ID: 1577153
Sample Name: arm5.nn-20241218-0633.elf
Cookbook: defaultlinuxfilecookbook.jbs
Time: 07:36:39
Date: 18/12/2024
Version: 41.0.0 Charoite

Table of Contents

Linux Analysis Report

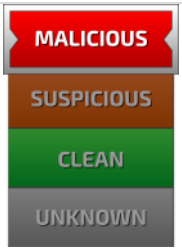
arm5.nn-20241218-0633.elf

Overview

General Information

Sample name:	arm5.nn-20241218-0633.elf
Analysis ID:	1577153
MD5:	22ad871042ce…
SHA1:	f68d2d02fb6df2..
SHA256:	1daa64d77d63…
Tags:	user-elfdigest
Infos:	

Detection



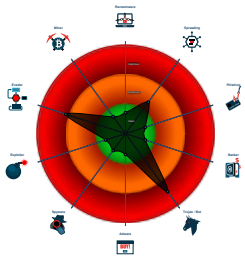
Mirai, Okiru

Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Yara detected Okiru
- Sample deletes itself
- Detected TCP or UDP traffic on non…
- Enumerates processes within the "p…
- Executes the "rm" command used t…
- Found strings indicative of a multi-p…
- Sample contains strings indicative o…
- Sample has stripped symbol table

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1577153
Start date and time:	2024-12-18 07:36:39 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample name:	arm5.nn-20241218-0633.elf
Detection:	MAL
Classification:	mal76.troj.evad.linELF@0/2@0/0

Warnings

Runtime Messages

Command:	/tmp/arm5.nn-20241218-0633.elf
PID:	6208
Exit Code:	139
Exit Code Info:	SIGSEGV (11) Segmentation fault invalid memory reference
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 11 (Segmentation fault) - core dumped

Process Tree

- **system is lnxubuntu20**

- dash New Fork (PID: 6195, Parent: 4334)
  - rm (PID: 6195, Parent: 4334, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.2Vk4GHUvv3 /tmp/tmp.AyMCUiGuNP /tmp/tmp.0eZyUHHcgu
- dash New Fork (PID: 6196, Parent: 4334)
  - rm (PID: 6196, Parent: 4334, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.2Vk4GHUvv3 /tmp/tmp.AyMCUiGuNP /tmp/tmp.0eZyUHHcgu
  - arm5.nn-20241218-0633.elf (PID: 6208, Parent: 6121, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm5.nn-20241218-0633.elf
    - arm5.nn-20241218-0633.elf New Fork (PID: 6233, Parent: 6208)
      - arm5.nn-20241218-0633.elf New Fork (PID: 6235, Parent: 6233)
      - arm5.nn-20241218-0633.elf New Fork (PID: 6236, Parent: 6233)
      - arm5.nn-20241218-0633.elf New Fork (PID: 6238, Parent: 6233)
- udisksd New Fork (PID: 6219, Parent: 799)
  - dumpe2fs (PID: 6219, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- udisksd New Fork (PID: 6298, Parent: 799)
  - dumpe2fs (PID: 6298, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- udisksd New Fork (PID: 6299, Parent: 799)
  - dumpe2fs (PID: 6299, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- gnome-session-binary New Fork (PID: 6331, Parent: 1477)
  - sh (PID: 6331, Parent: 1477, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
  - gsd-housekeeping (PID: 6331, Parent: 1477, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- udisksd New Fork (PID: 6332, Parent: 799)
  - dumpe2fs (PID: 6332, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- udisksd New Fork (PID: 6336, Parent: 799)
  - dumpe2fs (PID: 6336, Parent: 799, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	http://osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	http://https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
arm5.nn-20241218-0633.elf	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	
arm5.nn-20241218-0633.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6208.1.00007fe574017000.00007fe574031000.r-x.sdmp	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	
6208.1.00007fe574017000.00007fe574031000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Process Memory Space: arm5.nn-20241218-0633.elf PID: 6208	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Hooking and other Techniques for Hiding and Protection

