x162a0	272	FUNC	<unknown>	HIDDEN	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__Gl_config_close			.symtab	0x1adf8	52	FUNC	<unknown>	HIDDEN	2
__Gl_config_open			.symtab	0x1ae2c	72	FUNC	<unknown>	HIDDEN	2
__Gl_config_read			.symtab	0x1aad0	808	FUNC	<unknown>	HIDDEN	2
__Gl_connect			.symtab	0x16958	116	FUNC	<unknown>	HIDDEN	2
__Gl_exit			.symtab	0x18aa0	196	FUNC	<unknown>	HIDDEN	2
__Gl_fclose			.symtab	0x1ae74	816	FUNC	<unknown>	HIDDEN	2
__Gl_fcntl			.symtab	0x15e38	244	FUNC	<unknown>	HIDDEN	2
__Gl_fflush_unlocked			.symtab	0x1bd48	940	FUNC	<unknown>	HIDDEN	2
__Gl_fgetc			.symtab	0x1b838	324	FUNC	<unknown>	HIDDEN	2
__Gl_fgetc_unlocked			.symtab	0x1c0f4	300	FUNC	<unknown>	HIDDEN	2
__Gl_fgets			.symtab	0x1b97c	284	FUNC	<unknown>	HIDDEN	2
__Gl_fgets_unlocked			.symtab	0x1c220	160	FUNC	<unknown>	HIDDEN	2
__Gl_fopen			.symtab	0x1b1a4	32	FUNC	<unknown>	HIDDEN	2
__Gl_fork			.symtab	0x192d4	972	FUNC	<unknown>	HIDDEN	2
__Gl_fstat			.symtab	0x1a4a8	100	FUNC	<unknown>	HIDDEN	2
__Gl_getc_unlocked			.symtab	0x1c0f4	300	FUNC	<unknown>	HIDDEN	2
__Gl_getdtablesize			.symtab	0x1a5ac	44	FUNC	<unknown>	HIDDEN	2
__Gl_getegid			.symtab	0x1a5d8	20	FUNC	<unknown>	HIDDEN	2
__Gl_geteuid			.symtab	0x1a5ec	20	FUNC	<unknown>	HIDDEN	2
__Gl_getgid			.symtab	0x1a600	20	FUNC	<unknown>	HIDDEN	2
__Gl_getpagesize			.symtab	0x1a614	40	FUNC	<unknown>	HIDDEN	2
__Gl_getpid			.symtab	0x19738	72	FUNC	<unknown>	HIDDEN	2
__Gl_getrlimit			.symtab	0x1a63c	56	FUNC	<unknown>	HIDDEN	2
__Gl_getsockname			.symtab	0x169cc	68	FUNC	<unknown>	HIDDEN	2
__Gl_gettimeofday			.symtab	0x1a674	64	FUNC	<unknown>	HIDDEN	2
__Gl_getuid			.symtab	0x1a6b4	20	FUNC	<unknown>	HIDDEN	2
__Gl_inet_addr			.symtab	0x167f0	40	FUNC	<unknown>	HIDDEN	2
__Gl_inet_aton			.symtab	0x1cb2c	248	FUNC	<unknown>	HIDDEN	2
__Gl_initstate_r			.symtab	0x188bc	248	FUNC	<unknown>	HIDDEN	2
__Gl_ioctl			.symtab	0x15f40	224	FUNC	<unknown>	HIDDEN	2
__Gl_isatty			.symtab	0x1ca8c	36	FUNC	<unknown>	HIDDEN	2
__Gl_kill			.symtab	0x16020	56	FUNC	<unknown>	HIDDEN	2
__Gl_listen			.symtab	0x16a58	64	FUNC	<unknown>	HIDDEN	2
__Gl_lseek64			.symtab	0x1d40c	112	FUNC	<unknown>	HIDDEN	2
__Gl_memcpy			.symtab	0x16730	4	FUNC	<unknown>	HIDDEN	2
__Gl_memmove			.symtab	0x16740	4	FUNC	<unknown>	HIDDEN	2
__Gl_mempcpy			.symtab	0x1d3a8	36	FUNC	<unknown>	HIDDEN	2
__Gl_memset			.symtab	0x16750	156	FUNC	<unknown>	HIDDEN	2
__Gl_mmap			.symtab	0x1a29c	124	FUNC	<unknown>	HIDDEN	2
__Gl_mremap			.symtab	0x1a6c8	68	FUNC	<unknown>	HIDDEN	2
__Gl_munmap			.symtab	0x1a70c	64	FUNC	<unknown>	HIDDEN	2
__Gl_nanosleep			.symtab	0x1a78c	96	FUNC	<unknown>	HIDDEN	2
__Gl_open			.symtab	0x19a50	100	FUNC	<unknown>	HIDDEN	2
__Gl_opendir			.symtab	0x16480	196	FUNC	<unknown>	HIDDEN	2
__Gl_raise			.symtab	0x19780	240	FUNC	<unknown>	HIDDEN	2
__Gl_random			.symtab	0x18494	164	FUNC	<unknown>	HIDDEN	2
__Gl_random_r			.symtab	0x18754	144	FUNC	<unknown>	HIDDEN	2
__Gl_read			.symtab	0x19b70	100	FUNC	<unknown>	HIDDEN	2
__Gl_readdir			.symtab	0x165f4	232	FUNC	<unknown>	HIDDEN	2
__Gl_readdir64			.symtab	0x1a9e4	236	FUNC	<unknown>	HIDDEN	2
__Gl_readlink			.symtab	0x1609c	64	FUNC	<unknown>	HIDDEN	2
__Gl_recv			.symtab	0x16adc	112	FUNC	<unknown>	HIDDEN	2
__Gl_recvfrom			.symtab	0x16b94	136	FUNC	<unknown>	HIDDEN	2
__Gl_sbrk			.symtab	0x1a7ec	108	FUNC	<unknown>	HIDDEN	2
__Gl_select			.symtab	0x16120	132	FUNC	<unknown>	HIDDEN	2
__Gl_send			.symtab	0x16c60	112	FUNC	<unknown>	HIDDEN	2
__Gl_sendto			.symtab	0x16d1c	136	FUNC	<unknown>	HIDDEN	2
__Gl_setsid			.symtab	0x161a4	64	FUNC	<unknown>	HIDDEN	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__Gl_setsockopt			.symtab	0x16da4	72	FUNC	<unknown>	HIDDEN	2
__Gl_setstate_r			.symtab	0x189b4	236	FUNC	<unknown>	HIDDEN	2
__Gl_sigaction			.symtab	0x1a344	136	FUNC	<unknown>	HIDDEN	2
__Gl_sigaddset			.symtab	0x16e30	80	FUNC	<unknown>	HIDDEN	2
__Gl_sigemptyset			.symtab	0x16e80	20	FUNC	<unknown>	HIDDEN	2
__Gl_signal			.symtab	0x16e94	196	FUNC	<unknown>	HIDDEN	2
__Gl_sigprocmask			.symtab	0x161e4	140	FUNC	<unknown>	HIDDEN	2
__Gl_sleep			.symtab	0x19870	300	FUNC	<unknown>	HIDDEN	2
__Gl_socket			.symtab	0x16dec	68	FUNC	<unknown>	HIDDEN	2
__Gl_srandom_r			.symtab	0x187e4	216	FUNC	<unknown>	HIDDEN	2
__Gl_strchr			.symtab	0x1c7d0	240	FUNC	<unknown>	HIDDEN	2
__Gl_strchrnul			.symtab	0x1c8c0	236	FUNC	<unknown>	HIDDEN	2
__Gl_strcmp			.symtab	0x1c750	28	FUNC	<unknown>	HIDDEN	2
__Gl_strcoll			.symtab	0x1c750	28	FUNC	<unknown>	HIDDEN	2
__Gl_strerrorn			.symtab	0x1c9ac	68	FUNC	<unknown>	HIDDEN	2
__Gl_strlen			.symtab	0x1c770	96	FUNC	<unknown>	HIDDEN	2
__Gl_strchr			.symtab	0x1c9f0	80	FUNC	<unknown>	HIDDEN	2
__Gl_strerrorn			.symtab	0x1ca40	76	FUNC	<unknown>	HIDDEN	2
__Gl_sysconf			.symtab	0x18cb0	1572	FUNC	<unknown>	HIDDEN	2
__Gl_tcgetattr			.symtab	0x1cab0	124	FUNC	<unknown>	HIDDEN	2
__Gl_time			.symtab	0x16270	48	FUNC	<unknown>	HIDDEN	2
__Gl_times			.symtab	0x1a858	20	FUNC	<unknown>	HIDDEN	2
__Gl_write			.symtab	0x19ae0	100	FUNC	<unknown>	HIDDEN	2
_JCR_END__			.symtab	0x2000c	0	OBJECT	<unknown>	DEFAULT	11
_JCR_LIST__			.symtab	0x2000c	0	OBJECT	<unknown>	DEFAULT	11
___Unwind_ForceUnwind			.symtab	0x1e1d0	36	FUNC	<unknown>	HIDDEN	2
___Unwind_RaiseException			.symtab	0x1e164	36	FUNC	<unknown>	HIDDEN	2
___Unwind_Resume			.symtab	0x1e188	36	FUNC	<unknown>	HIDDEN	2
___Unwind_Resume_or_Rethrow			.symtab	0x1e1ac	36	FUNC	<unknown>	HIDDEN	2
_aeabi_idiv			.symtab	0x15c48	0	FUNC	<unknown>	HIDDEN	2
_aeabi_idivmod			.symtab	0x15d74	24	FUNC	<unknown>	HIDDEN	2
_aeabi_read_tp			.symtab	0x1a3f0	8	FUNC	<unknown>	DEFAULT	2
_aeabi_uidiv			.symtab	0x15b34	0	FUNC	<unknown>	HIDDEN	2
_aeabi_uidivmod			.symtab	0x15c30	24	FUNC	<unknown>	HIDDEN	2
_aeabi_unwind_cpp_pr0			.symtab	0x1e130	8	FUNC	<unknown>	HIDDEN	2
_aeabi_unwind_cpp_pr1			.symtab	0x1e128	8	FUNC	<unknown>	HIDDEN	2
_aeabi_unwind_cpp_pr2			.symtab	0x1e120	8	FUNC	<unknown>	HIDDEN	2
_app_fini			.symtab	0x20894	4	OBJECT	<unknown>	HIDDEN	14
_atexit_lock			.symtab	0x201a8	24	OBJECT	<unknown>	DEFAULT	13
_bss_end__			.symtab	0x235a8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_bss_start			.symtab	0x202bc	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_bss_start__			.symtab	0x202bc	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_check_one_fd			.symtab	0x19e04	84	FUNC	<unknown>	DEFAULT	2
_close			.symtab	0x199c0	100	FUNC	<unknown>	DEFAULT	2
_close_nocancel			.symtab	0x199a4	24	FUNC	<unknown>	DEFAULT	2
_ctype_b			.symtab	0x201d0	4	OBJECT	<unknown>	DEFAULT	13
_curbrk			.symtab	0x22df8	4	OBJECT	<unknown>	HIDDEN	14
_cxa_begin_cleanup			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_cxa_call_unexpected			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_cxa_type_match			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_data_start			.symtab	0x200b8	0	NOTYPE	<unknown>	DEFAULT	13
_default_rt_sa_restorer			.symtab	0x1a3e4	0	FUNC	<unknown>	DEFAULT	2
_default_sa_restorer			.symtab	0x1a3d8	0	FUNC	<unknown>	DEFAULT	2
_deregister_frame_info			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_div0			.symtab	0x15d8c	20	FUNC	<unknown>	HIDDEN	2
_divsi3			.symtab	0x15c48	300	FUNC	<unknown>	HIDDEN	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__do_global_dtors_aux			.symtab	0x80f0	0	FUNC	<unknown>	DEFAULT	2
__do_global_dtors_aux_fini_array_entry			.symtab	0x20008	0	OBJECT	<unknown>	DEFAULT	10
__end__			.symtab	0x235a8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__environ			.symtab	0x2088c	4	OBJECT	<unknown>	DEFAULT	14
__errno_location			.symtab	0x166dc	32	FUNC	<unknown>	DEFAULT	2
__errno_location.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__exidx_end			.symtab	0x1fe24	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__exidx_start			.symtab	0x1fd0c	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__exit_cleanup			.symtab	0x2033c	4	OBJECT	<unknown>	HIDDEN	14
__fcntl_nocancel			.symtab	0x15da0	152	FUNC	<unknown>	DEFAULT	2
__fgetc_unlocked			.symtab	0x1c0f4	300	FUNC	<unknown>	DEFAULT	2
__fini_array_end			.symtab	0x2000c	0	NOTYPE	<unknown>	HIDDEN	10
__fini_array_start			.symtab	0x20008	0	NOTYPE	<unknown>	HIDDEN	10
__fork			.symtab	0x192d4	972	FUNC	<unknown>	DEFAULT	2
__fork_generation_pointer			.symtab	0x23574	4	OBJECT	<unknown>	HIDDEN	14
__fork_handlers			.symtab	0x23578	4	OBJECT	<unknown>	HIDDEN	14
__fork_lock			.symtab	0x20340	4	OBJECT	<unknown>	HIDDEN	14
__frame_dummy_init_array_entry			.symtab	0x20004	0	OBJECT	<unknown>	DEFAULT	9
__getdents			.symtab	0x1a50c	160	FUNC	<unknown>	HIDDEN	2
__getdents64			.symtab	0x1d058	328	FUNC	<unknown>	HIDDEN	2
__getpagesize			.symtab	0x1a614	40	FUNC	<unknown>	DEFAULT	2
__getpid			.symtab	0x19738	72	FUNC	<unknown>	DEFAULT	2
__gnu_Unwind_Find_exidx			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__gnu_Unwind_ForcedUnwind			.symtab	0x1d8d4	28	FUNC	<unknown>	HIDDEN	2
__gnu_Unwind_RaiseException			.symtab	0x1d9bc	184	FUNC	<unknown>	HIDDEN	2
__gnu_Unwind_Restore_VFP			.symtab	0x1e154	0	FUNC	<unknown>	HIDDEN	2
__gnu_Unwind_Resume			.symtab	0x1d950	108	FUNC	<unknown>	HIDDEN	2
__gnu_Unwind_Resume_or_Rethrow			.symtab	0x1da74	32	FUNC	<unknown>	HIDDEN	2
__gnu_Unwind_Save_VFP			.symtab	0x1e15c	0	FUNC	<unknown>	HIDDEN	2
__gnu_unwind_execute			.symtab	0x1e238	1812	FUNC	<unknown>	HIDDEN	2
__gnu_unwind_frame			.symtab	0x1e94c	72	FUNC	<unknown>	HIDDEN	2
__gnu_unwind_pr_common			.symtab	0x1dbd8	1352	FUNC	<unknown>	DEFAULT	2
__h_errno_location			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__init_array_end			.symtab	0x20008	0	NOTYPE	<unknown>	HIDDEN	9
__init_array_start			.symtab	0x20004	0	NOTYPE	<unknown>	HIDDEN	9
__libc_accept			.symtab	0x1685c	116	FUNC	<unknown>	DEFAULT	2
__libc_close			.symtab	0x199c0	100	FUNC	<unknown>	DEFAULT	2
__libc_connect			.symtab	0x16958	116	FUNC	<unknown>	DEFAULT	2
__libc_disable_asynccancel			.symtab	0x19be0	136	FUNC	<unknown>	HIDDEN	2
__libc_enable_asynccancel			.symtab	0x19c68	220	FUNC	<unknown>	HIDDEN	2
__libc_errno			.symtab	0x0	4	TLS	<unknown>	HIDDEN	8
__libc_fcntl			.symtab	0x15e38	244	FUNC	<unknown>	DEFAULT	2
__libc_fork			.symtab	0x192d4	972	FUNC	<unknown>	DEFAULT	2
__libc_h_errno			.symtab	0x4	4	TLS	<unknown>	HIDDEN	8
__libc_multiple_threads			.symtab	0x2357c	4	OBJECT	<unknown>	HIDDEN	14
__libc_nanosleep			.symtab	0x1a78c	96	FUNC	<unknown>	DEFAULT	2
__libc_open			.symtab	0x19a50	100	FUNC	<unknown>	DEFAULT	2
__libc_read			.symtab	0x19b70	100	FUNC	<unknown>	DEFAULT	2
__libc_recv			.symtab	0x16adc	112	FUNC	<unknown>	DEFAULT	2
__libc_recvfrom			.symtab	0x16b94	136	FUNC	<unknown>	DEFAULT	2
__libc_select			.symtab	0x16120	132	FUNC	<unknown>	DEFAULT	2
__libc_send			.symtab	0x16c60	112	FUNC	<unknown>	DEFAULT	2
__libc_sendto			.symtab	0x16d1c	136	FUNC	<unknown>	DEFAULT	2
__libc_setup_tls			.symtab	0x1cd28	560	FUNC	<unknown>	DEFAULT	2
__libc_sigaction			.symtab	0x1a344	136	FUNC	<unknown>	DEFAULT	2
__libc_stack_end			.symtab	0x20888	4	OBJECT	<unknown>	DEFAULT	14