Sample deletes itself

Stealing of Sensitive Information

Yara detected Mirai

Yara detected Okiru

Remote Access Functionality

Yara detected Mirai

Yara detected Okiru

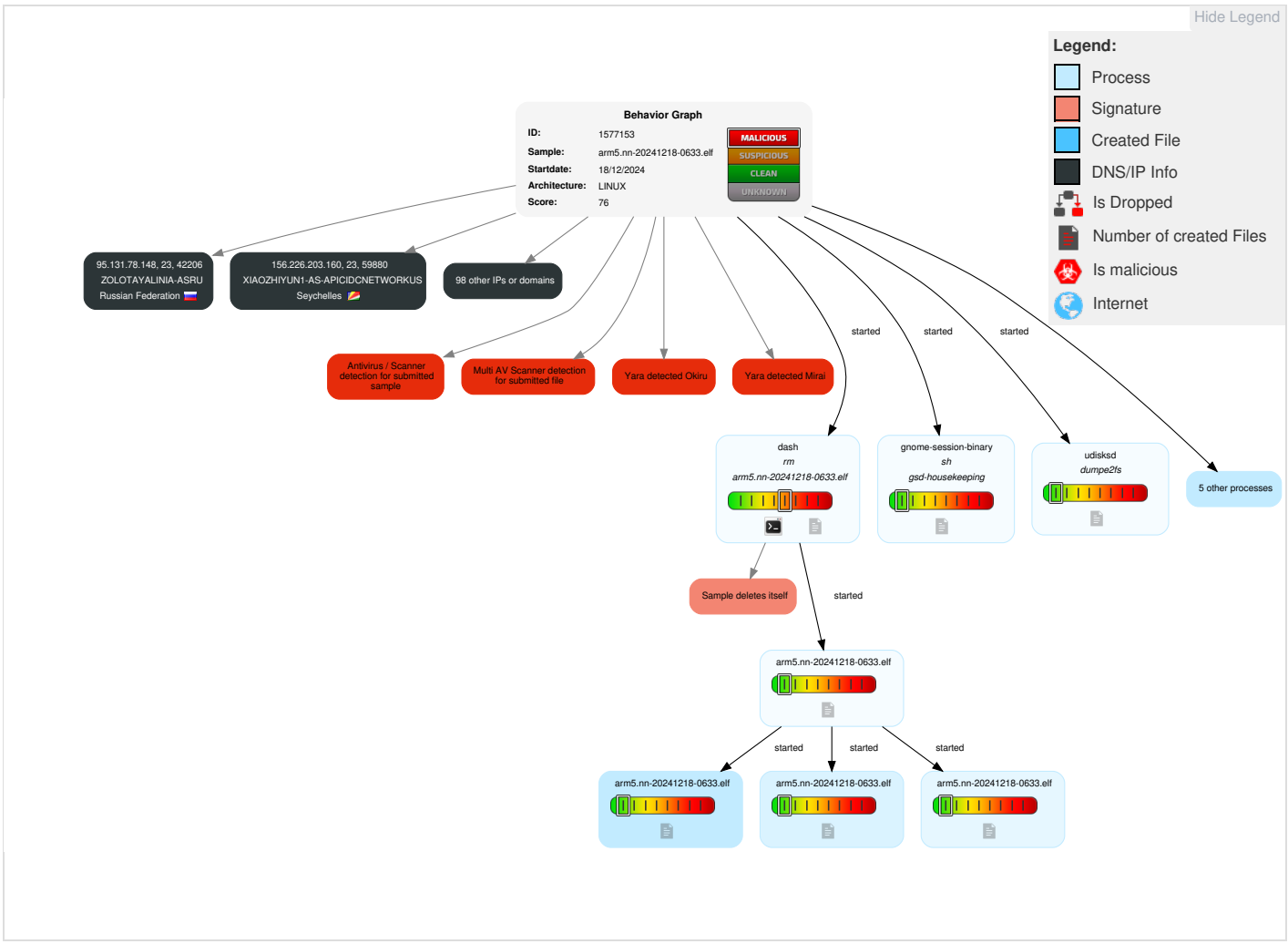
Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	1 Scripting	Valid Accounts	Windows Management Instrumentation	1 Scripting	Path Interception	1 1 File Deletion	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arm5.nn-20241218-0633.elf	37%	Virustotal		Browse
arm5.nn-20241218-0633.elf	47%	ReversingLabs	Linux.Backdoor.Mirai	
arm5.nn-20241218-0633.elf	100%	Avira	EXP/ELF.Mirai.W	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