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__libc_write			.symtab	0x19ae0	100	FUNC	<unknown>	DEFAULT	2
__lll_lock_wait_private			.symtab	0x196a0	152	FUNC	<unknown>	HIDDEN	2
__malloc_consolidate			.symtab	0x17f24	436	FUNC	<unknown>	HIDDEN	2
__malloc_largebin_index			.symtab	0x16fc4	120	FUNC	<unknown>	DEFAULT	2
__malloc_lock			.symtab	0x200cc	24	OBJECT	<unknown>	DEFAULT	13
__malloc_state			.symtab	0x231fc	888	OBJECT	<unknown>	DEFAULT	14
__malloc_trim			.symtab	0x17e74	176	FUNC	<unknown>	DEFAULT	2
__nptl_deallocate_tsd			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDE F
__nptl_nthreads			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDE F
__open			.symtab	0x19a50	100	FUNC	<unknown>	DEFAULT	2
__open_nocancel			.symtab	0x19a34	24	FUNC	<unknown>	DEFAULT	2
__pagesize			.symtab	0x20890	4	OBJECT	<unknown>	DEFAULT	14
__preinit_array_end			.symtab	0x20004	0	NOTYPE	<unknown>	HIDDEN	8
__preinit_array_start			.symtab	0x20004	0	NOTYPE	<unknown>	HIDDEN	8
__progname			.symtab	0x201c4	4	OBJECT	<unknown>	DEFAULT	13
__progname_full			.symtab	0x201c8	4	OBJECT	<unknown>	DEFAULT	13
__pthread_initialize_minimal			.symtab	0x1cf58	12	FUNC	<unknown>	DEFAULT	2
__pthread_mutex_init			.symtab	0x19d4c	8	FUNC	<unknown>	DEFAULT	2
__pthread_mutex_lock			.symtab	0x19d44	8	FUNC	<unknown>	DEFAULT	2
__pthread_mutex_trylock			.symtab	0x19d44	8	FUNC	<unknown>	DEFAULT	2
__pthread_mutex_unlock			.symtab	0x19d44	8	FUNC	<unknown>	DEFAULT	2
__pthread_return_0			.symtab	0x19d44	8	FUNC	<unknown>	DEFAULT	2
__pthread_unwind			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDE F
__read			.symtab	0x19b70	100	FUNC	<unknown>	DEFAULT	2
__read_nocancel			.symtab	0x19b54	24	FUNC	<unknown>	DEFAULT	2
__register_frame_info			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDE F
__restore_core_regs			.symtab	0x1e138	28	FUNC	<unknown>	HIDDEN	2
__rtld_fini			.symtab	0x20898	4	OBJECT	<unknown>	HIDDEN	14
__sigaddset			.symtab	0x16f7c	36	FUNC	<unknown>	DEFAULT	2
__sigdelset			.symtab	0x16fa0	36	FUNC	<unknown>	DEFAULT	2
__sigismember			.symtab	0x16f58	36	FUNC	<unknown>	DEFAULT	2
__sigjmp_save			.symtab	0x1d3cc	64	FUNC	<unknown>	HIDDEN	2
__sigsetjmp			.symtab	0x1d04c	12	FUNC	<unknown>	DEFAULT	2
__stdin			.symtab	0x201e4	4	OBJECT	<unknown>	DEFAULT	13
__stdio_READ			.symtab	0x1d1a0	88	FUNC	<unknown>	HIDDEN	2
__stdio_WRITE			.symtab	0x1d1f8	220	FUNC	<unknown>	HIDDEN	2
__stdio_rfill			.symtab	0x1d2d4	48	FUNC	<unknown>	HIDDEN	2
__stdio_trans2r_o			.symtab	0x1d304	164	FUNC	<unknown>	HIDDEN	2
__stdio_wcommit			.symtab	0x1b808	48	FUNC	<unknown>	HIDDEN	2
__stdout			.symtab	0x201e8	4	OBJECT	<unknown>	DEFAULT	13
__sys_accept			.symtab	0x16818	68	FUNC	<unknown>	DEFAULT	2
__sys_connect			.symtab	0x16914	68	FUNC	<unknown>	DEFAULT	2
__sys_recv			.symtab	0x16a98	68	FUNC	<unknown>	DEFAULT	2
__sys_recvfrom			.symtab	0x16b4c	72	FUNC	<unknown>	DEFAULT	2
__sys_send			.symtab	0x16c1c	68	FUNC	<unknown>	DEFAULT	2
__sys_sendto			.symtab	0x16cd0	76	FUNC	<unknown>	DEFAULT	2
__syscall_error			.symtab	0x1a318	44	FUNC	<unknown>	HIDDEN	2
__syscall_error.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__syscall_fcntl.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__syscall_nanosleep			.symtab	0x1a74c	64	FUNC	<unknown>	DEFAULT	2
__syscall_rt_sigaction			.symtab	0x1a400	64	FUNC	<unknown>	DEFAULT	2
__syscall_rt_sigaction.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__syscall_select			.symtab	0x160dc	68	FUNC	<unknown>	DEFAULT	2
__tls_get_addr			.symtab	0x1cd04	36	FUNC	<unknown>	DEFAULT	2
__uClibc_fini			.symtab	0x19d88	124	FUNC	<unknown>	DEFAULT	2
__uClibc_init			.symtab	0x19e58	88	FUNC	<unknown>	DEFAULT	2

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__uClibc_main			.symtab	0x19eb0	1004	FUNC	<unknown>	DEFAULT	2
__uClibc_main.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
__uclibc_progname			.symtab	0x201c0	4	OBJECT	<unknown>	HIDDEN	13
__udivsi3			.symtab	0x15b34	252	FUNC	<unknown>	HIDDEN	2
__write			.symtab	0x19ae0	100	FUNC	<unknown>	DEFAULT	2
__write_nocancel			.symtab	0x19ac4	24	FUNC	<unknown>	DEFAULT	2
__xstat32_conv			.symtab	0x1a938	172	FUNC	<unknown>	HIDDEN	2
__xstat64_conv			.symtab	0x1a86c	204	FUNC	<unknown>	HIDDEN	2
_bss_end__			.symtab	0x235a8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_dl_aux_init			.symtab	0x1cf64	56	FUNC	<unknown>	DEFAULT	2
_dl_nothread_init_static_tls			.symtab	0x1cf9c	88	FUNC	<unknown>	HIDDEN	2
_dl_phdr			.symtab	0x235a0	4	OBJECT	<unknown>	DEFAULT	14
_dl_phnum			.symtab	0x235a4	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_dtv_gaps			.symtab	0x23594	1	OBJECT	<unknown>	DEFAULT	14
_dl_tls_dtv_slotinfo_list			.symtab	0x23590	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_generation			.symtab	0x23598	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_max_dtv_idx			.symtab	0x23588	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_setup			.symtab	0x1cc9c	104	FUNC	<unknown>	DEFAULT	2
_dl_tls_static_align			.symtab	0x23584	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_static_nelem			.symtab	0x2359c	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_static_size			.symtab	0x2358c	4	OBJECT	<unknown>	DEFAULT	14
_dl_tls_static_used			.symtab	0x23580	4	OBJECT	<unknown>	DEFAULT	14
_edata			.symtab	0x202bc	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_end			.symtab	0x235a8	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_exit			.symtab	0x1a440	104	FUNC	<unknown>	DEFAULT	2
_exit.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_fini			.symtab	0x1e9c8	0	FUNC	<unknown>	DEFAULT	3
_fixed_buffers			.symtab	0x208bc	8192	OBJECT	<unknown>	DEFAULT	14
_fopen.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_init			.symtab	0x80d4	0	FUNC	<unknown>	DEFAULT	1
_memcpy			.symtab	0x1c2c0	0	FUNC	<unknown>	HIDDEN	2
_pthread_cleanup_pop_restore			.symtab	0x19d5c	44	FUNC	<unknown>	DEFAULT	2
_pthread_cleanup_push_defer			.symtab	0x19d54	8	FUNC	<unknown>	DEFAULT	2
_rfill.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_setjmp			.symtab	0x1a3cc	8	FUNC	<unknown>	DEFAULT	2
_sigintr			.symtab	0x231f4	8	OBJECT	<unknown>	HIDDEN	14
_start			.symtab	0x8194	0	FUNC	<unknown>	DEFAULT	2
_stdio.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_stdio_fopen			.symtab	0x1b1c4	1120	FUNC	<unknown>	HIDDEN	2
_stdio_init			.symtab	0x1b624	128	FUNC	<unknown>	HIDDEN	2
_stdio_openlist			.symtab	0x201ec	4	OBJECT	<unknown>	DEFAULT	13
_stdio_openlist_add_lock			.symtab	0x2089c	12	OBJECT	<unknown>	DEFAULT	14
_stdio_openlist_dec_use			.symtab	0x1ba98	688	FUNC	<unknown>	HIDDEN	2
_stdio_openlist_del_count			.symtab	0x208b8	4	OBJECT	<unknown>	DEFAULT	14
_stdio_openlist_del_lock			.symtab	0x208a8	12	OBJECT	<unknown>	DEFAULT	14
_stdio_openlist_use_count			.symtab	0x208b4	4	OBJECT	<unknown>	DEFAULT	14
_stdio_streams			.symtab	0x201f0	204	OBJECT	<unknown>	DEFAULT	13
_stdio_term			.symtab	0x1b6a4	356	FUNC	<unknown>	HIDDEN	2
_stdio_user_locking			.symtab	0x201d4	4	OBJECT	<unknown>	DEFAULT	13
_trans2r.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_wcommit.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
abort			.symtab	0x18354	296	FUNC	<unknown>	DEFAULT	2
abort.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
accept			.symtab	0x1685c	116	FUNC	<unknown>	DEFAULT	2
accept.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
add_auth_entry			.symtab	0x10c14	352	FUNC	<unknown>	DEFAULT	2
anti_gdb_entry			.symtab	0xfc30	24	FUNC	<unknown>	DEFAULT	2
attack.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
attack_app.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
attack_get_opt_int			.symtab	0xa5d0	112	FUNC	<unknown>	DEFAULT	2
attack_get_opt_ip			.symtab	0xa564	108	FUNC	<unknown>	DEFAULT	2
attack_get_opt_str			.symtab	0xa1f0	92	FUNC	<unknown>	DEFAULT	2
attack_gre.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
attack_gre_eth			.symtab	0xa9d4	1684	FUNC	<unknown>	DEFAULT	2
attack_gre_ip			.symtab	0xb068	1564	FUNC	<unknown>	DEFAULT	2
attack_init			.symtab	0xa640	916	FUNC	<unknown>	DEFAULT	2
attack_method_http			.symtab	0x81d0	8224	FUNC	<unknown>	DEFAULT	2
attack_parse			.symtab	0xa348	540	FUNC	<unknown>	DEFAULT	2
attack_start			.symtab	0xa24c	252	FUNC	<unknown>	DEFAULT	2
attack_tcp.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
attack_tcp_ack			.symtab	0xb684	1784	FUNC	<unknown>	DEFAULT	2
attack_tcp_syn			.symtab	0xbd7c	1708	FUNC	<unknown>	DEFAULT	2
attack_udp.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
attack_udp_dns			.symtab	0xcfec	1728	FUNC	<unknown>	DEFAULT	2
attack_udp_generic			.symtab	0xc6c8	1260	FUNC	<unknown>	DEFAULT	2
attack_udp_ovhhex			.symtab	0xd6ac	1716	FUNC	<unknown>	DEFAULT	2
attack_udp_plain			.symtab	0xc428	672	FUNC	<unknown>	DEFAULT	2
attack_udp_stdhex			.symtab	0xdd60	680	FUNC	<unknown>	DEFAULT	2
attack_udp_vse			.symtab	0xcbb4	1080	FUNC	<unknown>	DEFAULT	2
auth_table			.symtab	0x2032c	4	OBJECT	<unknown>	DEFAULT	14
auth_table_len			.symtab	0x20300	4	OBJECT	<unknown>	DEFAULT	14
auth_table_max_weight			.symtab	0x20330	2	OBJECT	<unknown>	DEFAULT	14
been_there_done_that			.symtab	0x20338	4	OBJECT	<unknown>	DEFAULT	14
bind			.symtab	0x168d0	68	FUNC	<unknown>	DEFAULT	2
bind.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
brk			.symtab	0x1cff4	88	FUNC	<unknown>	DEFAULT	2
brk.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
bsd_signal			.symtab	0x16e94	196	FUNC	<unknown>	DEFAULT	2
calloc			.symtab	0x17974	320	FUNC	<unknown>	DEFAULT	2
calloc.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
checksum.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
checksum_generic			.symtab	0xe008	80	FUNC	<unknown>	DEFAULT	2
checksum_tcpudp			.symtab	0xe058	164	FUNC	<unknown>	DEFAULT	2
clock			.symtab	0x166fc	52	FUNC	<unknown>	DEFAULT	2
clock.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
close			.symtab	0x199c0	100	FUNC	<unknown>	DEFAULT	2
closedir			.symtab	0x162a0	272	FUNC	<unknown>	DEFAULT	2
closedir.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
completed.5105			.symtab	0x202bc	1	OBJECT	<unknown>	DEFAULT	14
conn_table			.symtab	0x22e14	4	OBJECT	<unknown>	DEFAULT	14
connect			.symtab	0x16958	116	FUNC	<unknown>	DEFAULT	2
connect.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
crtstuff.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
crtstuff.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
dl-support.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
ensure_single_instance			.symtab	0xfc48	428	FUNC	<unknown>	DEFAULT	2
environ			.symtab	0x2088c	4	OBJECT	<unknown>	DEFAULT	14
errno			.symtab	0x0	4	TLS	<unknown>	DEFAULT	8
errno.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
exit			.symtab	0x18aa0	196	FUNC	<unknown>	DEFAULT	2
exit.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fake_time			.symtab	0x20334	4	OBJECT	<unknown>	DEFAULT	14
fclose			.symtab	0x1ae74	816	FUNC	<unknown>	DEFAULT	2
fclose.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fcntl			.symtab	0x15e38	244	FUNC	<unknown>	DEFAULT	2
fd_ctrl			.symtab	0x200b8	4	OBJECT	<unknown>	DEFAULT	13