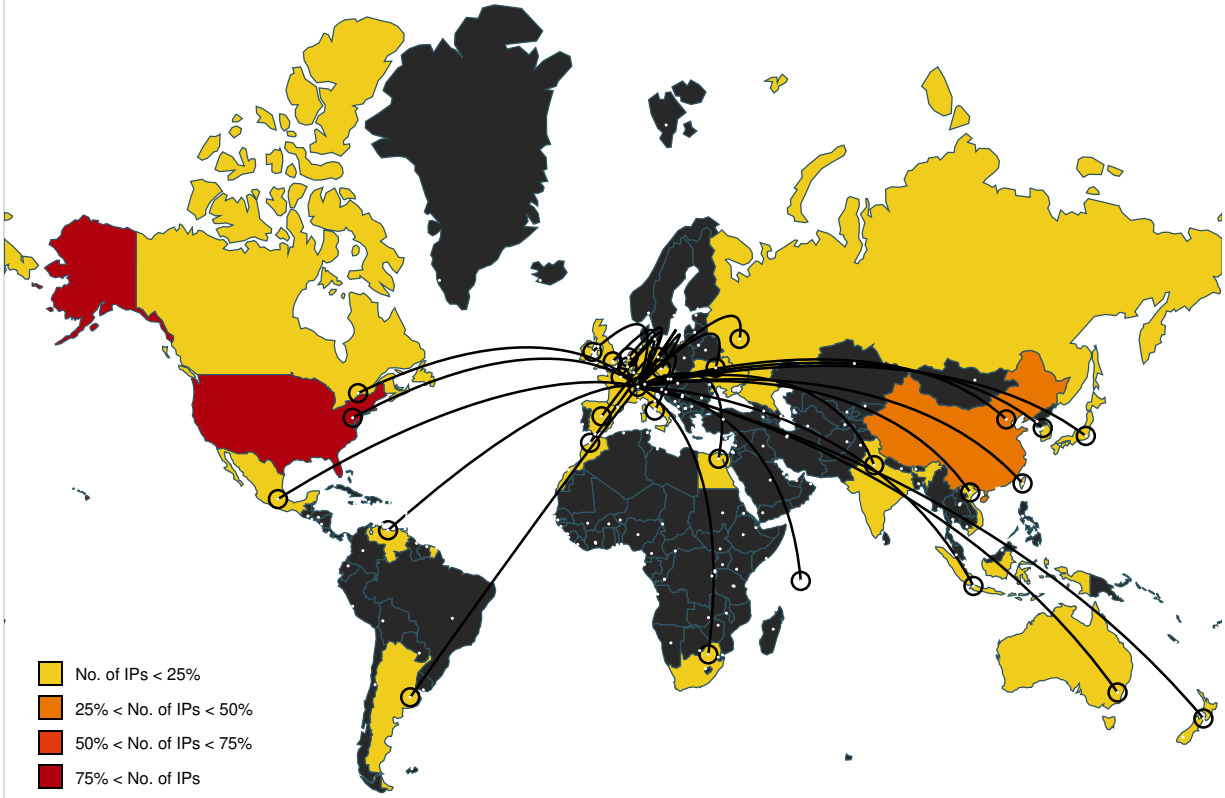
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
15.157.206.185	unknown	United States		71	HP-INTERNET-ASUS	false
155.190.105.235	unknown	Netherlands		20437	AS20437US	false
164.35.51.211	unknown	Belgium		29355	KCELL-ASKZ	false
40.222.127.195	unknown	United States		4249	LILLY-ASUS	false
40.1.165.90	unknown	United States		4249	LILLY-ASUS	false
153.122.122.184	unknown	Japan		131921	GMOCLGMOCLOUDKKJP	false
61.14.205.143	unknown	India		17970	SKYBB-AS-APSKYBroadbandSKYCableCorporationPH	false
207.67.91.54	unknown	United States		30560	GE-MS001US	false
103.143.208.58	unknown	Viet Nam		56150	VHOST-AS-VNVietSolutionsServicesTradingCompanyLimited	false
105.158.78.210	unknown	Morocco		36903	MT-MPLSMA	false
128.66.90.39	unknown	Italy		24608	WINDTRE-ASIT	false
181.183.175.74	unknown	Venezuela		6306	TELEFONICAVENEZOLANACAVE	false
113.13.84.34	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
111.206.47.61	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
148.250.47.5	unknown	Mexico		6503	AxtelSABdeCVMX	false
183.169.48.230	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
220.109.229.200	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
114.74.255.223	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
97.67.71.162	unknown	United States		7029	WINDSTREAMUS	false
123.41.174.130	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.156.48.202	unknown	Switzerland		34578	BEDAGCH	false
112.32.29.51	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
120.196.43.25	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
39.241.4.20	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
79.34.169.131	unknown	Italy		3269	ASN-IBSNAZIT	false
106.108.224.219	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
94.27.2.107	unknown	Ukraine		12530	GOLDENTELECOM-UKRAINEKyivstarPJSCUA	false
33.71.230.164	unknown	United States		2686	ATGS-MMD-ASUS	false
22.4.220.86	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
218.118.11.201	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
210.168.244.162	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
60.216.14.26	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
163.27.95.84	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
173.135.10.184	unknown	United States		10507	SPCSUS	false
37.44.196.174	unknown	Russian Federation		48430	FIRSTDC-ASRU	false
14.177.224.114	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
95.131.78.148	unknown	Russian Federation		41148	ZOLOTAYALINIA-ASRU	false
18.40.70.108	unknown	United States		3	MIT-GATEWAYSUS	false
151.17.74.40	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
83.195.166.18	unknown	France		3215	FranceTelecom-OrangeFR	false
204.208.17.206	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
155.31.220.224	unknown	United States		11809	NET-ERAU-PRCUS	false
91.162.44.227	unknown	France		12322	PROXADFR	false
26.69.120.206	unknown	United States		7922	COMCAST-7922US	false
131.29.217.221	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
148.133.136.251	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
17.192.105.73	unknown	United States		714	APPLE-ENGINEERINGUS	false
217.36.158.157	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
138.222.188.250	unknown	Switzerland		10497	WORLDBANKUS	false
17.157.67.104	unknown	United States		714	APPLE-ENGINEERINGUS	false