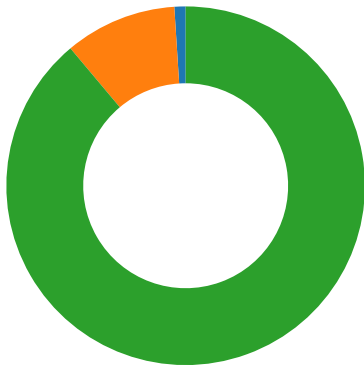
Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
fd_serv			.symtab	0x200bc	4	OBJECT	<unknown>	DEFAULT	13
fd_to_DIR			.symtab	0x163b0	208	FUNC	<unknown>	DEFAULT	2
fdopendir			.symtab	0x16544	176	FUNC	<unknown>	DEFAULT	2
fflush_unlocked			.symtab	0x1bd48	940	FUNC	<unknown>	DEFAULT	2
fflush_unlocked.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fgetc			.symtab	0x1b838	324	FUNC	<unknown>	DEFAULT	2
fgetc.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fgetc_unlocked			.symtab	0x1c0f4	300	FUNC	<unknown>	DEFAULT	2
fgetc_unlocked.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fgets			.symtab	0x1b97c	284	FUNC	<unknown>	DEFAULT	2
fgets.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fgets_unlocked			.symtab	0x1c220	160	FUNC	<unknown>	DEFAULT	2
fgets_unlocked.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fopen			.symtab	0x1b1a4	32	FUNC	<unknown>	DEFAULT	2
fopen.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fork			.symtab	0x192d4	972	FUNC	<unknown>	DEFAULT	2
fork.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fork_handler_pool			.symtab	0x20344	1348	OBJECT	<unknown>	DEFAULT	14
frame_dummy			.symtab	0x8134	0	FUNC	<unknown>	DEFAULT	2
free			.symtab	0x180d8	572	FUNC	<unknown>	DEFAULT	2
free.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
fstat			.symtab	0x1a4a8	100	FUNC	<unknown>	DEFAULT	2
fstat.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
get_eit_entry			.symtab	0x1d564	544	FUNC	<unknown>	DEFAULT	2
getc			.symtab	0x1b838	324	FUNC	<unknown>	DEFAULT	2
getc_unlocked			.symtab	0x1c0f4	300	FUNC	<unknown>	DEFAULT	2
getdents.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getdents64.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getdtablesize			.symtab	0x1a5ac	44	FUNC	<unknown>	DEFAULT	2
getdtablesize.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getegid			.symtab	0x1a5d8	20	FUNC	<unknown>	DEFAULT	2
getegid.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
geteuid			.symtab	0x1a5ec	20	FUNC	<unknown>	DEFAULT	2
geteuid.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getgid			.symtab	0x1a600	20	FUNC	<unknown>	DEFAULT	2
getgid.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getpagesize			.symtab	0x1a614	40	FUNC	<unknown>	DEFAULT	2
getpagesize.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getpid			.symtab	0x19738	72	FUNC	<unknown>	DEFAULT	2
getpid.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getppid			.symtab	0x15f2c	20	FUNC	<unknown>	DEFAULT	2
getppid.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getrlimit			.symtab	0x1a63c	56	FUNC	<unknown>	DEFAULT	2
getrlimit.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getsockname			.symtab	0x169cc	68	FUNC	<unknown>	DEFAULT	2
getsockname.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getsockopt			.symtab	0x16a10	72	FUNC	<unknown>	DEFAULT	2
getsockopt.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
gettimeofday			.symtab	0x1a674	64	FUNC	<unknown>	DEFAULT	2
gettimeofday.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
getuid			.symtab	0x1a6b4	20	FUNC	<unknown>	DEFAULT	2
getuid.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
h_errno			.symtab	0x4	4	TLS	<unknown>	DEFAULT	8
index			.symtab	0x1c7d0	240	FUNC	<unknown>	DEFAULT	2
inet_addr			.symtab	0x167f0	40	FUNC	<unknown>	DEFAULT	2
inet_aton			.symtab	0x1cb2c	248	FUNC	<unknown>	DEFAULT	2
inet_aton.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
inet_makeaddr.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
init_static_tls			.symtab	0x1cc24	120	FUNC	<unknown>	DEFAULT	2
initfini.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
initfini.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
initstate			.symtab	0x185f0	192	FUNC	<unknown>	DEFAULT	2
initstate_r			.symtab	0x188bc	248	FUNC	<unknown>	DEFAULT	2
ioctl			.symtab	0x15f40	224	FUNC	<unknown>	DEFAULT	2
ioctl.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
ioctl_keeppalive			.symtab	0xfe3c	608	FUNC	<unknown>	DEFAULT	2
ioctl_pid			.symtab	0x202e8	4	OBJECT	<unknown>	DEFAULT	14
isatty			.symtab	0x1ca8c	36	FUNC	<unknown>	DEFAULT	2
isatty.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
kill			.symtab	0x16020	56	FUNC	<unknown>	DEFAULT	2
kill.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
killer.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
killer_init			.symtab	0xe6a0	5520	FUNC	<unknown>	DEFAULT	2
killer_kill			.symtab	0xe0fc	40	FUNC	<unknown>	DEFAULT	2
killer_kill_by_port			.symtab	0xe124	1404	FUNC	<unknown>	DEFAULT	2
killer_pid			.symtab	0x202e0	4	OBJECT	<unknown>	DEFAULT	14
killer_realpath			.symtab	0x22e00	4	OBJECT	<unknown>	DEFAULT	14
killer_realpath_len			.symtab	0x202e4	4	OBJECT	<unknown>	DEFAULT	14
libc-cancellation.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
libc-lowlevellock.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
libc-tls.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
libc_multiple_threads.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
listen			.symtab	0x16a58	64	FUNC	<unknown>	DEFAULT	2
listen.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
llseek.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
local_bind.4764			.symtab	0x200c4	1	OBJECT	<unknown>	DEFAULT	13
lseek64			.symtab	0x1d40c	112	FUNC	<unknown>	DEFAULT	2
main			.symtab	0x1009c	1964	FUNC	<unknown>	DEFAULT	2
main.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
malloc			.symtab	0x1703c	2360	FUNC	<unknown>	DEFAULT	2
malloc.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
malloc_trim			.symtab	0x18314	64	FUNC	<unknown>	DEFAULT	2
memcpy			.symtab	0x16730	4	FUNC	<unknown>	DEFAULT	2
memmove			.symtab	0x16740	4	FUNC	<unknown>	DEFAULT	2
mempcpy			.symtab	0x1d3a8	36	FUNC	<unknown>	DEFAULT	2
mempcpy.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
memset			.symtab	0x16750	156	FUNC	<unknown>	DEFAULT	2
methods			.symtab	0x202dc	4	OBJECT	<unknown>	DEFAULT	14
methods_len			.symtab	0x202d8	1	OBJECT	<unknown>	DEFAULT	14
mmap			.symtab	0x1a29c	124	FUNC	<unknown>	DEFAULT	2
mmap.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
mremap			.symtab	0x1a6c8	68	FUNC	<unknown>	DEFAULT	2
mremap.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
munmap			.symtab	0x1a70c	64	FUNC	<unknown>	DEFAULT	2
munmap.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
mylock			.symtab	0x200e4	24	OBJECT	<unknown>	DEFAULT	13
mylock			.symtab	0x200fc	24	OBJECT	<unknown>	DEFAULT	13
nanosleep			.symtab	0x1a78c	96	FUNC	<unknown>	DEFAULT	2
nanosleep.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
nprocessors_onln			.symtab	0x18b64	332	FUNC	<unknown>	DEFAULT	2
object.5113			.symtab	0x202c0	24	OBJECT	<unknown>	DEFAULT	14
open			.symtab	0x19a50	100	FUNC	<unknown>	DEFAULT	2
opendir			.symtab	0x16480	196	FUNC	<unknown>	DEFAULT	2
opendir.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
parse_config.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
pending_connection			.symtab	0x202ec	1	OBJECT	<unknown>	DEFAULT	14

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
pr-support.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
prctl			.symtab	0x16058	68	FUNC	<unknown>	DEFAULT	2
prctl.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
program_invocation_name			.symtab	0x201c8	4	OBJECT	<unknown>	DEFAULT	13
program_invocation_short_name			.symtab	0x201c4	4	OBJECT	<unknown>	DEFAULT	13
raise			.symtab	0x19780	240	FUNC	<unknown>	DEFAULT	2
raise.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
rand			.symtab	0x1847c	24	FUNC	<unknown>	DEFAULT	2
rand.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
rand.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
rand_alpha_str			.symtab	0x1090c	316	FUNC	<unknown>	DEFAULT	2
rand_init			.symtab	0x108a4	104	FUNC	<unknown>	DEFAULT	2
rand_next			.symtab	0x10848	92	FUNC	<unknown>	DEFAULT	2
rand_str			.symtab	0x10a48	220	FUNC	<unknown>	DEFAULT	2
random			.symtab	0x18494	164	FUNC	<unknown>	DEFAULT	2
random.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
random_poly_info			.symtab	0x1f934	40	OBJECT	<unknown>	DEFAULT	4
random_r			.symtab	0x18754	144	FUNC	<unknown>	DEFAULT	2
random_r.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
randtbl			.symtab	0x20114	128	OBJECT	<unknown>	DEFAULT	13
read			.symtab	0x19b70	100	FUNC	<unknown>	DEFAULT	2
readdir			.symtab	0x165f4	232	FUNC	<unknown>	DEFAULT	2
readdir.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
readdir64			.symtab	0x1a9e4	236	FUNC	<unknown>	DEFAULT	2
readdir64.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
readlink			.symtab	0x1609c	64	FUNC	<unknown>	DEFAULT	2
readlink.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
realloc			.symtab	0x17ab4	960	FUNC	<unknown>	DEFAULT	2
realloc.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
recv			.symtab	0x16adc	112	FUNC	<unknown>	DEFAULT	2
recv.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
recvfrom			.symtab	0x16b94	136	FUNC	<unknown>	DEFAULT	2
recvfrom.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
register-atfork.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
resolv.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
resolve_cnc_addr			.symtab	0xfdf4	72	FUNC	<unknown>	DEFAULT	2
resolve_func			.symtab	0x200c0	4	OBJECT	<unknown>	DEFAULT	13
restore_core_regs			.symtab	0x1e138	28	FUNC	<unknown>	HIDDEN	2
rindex			.symtab	0x1c9f0	80	FUNC	<unknown>	DEFAULT	2
rsck			.symtab	0x22e18	4	OBJECT	<unknown>	DEFAULT	14
rsck_out			.symtab	0x22e20	4	OBJECT	<unknown>	DEFAULT	14
sbrk			.symtab	0x1a7ec	108	FUNC	<unknown>	DEFAULT	2
sbrk.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
scanner.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
scanner_init			.symtab	0x10d74	13452	FUNC	<unknown>	DEFAULT	2
scanner_kill			.symtab	0x10b24	40	FUNC	<unknown>	DEFAULT	2
scanner_pid			.symtab	0x22e1c	4	OBJECT	<unknown>	DEFAULT	14
scanner_rawpkt			.symtab	0x20304	40	OBJECT	<unknown>	DEFAULT	14
select			.symtab	0x16120	132	FUNC	<unknown>	DEFAULT	2
select.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
send			.symtab	0x16c60	112	FUNC	<unknown>	DEFAULT	2
send.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
sendto			.symtab	0x16d1c	136	FUNC	<unknown>	DEFAULT	2
sendto.c			.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS

Network Behavior

Network Port Distribution



Total Packets: 99

- 23 (Telnet)
- 2323 undefined
- 63645 undefined

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 12:25:21.279584885 CEST	192.168.2.23	1.1.1.1	0x4fc4	Standard query (0)	daisy.ubun tu.com	A (IP address)	IN (0x0001)
May 27, 2022 12:25:21.279680014 CEST	192.168.2.23	1.1.1.1	0xc71c	Standard query (0)	daisy.ubun tu.com	28	IN (0x0001)
May 27, 2022 12:25:21.574745893 CEST	192.168.2.23	1.1.1.1	0xba07	Standard query (0)	daisy.ubun tu.com	28	IN (0x0001)
May 27, 2022 12:26:48.042598009 CEST	192.168.2.23	1.1.1.1	0x2ac4	Standard query (0)	daisy.ubun tu.com	28	IN (0x0001)
May 27, 2022 12:27:03.098156929 CEST	192.168.2.23	1.1.1.1	0xd584	Standard query (0)	daisy.ubun tu.com	28	IN (0x0001)
May 27, 2022 12:27:21.695652008 CEST	192.168.2.23	1.1.1.1	0xcfa8	Standard query (0)	daisy.ubun tu.com	28	IN (0x0001)
May 27, 2022 12:27:45.585656881 CEST	192.168.2.23	1.1.1.1	0x8eca	Standard query (0)	daisy.ubun tu.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 12:25:21.296778917 CEST	1.1.1.1	192.168.2.23	0x4fc4	No error (0)	daisy.ubun tu.com		185.125.188.137	A (IP address)	IN (0x0001)
May 27, 2022 12:25:21.296778917 CEST	1.1.1.1	192.168.2.23	0x4fc4	No error (0)	daisy.ubun tu.com		185.125.188.136	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: 6gIL6GLh9R PID: 6234, Parent PID: 6129

General

Start time:	12:24:50
Start date:	27/05/2022
Path:	/tmp/6gIL6GLh9R
Arguments:	/tmp/6gIL6GLh9R
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: 6glL6GLh9R PID: 6236, Parent PID: 6234		—
General		—
Start time:	12:24:51	
Start date:	27/05/2022	
Path:	/tmp/6glL6GLh9R	
Arguments:	n/a	
File size:	4956856 bytes	
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1	

Analysis Process: 6glL6GLh9R PID: 6237, Parent PID: 6234		—
General		—
Start time:	12:24:51	
Start date:	27/05/2022	
Path:	/tmp/6glL6GLh9R	
Arguments:	n/a	
File size:	4956856 bytes	
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1	

Analysis Process: 6glL6GLh9R PID: 6240, Parent PID: 6237		—
General		—
Start time:	12:24:51	
Start date:	27/05/2022	
Path:	/tmp/6glL6GLh9R	
Arguments:	n/a	
File size:	4956856 bytes	
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1	

Analysis Process: 6glL6GLh9R PID: 6241, Parent PID: 6237		—
General		—
Start time:	12:24:51	
Start date:	27/05/2022	
Path:	/tmp/6glL6GLh9R	
Arguments:	n/a	
File size:	4956856 bytes	
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1	

File Activities		—
File Deleted		▼
File Read		▼
File Written		▼
Directory Enumerated		▼

Analysis Process: 6glL6GLh9R PID: 6242, Parent PID: 6237		—
General		—
Start time:	12:24:51	
Start date:	27/05/2022	
Path:	/tmp/6glL6GLh9R	
Arguments:	n/a	
File size:	4956856 bytes	
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1	

Analysis Process: systemd PID: 6249, Parent PID: 1		—
General		—

Start time:	12:24:58
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6249, Parent PID: 1

General

Start time:	12:24:58
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 6266, Parent PID: 1

General

Start time:	12:24:58
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 6266, Parent PID: 1

General

Start time:	12:24:58
Start date:	27/05/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 6270, Parent PID: 1

General

Start time:	12:25:00
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6270, Parent PID: 1

General		—
Start time:	12:25:00	
Start date:	27/05/2022	
Path:	/usr/bin/journalctl	
Arguments:	/usr/bin/journalctl --flush	
File size:	80120 bytes	
MD5 hash:	bf3a987344f3bacafc44efd882abda8b	

File Activities		—
File Read		▼

Analysis Process: systemd PID: 6323, Parent PID: 1		—
General		—
Start time:	12:25:17	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: whoopsie PID: 6323, Parent PID: 1		—
General		—
Start time:	12:25:17	
Start date:	27/05/2022	
Path:	/usr/bin/whoopsie	
Arguments:	/usr/bin/whoopsie -f	
File size:	68592 bytes	
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8	

File Activities		—
File Created		▼
File Read		▼
File Written		▼
File Moved		▼
Directory Enumerated		▼
Directory Created		▼
Permission Modified		▼

Analysis Process: systemd PID: 6327, Parent PID: 1		—
General		—
Start time:	12:25:17	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: dbus-daemon PID: 6327, Parent PID: 1		—
General		—
Start time:	12:25:17	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: systemd PID: 6328, Parent PID: 1860 —

General	—
Start time:	12:25:17
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6328, Parent PID: 1860 —

General	—
Start time:	12:25:17
Start date:	27/05/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities	—
File Read	▼
File Written	▼
Directory Enumerated	▼
Directory Created	▼

Analysis Process: systemd PID: 6333, Parent PID: 1 —

General	—
Start time:	12:25:19
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 6333, Parent PID: 1 —

General	—
Start time:	12:25:19
Start date:	27/05/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

File Activities	—
File Read	▼

Analysis Process: systemd PID: 6336, Parent PID: 1 —

General	—
Start time:	12:25:19
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 6336, Parent PID: 1

General

Start time:	12:25:19
Start date:	27/05/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaef

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 6399, Parent PID: 1

General

Start time:	12:25:20
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 6399, Parent PID: 1

General

Start time:	12:25:20
Start date:	27/05/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 6404, Parent PID: 1

General

Start time:	12:25:22
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 6404, Parent PID: 1

General		—
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/sbin/agetty	
Arguments:	/sbin/agetty -o "-p -- \u" --noclear tty2 linux	
File size:	69000 bytes	
MD5 hash:	3a374724ba7e863768139bdd60ca36f7	

File Activities		—
File Read		▼
File Written		▼
Owner / Group Modified		▼
Permission Modified		▼

Analysis Process: systemd PID: 6406, Parent PID: 1 —

General		—
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: rsyslogd PID: 6406, Parent PID: 1 —

General		—
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/usr/sbin/rsyslogd	
Arguments:	/usr/sbin/rsyslogd -n -iNONE	
File size:	727248 bytes	
MD5 hash:	0b8087fc907c42eb3c81a691db258e33	

File Activities		—
File Read		▼
File Written		▼
Directory Enumerated		▼

Analysis Process: gdm3 PID: 6408, Parent PID: 1320 —

General		—
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/usr/sbin/gdm3	
Arguments:	n/a	
File size:	453296 bytes	
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f	

Analysis Process: Default PID: 6408, Parent PID: 1320 —

General		—
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/etc/gdm3/PrimeOff/Default	
Arguments:	/etc/gdm3/PrimeOff/Default	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

File Activities		—
File Read		▼
Analysis Process: systemd-udev PID: 6409, Parent PID: 6306		
General		
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd-udev	
Arguments:	n/a	
File size:	744008 bytes	
MD5 hash:	f73f513acb71492d92fab1f44611f64a	

Analysis Process: cached_setup_terminal.sh PID: 6409, Parent PID: 6306		
General		
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/etc/console-setup/cached_setup_terminal.sh	
Arguments:	/etc/console-setup/cached_setup_terminal.sh vcs2	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

File Activities		—
File Read		▼
Analysis Process: gdm3 PID: 6410, Parent PID: 1320		
General		
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/usr/sbin/gdm3	
Arguments:	n/a	
File size:	453296 bytes	
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f	

Analysis Process: Default PID: 6410, Parent PID: 1320		
General		
Start time:	12:25:22	
Start date:	27/05/2022	
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: 6411, Parent PID: 1320		
General		
Start time:	12:25:22	
Start date:	27/05/2022	
Path:	/usr/sbin/gdm3	
Arguments:	n/a	
File size:	453296 bytes	
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f	

Analysis Process: Default PID: 6411, Parent PID: 1320		—
General		—
Start time:	12:25:22	
Start date:	27/05/2022	
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: 6417, Parent PID: 1		—
General		—
Start time:	12:25:23	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: gpu-manager PID: 6417, Parent PID: 1		—
General		—
Start time:	12:25:23	
Start date:	27/05/2022	
Path:	/usr/bin/gpu-manager	
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log	
File size:	76616 bytes	
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761	

File Activities		—
File Deleted		▼
File Read		▼
File Written		▼
Directory Enumerated		▼

Analysis Process: gpu-manager PID: 6418, Parent PID: 6417		—
General		—
Start time:	12:25:24	
Start date:	27/05/2022	
Path:	/usr/bin/gpu-manager	
Arguments:	n/a	
File size:	76616 bytes	
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761	

Analysis Process: sh PID: 6418, Parent PID: 6417		—
General		—
Start time:	12:25:24	
Start date:	27/05/2022	
Path:	/bin/sh	
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[:space:]]*\$\" /etc/modprobe.d/*.conf"	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: sh PID: 6419, Parent PID: 6418 —

General	—
Start time:	12:25:24
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6419, Parent PID: 6418 —

General	—
Start time:	12:25:24
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*\$/etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	—
File Read	▼

Analysis Process: gpu-manager PID: 6420, Parent PID: 6417 —

General	—
Start time:	12:25:24
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6420, Parent PID: 6417 —

General	—
Start time:	12:25:24
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*\$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: sh PID: 6421, Parent PID: 6420 —

General	—
Start time:	12:25:24
Start date:	27/05/2022
Path:	/bin/sh

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

Analysis Process: grep PID: 6421, Parent PID: 6420

General

Start time:	12:25:24
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*\$/lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6422, Parent PID: 6417

General

Start time:	12:25:24
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6422, Parent PID: 6417

General

Start time:	12:25:24
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*\$\" /etc/modprobe.d/*.*conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6423, Parent PID: 6422

General

Start time:	12:25:24
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6423, Parent PID: 6422

General

Start time:	12:25:24
Start date:	27/05/2022
Path:	/usr/bin/grep

Arguments:	grep -G ^blacklist.*radeon[[:space:]]*\$/etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6424, Parent PID: 6417

General

Start time:	12:25:25
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6424, Parent PID: 6417

General

Start time:	12:25:25
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*\$/lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6425, Parent PID: 6424

General

Start time:	12:25:25
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6425, Parent PID: 6424

General

Start time:	12:25:25
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*\$/lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6426, Parent PID: 6417

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6426, Parent PID: 6417

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*\$/etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6427, Parent PID: 6426

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6427, Parent PID: 6426

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6428, Parent PID: 6417

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6428, Parent PID: 6417

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[:space:]]*\$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6429, Parent PID: 6428

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6429, Parent PID: 6428

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	
File Read	

Analysis Process: gpu-manager PID: 6430, Parent PID: 6417

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6430, Parent PID: 6417

General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6431, Parent PID: 6430	
General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6431, Parent PID: 6430	
General	
Start time:	12:25:26
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	
File Read	

Analysis Process: gpu-manager PID: 6433, Parent PID: 6417	
General	
Start time:	12:25:27
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6433, Parent PID: 6417	
General	
Start time:	12:25:27
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6435, Parent PID: 6433	
General	
Start time:	12:25:28
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6435, Parent PID: 6433	
General	
Start time:	12:25:28
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	
File Read	

Analysis Process: systemd PID: 6439, Parent PID: 1	
General	
Start time:	12:25:29
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 6439, Parent PID: 1	
General	
Start time:	12:25:29
Start date:	27/05/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: generate-config PID: 6440, Parent PID: 6439	
General	
Start time:	12:25:30
Start date:	27/05/2022
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 6440, Parent PID: 6439	
General	
Start time:	12:25:30
Start date:	27/05/2022
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities	
File Read	

Directory Enumerated

Analysis Process: systemd PID: 6441, Parent PID: 1

General	
Start time:	12:25:33
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 6441, Parent PID: 1

General	
Start time:	12:25:33
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 6446, Parent PID: 1

General	
Start time:	12:25:43
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 6446, Parent PID: 1

General	
Start time:	12:25:43
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities

File Deleted

File Read

File Written

Directory Created

Owner / Group Modified

Permission Modified

Analysis Process: gdm3 PID: 6451, Parent PID: 6446

General	
Start time:	12:25:43
Start date:	27/05/2022

Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities	—
Directory Enumerated	▼

Analysis Process: plymouth PID: 6451, Parent PID: 6446	—
---	---

General	—
Start time:	12:25:43
Start date:	27/05/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

File Activities	—
File Read	▼

Analysis Process: gdm3 PID: 6470, Parent PID: 6446	—
---	---

General	—
Start time:	12:25:45
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities	—
Directory Enumerated	▼

Analysis Process: gdm-session-worker PID: 6470, Parent PID: 6446	—
---	---

General	—
Start time:	12:25:45
Start date:	27/05/2022
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: 6474, Parent PID: 6470	—
---	---

General	—
Start time:	12:25:48
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 6474, Parent PID: 6470		—
General		—
Start time:	12:25:48	
Start date:	27/05/2022	
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		▼
Directory Created		▼

Analysis Process: gdm-wayland-session PID: 6476, Parent PID: 6474		—
General		—
Start time:	12:25:48	
Start date:	27/05/2022	
Path:	/usr/lib/gdm3/gdm-wayland-session	
Arguments:	n/a	
File size:	76368 bytes	
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c	

File Activities		—
Directory Enumerated		▼

Analysis Process: dbus-daemon PID: 6476, Parent PID: 6474		—
General		—
Start time:	12:25:48	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	dbus-daemon --print-address 3 --session	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

File Activities		—
File Read		▼
Directory Enumerated		▼

Analysis Process: dbus-daemon PID: 6480, Parent PID: 6476		—
General		—
Start time:	12:25:49	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	n/a	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

Analysis Process: dbus-daemon PID: 6481, Parent PID: 6480		—
General		—
Start time:	12:25:49	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	n/a	
File size:	249032 bytes	

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

File Activities	—
File Written	▼

Analysis Process: false PID: 6481, Parent PID: 6480 —

General	—
Start time:	12:25:49
Start date:	27/05/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities	—
File Read	▼

Analysis Process: gdm-wayland-session PID: 6482, Parent PID: 6474 —

General	—
Start time:	12:25:49
Start date:	27/05/2022
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: 6482, Parent PID: 6474 —

General	—
Start time:	12:25:49
Start date:	27/05/2022
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: 6483, Parent PID: 6482 —

General	—
Start time:	12:25:49
Start date:	27/05/2022
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 6483, Parent PID: 6482 —