109.154.252.158	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
140.167.74.158	unknown	Canada		56736	VASTRAGOTALANDSREGIONENSE	false
55.106.253.168	unknown	United States		361	DNIC-ASBLK-00306-00371US	false
87.149.9.130	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
140.183.143.218	unknown	United States		1503	DNIC-AS-01503US	false
16.207.88.180	unknown	United States		unknown	unknown	false
204.51.124.162	unknown	United States		11303	DATARETURNUS	false
212.90.254.134	unknown	Czech Republic		6740	TISCALICZ	false
114.97.146.113	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
56.58.95.82	unknown	United States		2686	ATGS-MMD-ASUS	false
135.145.118.150	unknown	United States		14962	NCR-252US	false
156.183.7.142	unknown	Egypt		36992	ETISALAT-MISREG	false
66.182.204.117	unknown	United States		20135	MTL-19US	false
214.93.142.185	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
162.175.43.176	unknown	United States		21928	T-MOBILE-AS21928US	false
48.55.16.11	unknown	United States		2686	ATGS-MMD-ASUS	false
59.63.145.177	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
220.123.218.34	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
87.42.38.223	unknown	Ireland		1213	HEANETIE	false
173.46.131.236	unknown	United States		29748	QTS-ASHUS	false
82.231.152.180	unknown	France		12322	PROXADFR	false
93.246.187.209	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
50.21.101.99	unknown	United States		17184	ATL-CBEYONDUS	false
60.220.10.238	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
200.79.141.155	unknown	Mexico		8151	UninetSAdeCVMX	false
49.68.231.143	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
119.70.200.0	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
97.221.104.163	unknown	United States		6167	CELLCO-PARTUS	false
141.61.24.32	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
34.65.20.112	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
145.51.240.33	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
184.183.159.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
158.97.33.46	unknown	Mexico		3640	CICESEMX	false
110.162.74.168	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
134.179.57.223	unknown	United States		26854	NYSUS	false
103.164.226.56	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
74.19.59.248	unknown	United States		7922	COMCAST-7922US	false
32.224.145.220	unknown	United States		2686	ATGS-MMD-ASUS	false
152.22.206.134	unknown	United States		17031	WINSTON-SALEM-SCHOOLSUS	false
156.226.203.160	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	false
135.254.221.60	unknown	United States		10455	LUCENT-CIOUS	false
56.3.220.202	unknown	United States		2686	ATGS-MMD-ASUS	false
66.98.194.87	unknown	United States		36351	SOFTLAYERUS	false
136.148.214.22	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
35.105.190.38	unknown	United States		237	MERIT-AS-14US	false
49.226.56.203	unknown	New Zealand		9500	VODAFONE-TRANSIT-ASVodafoneNZLtdNZ	false
222.61.248.29	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
80.31.14.153	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
200.80.229.78	unknown	Argentina		27754	CooperativaBatandeObrasyServPublicosLtdaAR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.132.12.178	unknown	South Africa		10474	OPTINETZA	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