General	—
Start time:	12:25:49
Start date:	27/05/2022
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	▼

Analysis Process: gdm3 PID: 6484, Parent PID: 6446 —

General	—
Start time:	12:25:50
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities	—
Directory Enumerated	▼

Analysis Process: Default PID: 6484, Parent PID: 6446 —

General	—
Start time:	12:25:50
Start date:	27/05/2022
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: 6485, Parent PID: 6446 —

General	—
Start time:	12:25:50
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

File Activities	—
Directory Enumerated	▼

Analysis Process: Default PID: 6485, Parent PID: 6446 —

General	—
Start time:	12:25:50
Start date:	27/05/2022
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: 6452, Parent PID: 1		—
General		—
Start time:	12:25:43	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: accounts-daemon PID: 6452, Parent PID: 1		—
General		—
Start time:	12:25:43	
Start date:	27/05/2022	
Path:	/usr/lib/accounts-service/accounts-daemon	
Arguments:	/usr/lib/accounts-service/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: 6465, Parent PID: 6452		—
General		—
Start time:	12:25:43	
Start date:	27/05/2022	
Path:	/usr/lib/accounts-service/accounts-daemon	
Arguments:	n/a	
File size:	203192 bytes	
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30	

File Activities		—
Directory Enumerated		▼

Analysis Process: language-validate PID: 6465, Parent PID: 6452		—
General		—
Start time:	12:25:43	
Start date:	27/05/2022	
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: 6466, Parent PID: 6465		—
General		—
Start time:	12:25:43	
Start date:	27/05/2022	

Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 6466, Parent PID: 6465

General	
Start time:	12:25:43
Start date:	27/05/2022
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: 6467, Parent PID: 6466

General	
Start time:	12:25:43
Start date:	27/05/2022
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 6467, Parent PID: 6466

General	
Start time:	12:25:43
Start date:	27/05/2022
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: 6468, Parent PID: 6467

General	
Start time:	12:25:44
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 6468, Parent PID: 6467

General	
Start time:	12:25:44
Start date:	27/05/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes

MD5 hash:	c72a78792469db86d91369c9057f20d2
-----------	----------------------------------

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: sh PID: 6469, Parent PID: 6467	—
---	---

General	—
Start time:	12:25:44
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6469, Parent PID: 6467	—
---	---

General	—
Start time:	12:25:44
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	—
File Read	▼

Analysis Process: gvfsd-fuse PID: 6493, Parent PID: 2038	—
---	---

General	—
Start time:	12:26:02
Start date:	27/05/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 6493, Parent PID: 2038	—
---	---

General	—
Start time:	12:26:02
Start date:	27/05/2022
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdc97a91acea900566

File Activities	—
File Read	▼

Analysis Process: systemd PID: 6515, Parent PID: 1	—
---	---

General	—
Start time:	12:26:42
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

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

Analysis Process: journalctl PID: 6515, Parent PID: 1

General	
Start time:	12:26:42
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read

Analysis Process: systemd PID: 6516, Parent PID: 1

General	
Start time:	12:26:42
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 6516, Parent PID: 1

General	
Start time:	12:26:42
Start date:	27/05/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 6517, Parent PID: 1

General	
Start time:	12:26:43
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 6517, Parent PID: 1

General	
Start time:	12:26:43
Start date:	27/05/2022
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: 6520, Parent PID: 1	—
General	—
Start time:	12:26:44
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 6520, Parent PID: 1	—
General	—
Start time:	12:26:44
Start date:	27/05/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: systemd PID: 6522, Parent PID: 1860	—
General	—
Start time:	12:26:46
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6522, Parent PID: 1860	—
General	—
Start time:	12:26:46
Start date:	27/05/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities	—
File Read	▼
File Written	▼

Directory Enumerated	▼
Directory Created	▼

Analysis Process: systemd PID: 6526, Parent PID: 1		—
General		—
Start time:	12:26:46	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: systemd-logind PID: 6526, Parent PID: 1		—
General		—
Start time:	12:26:46	
Start date:	27/05/2022	
Path:	/lib/systemd/systemd-logind	
Arguments:	/lib/systemd/systemd-logind	
File size:	268576 bytes	
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef	

File Activities	—
File Read	▼
File Written	▼
File Moved	▼
Directory Enumerated	▼
Directory Created	▼
Permission Modified	▼

Analysis Process: systemd PID: 6584, Parent PID: 1		—
General		—
Start time:	12:26:47	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: rtkit-daemon PID: 6584, Parent PID: 1		—
General		—
Start time:	12:26:47	
Start date:	27/05/2022	
Path:	/usr/libexec/rtkit-daemon	
Arguments:	/usr/libexec/rtkit-daemon	
File size:	68096 bytes	
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7	

File Activities	—
File Read	▼

Analysis Process: systemd PID: 6585, Parent PID: 1		—
General		—
Start time:	12:26:47	
Start date:	27/05/2022	

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

Analysis Process: gpu-manager PID: 6585, Parent PID: 1

General

Start time:	12:26:47
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Analysis Process: gpu-manager PID: 6589, Parent PID: 6585

General

Start time:	12:26:48
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6589, Parent PID: 6585

General

Start time:	12:26:48
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6590, Parent PID: 6589

General

Start time:	12:26:48
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6590, Parent PID: 6589

General

Start time:	12:26:48
Start date:	27/05/2022

Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6596, Parent PID: 6585

General

Start time:	12:26:49
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6596, Parent PID: 6585

General

Start time:	12:26:49
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*\$\" /lib/modprobe.d/*.*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6597, Parent PID: 6596

General

Start time:	12:26:49
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6597, Parent PID: 6596

General

Start time:	12:26:49
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6599, Parent PID: 6585

General	
Start time:	12:26:49
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6599, Parent PID: 6585

General	
Start time:	12:26:49
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 6601, Parent PID: 6599

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6601, Parent PID: 6599

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: gpu-manager PID: 6602, Parent PID: 6585

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6602, Parent PID: 6585

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*\$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6604, Parent PID: 6602

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6604, Parent PID: 6602

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	
File Read	

Analysis Process: gpu-manager PID: 6605, Parent PID: 6585

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6605, Parent PID: 6585

General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6606, Parent PID: 6605	
General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6606, Parent PID: 6605	
General	
Start time:	12:26:50
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*\$/etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	
File Read	

Analysis Process: gpu-manager PID: 6607, Parent PID: 6585	
General	
Start time:	12:26:51
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6607, Parent PID: 6585	
General	
Start time:	12:26:51
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*\$/lib/modprobe.d/*conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6608, Parent PID: 6607	
General	
Start time:	12:26:51
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6608, Parent PID: 6607	
General	
Start time:	12:26:51
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities	
File Read	

Analysis Process: gpu-manager PID: 6610, Parent PID: 6585	
General	
Start time:	12:26:52
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6610, Parent PID: 6585	
General	
Start time:	12:26:52
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 6611, Parent PID: 6610	
General	
Start time:	12:26:52
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6611, Parent PID: 6610	
General	
Start time:	12:26:52
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities		—
File Read		▼
Analysis Process: gpu-manager PID: 6615, Parent PID: 6585		—
General		—
Start time:	12:26:52	
Start date:	27/05/2022	
Path:	/usr/bin/gpu-manager	
Arguments:	n/a	
File size:	76616 bytes	
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761	

Analysis Process: sh PID: 6615, Parent PID: 6585		—
General		—
Start time:	12:26:52	
Start date:	27/05/2022	
Path:	/bin/sh	
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /lib/modprobe.d/*.conf"	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

File Activities		—
File Read		▼
Directory Enumerated		▼

Analysis Process: sh PID: 6616, Parent PID: 6615		—
General		—
Start time:	12:26:53	
Start date:	27/05/2022	
Path:	/bin/sh	
Arguments:	n/a	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: grep PID: 6616, Parent PID: 6615		—
General		—
Start time:	12:26:53	
Start date:	27/05/2022	
Path:	/usr/bin/grep	
Arguments:	grep -G ^blacklist.*nouveau[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf	
File size:	199136 bytes	
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5	

File Activities		—
File Read		▼

Analysis Process: systemd PID: 6588, Parent PID: 1		—
General		—
Start time:	12:26:48	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: polkitd PID: 6588, Parent PID: 1	
General	
Start time:	12:26:48
Start date:	27/05/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

File Activities	
File Read	
Directory Enumerated	
Directory Created	

Analysis Process: systemd PID: 6598, Parent PID: 1	
General	
Start time:	12:26:49
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6598, Parent PID: 1	
General	
Start time:	12:26:49
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities	
File Read	

Analysis Process: systemd PID: 6600, Parent PID: 1	
General	
Start time:	12:26:55
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 6600, Parent PID: 1	
General	
Start time:	12:26:55
Start date:	27/05/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \lu" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

File Activities	
------------------------	--

File Read	▼
File Written	▼
Owner / Group Modified	▼
Permission Modified	▼

Analysis Process: systemd PID: 6609, Parent PID: 1

General	—
Start time:	12:26:52
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 6609, Parent PID: 1

General	—
Start time:	12:26:52
Start date:	27/05/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities	—
File Read	▼
File Written	▼
Directory Enumerated	▼

Analysis Process: systemd PID: 6620, Parent PID: 1

General	—
Start time:	12:26:55
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 6620, Parent PID: 1

General	—
Start time:	12:26:55
Start date:	27/05/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: generate-config PID: 6623, Parent PID: 6620

General	—
Start time:	12:26:55
Start date:	27/05/2022

Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 6623, Parent PID: 6620

General	
Start time:	12:26:55
Start date:	27/05/2022
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

File Activities

File Read	
Directory Enumerated	

Analysis Process: systemd PID: 6622, Parent PID: 1

General	
Start time:	12:26:55
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6622, Parent PID: 1

General	
Start time:	12:26:55
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities

File Read	
------------------	--

Analysis Process: systemd PID: 6624, Parent PID: 1860

General	
Start time:	12:26:56
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 6624, Parent PID: 1860

General	
Start time:	12:26:56
Start date:	27/05/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes

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

File Activities	—
File Read	▼
Directory Enumerated	▼
Directory Created	▼

Analysis Process: systemd PID: 6625, Parent PID: 1 —

General	—
Start time:	12:26:56
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 6625, Parent PID: 1 —

General	—
Start time:	12:26:56
Start date:	27/05/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities	—
File Deleted	▼
File Read	▼
File Written	▼
File Moved	▼
Directory Enumerated	▼
Directory Created	▼

Analysis Process: systemd PID: 6628, Parent PID: 1 —

General	—
Start time:	12:26:59
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 6628, Parent PID: 1 —

General	—
Start time:	12:26:59
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: systemd PID: 6629, Parent PID: 1		—
General		—
Start time:	12:27:00	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: whoopsie PID: 6629, Parent PID: 1		—
General		—
Start time:	12:27:00	
Start date:	27/05/2022	
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: 6634, Parent PID: 1		—
General		—
Start time:	12:27:02	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: dbus-daemon PID: 6634, Parent PID: 1		—
General		—
Start time:	12:27:02	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

File Activities		—
File Read		▼
Directory Enumerated		▼

Analysis Process: systemd PID: 6635, Parent PID: 1860		—
General		—
Start time:	12:27:03	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	

File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6635, Parent PID: 1860	
General	
Start time:	12:27:03
Start date:	27/05/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities	
File Read	
File Written	
Directory Enumerated	
Directory Created	

Analysis Process: systemd PID: 6636, Parent PID: 1	
General	
Start time:	12:27:03
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6636, Parent PID: 1	
General	
Start time:	12:27:03
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

File Activities	
File Read	

Analysis Process: systemd PID: 6641, Parent PID: 1	
General	
Start time:	12:27:04
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 6641, Parent PID: 1	
General	
Start time:	12:27:04
Start date:	27/05/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes

MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaef
-----------	---------------------------------

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 6698, Parent PID: 1

General

Start time:	12:27:04
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 6698, Parent PID: 1

General

Start time:	12:27:04
Start date:	27/05/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

File Activities

File Read

Analysis Process: systemd PID: 6703, Parent PID: 1

General

Start time:	12:27:05
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 6703, Parent PID: 1

General

Start time:	12:27:05
Start date:	27/05/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

File Activities

File Read

Directory Enumerated

Directory Created

Analysis Process: systemd PID: 6707, Parent PID: 1	
General	
Start time:	12:27:10
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 6707, Parent PID: 1	
General	
Start time:	12:27:10
Start date:	27/05/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 6709, Parent PID: 1	
General	
Start time:	12:27:08
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 6709, Parent PID: 1	
General	
Start time:	12:27:08
Start date:	27/05/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

Analysis Process: systemd PID: 6716, Parent PID: 1	
General	
Start time:	12:27:09
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 6716, Parent PID: 1	
General	
Start time:	12:27:09
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm3 PID: 6719, Parent PID: 6716	
General	
Start time:	12:27:10
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: plymouth PID: 6719, Parent PID: 6716	
General	
Start time:	12:27:10
Start date:	27/05/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

Analysis Process: gdm3 PID: 6729, Parent PID: 6716	
General	
Start time:	12:27:12
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 6729, Parent PID: 6716	
General	
Start time:	12:27:12
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-session-worker PID: 6739, Parent PID: 6729	
General	
Start time:	12:27:17
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 6739, Parent PID: 6729	
General	
Start time:	12:27:17
Start date:	27/05/2022
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

Analysis Process: gdm-wayland-session PID: 6741, Parent PID: 6739		—
General		—
Start time:	12:27:17	
Start date:	27/05/2022	
Path:	/usr/lib/gdm3/gdm-wayland-session	
Arguments:	n/a	
File size:	76368 bytes	
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c	

Analysis Process: dbus-daemon PID: 6741, Parent PID: 6739		—
General		—
Start time:	12:27:17	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	dbus-daemon --print-address 3 --session	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

Analysis Process: dbus-daemon PID: 6751, Parent PID: 6741		—
General		—
Start time:	12:27:19	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	n/a	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

Analysis Process: dbus-daemon PID: 6752, Parent PID: 6751		—
General		—
Start time:	12:27:19	
Start date:	27/05/2022	
Path:	/usr/bin/dbus-daemon	
Arguments:	n/a	
File size:	249032 bytes	
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c	

Analysis Process: false PID: 6752, Parent PID: 6751		—
General		—
Start time:	12:27:19	
Start date:	27/05/2022	
Path:	/bin/false	
Arguments:	/bin/false	
File size:	39256 bytes	
MD5 hash:	3177546c74e4f0062909eae43d948bfc	

Analysis Process: gdm-wayland-session PID: 6753, Parent PID: 6739		—
General		—
Start time:	12:27:20	
Start date:	27/05/2022	
Path:	/usr/lib/gdm3/gdm-wayland-session	
Arguments:	n/a	
File size:	76368 bytes	
MD5 hash:	d3def63cf1e83f7fb8a0f13b1744ff7c	

Analysis Process: dbus-run-session PID: 6753, Parent PID: 6739		—
General		—
Start time:	12:27:20	
Start date:	27/05/2022	
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	

Analysis Process: gdm3 PID: 6754, Parent PID: 6716		—
General		—
Start time:	12:27:20	
Start date:	27/05/2022	
Path:	/usr/sbin/gdm3	
Arguments:	n/a	
File size:	453296 bytes	
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f	

Analysis Process: Default PID: 6754, Parent PID: 6716		—
General		—
Start time:	12:27:20	
Start date:	27/05/2022	
Path:	/etc/gdm3/PrimeOff/Default	
Arguments:	/etc/gdm3/PrimeOff/Default	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: gdm3 PID: 6756, Parent PID: 6716		—
General		—
Start time:	12:27:20	
Start date:	27/05/2022	
Path:	/usr/sbin/gdm3	
Arguments:	n/a	
File size:	453296 bytes	
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f	

Analysis Process: Default PID: 6756, Parent PID: 6716		—
General		—
Start time:	12:27:20	
Start date:	27/05/2022	
Path:	/etc/gdm3/PrimeOff/Default	
Arguments:	/etc/gdm3/PrimeOff/Default	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: systemd PID: 6720, Parent PID: 1		—
General		—
Start time:	12:27:10	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: accounts-daemon PID: 6720, Parent PID: 1		—
General		—
Start time:	12:27:10	
Start date:	27/05/2022	
Path:	/usr/lib/accountsservice/accounts-daemon	
Arguments:	/usr/lib/accountsservice/accounts-daemon	
File size:	203192 bytes	
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30	

Analysis Process: accounts-daemon PID: 6724, Parent PID: 6720		—
General		—
Start time:	12:27:10	
Start date:	27/05/2022	
Path:	/usr/lib/accountsservice/accounts-daemon	
Arguments:	n/a	
File size:	203192 bytes	
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30	

Analysis Process: language-validate PID: 6724, Parent PID: 6720		—
General		—
Start time:	12:27:10	
Start date:	27/05/2022	
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	

Analysis Process: language-validate PID: 6725, Parent PID: 6724		—
General		—
Start time:	12:27:10	
Start date:	27/05/2022	
Path:	/usr/share/language-tools/language-validate	
Arguments:	n/a	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: language-options PID: 6725, Parent PID: 6724		—
General		—
Start time:	12:27:10	
Start date:	27/05/2022	
Path:	/usr/share/language-tools/language-options	
Arguments:	/usr/share/language-tools/language-options	
File size:	3478464 bytes	
MD5 hash:	16a21f464119ea7fad1d3660de963637	

Analysis Process: language-options PID: 6726, Parent PID: 6725		—
General		—
Start time:	12:27:11	
Start date:	27/05/2022	
Path:	/usr/share/language-tools/language-options	
Arguments:	n/a	
File size:	3478464 bytes	
MD5 hash:	16a21f464119ea7fad1d3660de963637	

Analysis Process: sh PID: 6726, Parent PID: 6725	
General	
Start time:	12:27:11
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "locale -a grep -F .utf8 "
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6727, Parent PID: 6726	
General	
Start time:	12:27:11
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 6727, Parent PID: 6726	
General	
Start time:	12:27:11
Start date:	27/05/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 6728, Parent PID: 6726	
General	
Start time:	12:27:11
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6728, Parent PID: 6726	
General	
Start time:	12:27:11
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 6730, Parent PID: 1	
General	
Start time:	12:27:12
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6730, Parent PID: 1	
General	
Start time:	12:27:12
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 6734, Parent PID: 1	
General	
Start time:	12:27:13
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 6734, Parent PID: 1	
General	
Start time:	12:27:13
Start date:	27/05/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 6737, Parent PID: 1	
General	
Start time:	12:27:16
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 6737, Parent PID: 1	
General	
Start time:	12:27:16
Start date:	27/05/2022
Path:	/lib/systemd/systemd
Arguments:	/lib/systemd/systemd --user
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 6742, Parent PID: 6737	
General	
Start time:	12:27:17
Start date:	27/05/2022
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 6743, Parent PID: 6742	
General	
Start time:	12:27:18
Start date:	27/05/2022
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: 30-systemd-environment-d-generator PID: 6743, Parent PID: 6742	
General	
Start time:	12:27:18
Start date:	27/05/2022
Path:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
Arguments:	/usr/lib/systemd/user-environment-generators/30-systemd-environment-d-generator
File size:	14480 bytes
MD5 hash:	42417da8051ba8ee0eea7854c62d99ca

Analysis Process: systemd PID: 6850, Parent PID: 6737	
General	
Start time:	12:27:30
Start date:	27/05/2022
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemctl PID: 6850, Parent PID: 6737	
General	
Start time:	12:27:30
Start date:	27/05/2022
Path:	/bin/systemctl
Arguments:	/bin/systemctl --user set-environment DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/127/bus
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

Analysis Process: systemd PID: 6855, Parent PID: 6737	
General	
Start time:	12:27:31
Start date:	27/05/2022
Path:	/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6855, Parent PID: 6737	
General	
Start time:	12:27:32
Start date:	27/05/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 6744, Parent PID: 1	
General	
Start time:	12:27:18
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 6744, Parent PID: 1	
General	
Start time:	12:27:18
Start date:	27/05/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

Analysis Process: systemd PID: 6757, Parent PID: 1	
General	
Start time:	12:27:20
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 6757, Parent PID: 1	
General	
Start time:	12:27:20
Start date:	27/05/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 6759, Parent PID: 1860	
General	
Start time:	12:27:22
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6759, Parent PID: 1860	
General	
Start time:	12:27:22
Start date:	27/05/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 6762, Parent PID: 1	
General	
Start time:	12:27:23
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 6762, Parent PID: 1	
General	
Start time:	12:27:23
Start date:	27/05/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaef

Analysis Process: systemd PID: 6821, Parent PID: 1	
General	
Start time:	12:27:24
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 6821, Parent PID: 1	
General	
Start time:	12:27:24
Start date:	27/05/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

Analysis Process: systemd PID: 6824, Parent PID: 1	
General	
Start time:	12:27:25
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 6824, Parent PID: 1	
General	
Start time:	12:27:25
Start date:	27/05/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

Analysis Process: systemd PID: 6825, Parent PID: 1		—
General		—
Start time:	12:27:25	
Start date:	27/05/2022	
Path:	/usr/lib/systemd/systemd	
Arguments:	n/a	
File size:	1620224 bytes	
MD5 hash:	9b2bec7092a40488108543f9334aab75	

Analysis Process: gpu-manager PID: 6825, Parent PID: 1		—
General		—
Start time:	12:27:25	
Start date:	27/05/2022	
Path:	/usr/bin/gpu-manager	
Arguments:	/usr/bin/gpu-manager --log /var/log/gpu-manager.log	
File size:	76616 bytes	
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761	

Analysis Process: gpu-manager PID: 6827, Parent PID: 6825		—
General		—
Start time:	12:27:26	
Start date:	27/05/2022	
Path:	/usr/bin/gpu-manager	
Arguments:	n/a	
File size:	76616 bytes	
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761	

Analysis Process: sh PID: 6827, Parent PID: 6825		—
General		—
Start time:	12:27:26	
Start date:	27/05/2022	
Path:	/bin/sh	
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[:space:]]*\$\" /etc/modprobe.d/* .conf"	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: sh PID: 6828, Parent PID: 6827		—
General		—
Start time:	12:27:26	
Start date:	27/05/2022	
Path:	/bin/sh	
Arguments:	n/a	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: grep PID: 6828, Parent PID: 6827		—
General		—
Start time:	12:27:26	
Start date:	27/05/2022	
Path:	/usr/bin/grep	
Arguments:	grep -G ^blacklist.*nvidia[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf	

File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6832, Parent PID: 6825

General

Start time:	12:27:26
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6832, Parent PID: 6825

General

Start time:	12:27:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nvidia[[:space:]]*\$\" /lib/modprobe.d/*conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6833, Parent PID: 6832

General

Start time:	12:27:26
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6833, Parent PID: 6832

General

Start time:	12:27:26
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nvidia[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6834, Parent PID: 6825

General

Start time:	12:27:27
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6834, Parent PID: 6825