/etc/motd

/tmp/qemu-open.Lb1GCE (deleted)

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.222049438520164
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm5.nn-20241218-0633.elf
File size:	104'828 bytes
MD5:	22ad871042ce032b7225a4f11f1d3f86
SHA1:	f68d2d02fb6df23061174bd38324d8895a73ddbe
SHA256:	1daa64d77d6383023899ac2eeeb00fe93ed821cdfcf01bf829c3ed5fe2e20bf5
SHA512:	37998c63f92a2e0232f87a043c28bd631ef1d109ee3f1b4ad3a8ebf9c2eeafbc336ea16df3a9e9751ca8ef232aa9da6670901333b76a0b70b184dc828cd74493
SSDEEP:	3072:FLhmGTolcPLLem7y4CxUOvlwh432nnUo:FLhmGScjLem7rCxUOdcv
TLSH:	76A34C52F9819A22C5D566BBF66E02CC376613F8D2EF3207CD15AF24378682B0D7B641
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....(.....Q.td.....-...L."...UX.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)

ELF header

Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	104428
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

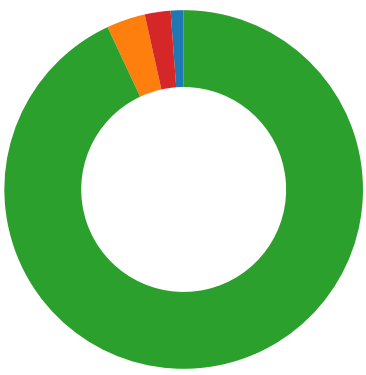
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x1618c	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1e23c	0x1623c	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e250	0x16250	0x2f88	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x291dc	0x191dc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x291e4	0x191e4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x291f0	0x191f0	0x5bc	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x297ac	0x197ac	0x2240	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x197ac	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	0x8000	0x8000	0x191d8	0x191d8	6.2340	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x191dc	0x291dc	0x291dc	0x5d0	0x2810	4.7697	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



Total Packets: 86

- 199 undefined
- 23 (Telnet)
- 38242 undefined
- 443 (HTTPS)

TCP Packets

System Behavior

Analysis Process: dash PID: 6195, Parent PID: 4334

General

Start time (UTC):	06:37:11
Start date (UTC):	18/12/2024
Path:	/usr/bin/dash
Arguments:	-
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 6195, Parent PID: 4334

General

Start time (UTC):	06:37:11
Start date (UTC):	18/12/2024
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.2Vk4GHUvv3 /tmp/tmp.AyMCUiGuNP /tmp/tmp.0eZyUHHcgu
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: dash PID: 6196, Parent PID: 4334

General

Start time (UTC):	06:37:11
Start date (UTC):	18/12/2024
Path:	/usr/bin/dash
Arguments:	-
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 6196, Parent PID: 4334

General

Start time (UTC):	06:37:11
Start date (UTC):	18/12/2024
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.2Vk4GHUvv3 /tmp/tmp.AyMCUiGuNP /tmp/tmp.0eZyUHHcgu
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: arm5.nn-20241218-0633.elf PID: 6208, Parent PID: 6121

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/tmp/arm5.nn-20241218-0633.elf

Arguments:	/tmp/arm5.nn-20241218-0633.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Symbolic Link Created

Analysis Process: arm5.nn-20241218-0633.elf PID: 6233, Parent PID: 6208

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/tmp/arm5.nn-20241218-0633.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm5.nn-20241218-0633.elf PID: 6235, Parent PID: 6233

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/tmp/arm5.nn-20241218-0633.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm5.nn-20241218-0633.elf PID: 6236, Parent PID: 6233

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/tmp/arm5.nn-20241218-0633.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: arm5.nn-20241218-0633.elf PID: 6238, Parent PID: 6233

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/tmp/arm5.nn-20241218-0633.elf
Arguments:	-
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

Directory Enumerated

Analysis Process: udisksd PID: 6219, Parent PID: 799

General	
Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: 6219, Parent PID: 799

General	
Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/sbin/dumpe2fs
Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read

Analysis Process: udisksd PID: 6298, Parent PID: 799

General	
Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: 6298, Parent PID: 799

General	
Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/sbin/dumpe2fs
Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read

Analysis Process: udisksd PID: 6299, Parent PID: 799

General	
Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: 6299, Parent PID: 799

General	
Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/sbin/dumpe2fs

Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read

Analysis Process: gnome-session-binary PID: **6331**, Parent PID: **1477**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/libexec/gnome-session-binary
Arguments:	-
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **6331**, Parent PID: **1477**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/bin/sh
Arguments:	/bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gsd-housekeeping PID: **6331**, Parent PID: **1477**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

File Activities

File Read

Analysis Process: udisksd PID: **6332**, Parent PID: **799**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **6332**, Parent PID: **799**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/sbin/dumpe2fs

Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read

Analysis Process: udisksd PID: **6336**, Parent PID: **799**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **6336**, Parent PID: **799**

General

Start time (UTC):	06:37:19
Start date (UTC):	18/12/2024
Path:	/usr/sbin/dumpe2fs
Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read