General

Start time:	12:27:27
Start date:	27/05/2022
Path:	/bin/sh

Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6835, Parent PID: 6834

General

Start time:	12:27:27
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6835, Parent PID: 6834

General

Start time:	12:27:27
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6837, Parent PID: 6825

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6837, Parent PID: 6825

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*radeon[[:space:]]*\$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6838, Parent PID: 6837

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6838, Parent PID: 6837

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*radeon[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6845, Parent PID: 6825

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6845, Parent PID: 6825

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*\$\" /etc/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6846, Parent PID: 6845

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6846, Parent PID: 6845

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6847, Parent PID: 6825

General

Start time:	12:27:29
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6847, Parent PID: 6825	
General	
Start time:	12:27:29
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*amdgpu[[:space:]]*\$/lib/modprobe.d/*conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6848, Parent PID: 6847	
General	
Start time:	12:27:29
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6848, Parent PID: 6847	
General	
Start time:	12:27:29
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*amdgpu[[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6851, Parent PID: 6825	
General	
Start time:	12:27:30
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6851, Parent PID: 6825	
General	
Start time:	12:27:30
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[[:space:]]*\$/etc/modprobe.d/*conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6852, Parent PID: 6851	
General	
Start time:	12:27:30
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6852, Parent PID: 6851**General**

Start time:	12:27:30
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[:space:]]*\$ /etc/modprobe.d/alsa-base.conf /etc/modprobe.d/amd64-microcode-blacklist.conf /etc/modprobe.d/blacklist-ath_pci.conf /etc/modprobe.d/blacklist-firewire.conf /etc/modprobe.d/blacklist-framebuffer.conf /etc/modprobe.d/blacklist-modem.conf /etc/modprobe.d/blacklist-oss.conf /etc/modprobe.d/blacklist-rare-network.conf /etc/modprobe.d/blacklist.conf /etc/modprobe.d/intel-microcode-blacklist.conf /etc/modprobe.d/iwlwifi.conf /etc/modprobe.d/mdadm.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: gpu-manager PID: 6853, Parent PID: 6825**General**

Start time:	12:27:31
Start date:	27/05/2022
Path:	/usr/bin/gpu-manager
Arguments:	n/a
File size:	76616 bytes
MD5 hash:	8fae9dd5dd67e1f33d873089c2fd8761

Analysis Process: sh PID: 6853, Parent PID: 6825**General**

Start time:	12:27:31
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	sh -c "grep -G \"^blacklist.*nouveau[:space:]]*\$\" /lib/modprobe.d/*.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sh PID: 6854, Parent PID: 6853**General**

Start time:	12:27:31
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6854, Parent PID: 6853**General**

Start time:	12:27:31
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -G ^blacklist.*nouveau[:space:]]*\$ /lib/modprobe.d/aliases.conf /lib/modprobe.d/blacklist_linux_5.4.0-72-generic.conf /lib/modprobe.d/blacklist_linux_5.4.0-81-generic.conf /lib/modprobe.d/fbdev-blacklist.conf /lib/modprobe.d/systemd.conf
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 6826, Parent PID: 1**General**

Start time:	12:27:32
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: agetty PID: 6826, Parent PID: 1

General

Start time:	12:27:32
Start date:	27/05/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 6836, Parent PID: 1

General

Start time:	12:27:27
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 6836, Parent PID: 1

General

Start time:	12:27:27
Start date:	27/05/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

Analysis Process: systemd PID: 6841, Parent PID: 1

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6841, Parent PID: 1

General

Start time:	12:27:28
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 6856, Parent PID: 1

General

Start time:	12:27:32
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6856, Parent PID: 1

General

Start time:	12:27:32
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 6857, Parent PID: 1

General

Start time:	12:27:32
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 6857, Parent PID: 1

General

Start time:	12:27:32
Start date:	27/05/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 6862, Parent PID: 1860

General

Start time:	12:27:35
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 6862, Parent PID: 1860

General

Start time:	12:27:35
Start date:	27/05/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 6863, Parent PID: 1

General

Start time:	12:27:35
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 6863, Parent PID: 1

General

Start time:	12:27:35
Start date:	27/05/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: generate-config PID: 6864, Parent PID: 6863

General

Start time:	12:27:36
Start date:	27/05/2022
Path:	/usr/share/gdm/generate-config
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: pkill PID: 6864, Parent PID: 6863

General

Start time:	12:27:36
Start date:	27/05/2022
Path:	/usr/bin/pkill
Arguments:	pkill --signal HUP --uid gdm dconf-service
File size:	30968 bytes
MD5 hash:	fa96a75a08109d8842e4865b2907d51f

Analysis Process: systemd PID: 6867, Parent PID: 1

General

Start time:	12:27:39
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 6867, Parent PID: 1

General

Start time:	12:27:39
Start date:	27/05/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

Analysis Process: systemd PID: 6868, Parent PID: 1

General

Start time:	12:27:40
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm-wait-for-drm PID: 6868, Parent PID: 1

General

Start time:	12:27:40
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-wait-for-drm
Arguments:	/usr/lib/gdm3/gdm-wait-for-drm
File size:	14640 bytes
MD5 hash:	82043ba752c6930b4e6aaea2f7747545

Analysis Process: systemd PID: 6870, Parent PID: 1

General

Start time:	12:27:41
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 6870, Parent PID: 1

General

Start time:	12:27:41
Start date:	27/05/2022
Path:	/usr/bin/dbus-daemon
Arguments:	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: systemd PID: 6871, Parent PID: 1860

General

Start time:	12:27:42
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6871, Parent PID: 1860

General

Start time:	12:27:42
Start date:	27/05/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 6874, Parent PID: 1

General

Start time:	12:27:43
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 6874, Parent PID: 1

General

Start time:	12:27:43
Start date:	27/05/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

Analysis Process: systemd PID: 6932, Parent PID: 1

General

Start time:	12:27:43
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 6932, Parent PID: 1

General

Start time:	12:27:43
Start date:	27/05/2022
Path:	/usr/libexec/rtkit-daemon
Arguments:	/usr/libexec/rtkit-daemon
File size:	68096 bytes
MD5 hash:	df0cacf1db4ec95ac70f5b6e06b8ffd7

Analysis Process: systemd PID: 6935, Parent PID: 1

General

Start time:	12:27:44
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6935, Parent PID: 1

General

Start time:	12:27:44
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --flush
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 6939, Parent PID: 1

General

Start time:	12:27:44
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: polkitd PID: 6939, Parent PID: 1

General

Start time:	12:27:44
Start date:	27/05/2022
Path:	/usr/lib/policykit-1/polkitd
Arguments:	/usr/lib/policykit-1/polkitd --no-debug
File size:	121504 bytes
MD5 hash:	8efc9b4b5b524210ad2ea1954a9d0e69

Analysis Process: systemd PID: 6944, Parent PID: 1

General

Start time:	12:27:53
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process:agetty PID: 6944, Parent PID: 1

General

Start time:	12:27:53
Start date:	27/05/2022
Path:	/sbin/agetty
Arguments:	/sbin/agetty -o "-p -- \u" --noclear tty2 linux
File size:	69000 bytes
MD5 hash:	3a374724ba7e863768139bdd60ca36f7

Analysis Process: systemd PID: 6945, Parent PID: 1

General

Start time:	12:27:48
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 6945, Parent PID: 1

General

Start time:	12:27:48
Start date:	27/05/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

Analysis Process: systemd PID: 6952, Parent PID: 1

General

Start time:	12:27:50
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 6952, Parent PID: 1

General

Start time:	12:27:50
Start date:	27/05/2022
Path:	/usr/bin/journalctl
Arguments:	/usr/bin/journalctl --smart-relinquish-var
File size:	80120 bytes
MD5 hash:	bf3a987344f3bacafc44efd882abda8b

Analysis Process: systemd PID: 6953, Parent PID: 1

General

Start time:	12:27:50
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 6953, Parent PID: 1

General

Start time:	12:27:50
Start date:	27/05/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 6954, Parent PID: 1

General

Start time:	12:27:51
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gdm3 PID: 6954, Parent PID: 1

General

Start time:	12:27:51
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	/usr/sbin/gdm3
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm3 PID: 6957, Parent PID: 6954

General

Start time:	12:27:52
Start date:	27/05/2022
Path:	/usr/sbin/gdm3

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

Analysis Process: plymouth PID: 6957, Parent PID: 6954

General

Start time:	12:27:52
Start date:	27/05/2022
Path:	/usr/bin/plymouth
Arguments:	plymouth --ping
File size:	51352 bytes
MD5 hash:	87003efd8dad470042f5e75360a8f49f

Analysis Process: gdm3 PID: 6969, Parent PID: 6954

General

Start time:	12:27:56
Start date:	27/05/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 6969, Parent PID: 6954

General

Start time:	12:27:56
Start date:	27/05/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	"gdm-session-worker [pam/gdm-launch-environment]"
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: systemd PID: 6958, Parent PID: 1

General

Start time:	12:27:52
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 6958, Parent PID: 1

General

Start time:	12:27:52
Start date:	27/05/2022
Path:	/usr/lib/accounts-service/accounts-daemon
Arguments:	/usr/lib/accounts-service/accounts-daemon
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

Analysis Process: accounts-daemon PID: 6964, Parent PID: 6958

General

Start time:	12:27:54
Start date:	27/05/2022
Path:	/usr/lib/accounts-service/accounts-daemon

Arguments:	n/a
File size:	203192 bytes
MD5 hash:	01a899e3fb5e7e434bea1290255a1f30

Analysis Process: language-validate PID: 6964, Parent PID: 6958		—
General		—
Start time:	12:27:54	
Start date:	27/05/2022	
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	

Analysis Process: language-validate PID: 6965, Parent PID: 6964		—
General		—
Start time:	12:27:54	
Start date:	27/05/2022	
Path:	/usr/share/language-tools/language-validate	
Arguments:	n/a	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: language-options PID: 6965, Parent PID: 6964		—
General		—
Start time:	12:27:54	
Start date:	27/05/2022	
Path:	/usr/share/language-tools/language-options	
Arguments:	/usr/share/language-tools/language-options	
File size:	3478464 bytes	
MD5 hash:	16a21f464119ea7fad1d3660de963637	

Analysis Process: language-options PID: 6966, Parent PID: 6965		—
General		—
Start time:	12:27:54	
Start date:	27/05/2022	
Path:	/usr/share/language-tools/language-options	
Arguments:	n/a	
File size:	3478464 bytes	
MD5 hash:	16a21f464119ea7fad1d3660de963637	

Analysis Process: sh PID: 6966, Parent PID: 6965		—
General		—
Start time:	12:27:54	
Start date:	27/05/2022	
Path:	/bin/sh	
Arguments:	sh -c "locale -a grep -F .utf8 "	
File size:	129816 bytes	
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c	

Analysis Process: sh PID: 6967, Parent PID: 6966		—
General		—
Start time:	12:27:54	
Start date:	27/05/2022	
Path:	/bin/sh	

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

Analysis Process: locale PID: 6967, Parent PID: 6966

General

Start time:	12:27:54
Start date:	27/05/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

Analysis Process: sh PID: 6968, Parent PID: 6966

General

Start time:	12:27:54
Start date:	27/05/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 6968, Parent PID: 6966

General

Start time:	12:27:54
Start date:	27/05/2022
Path:	/usr/bin/grep
Arguments:	grep -F .utf8
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

Analysis Process: systemd PID: 6973, Parent PID: 1

General

Start time:	12:27:57
Start date:	27/05/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 6973, Parent PID: 1

General

Start time:	12:27:57
Start date:	27/05/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8