ID: 1575253
Sample Name: mips.nn.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:46:08
Date: 15/12/2024
Version: 41.0.0 Charoite

Table of Contents

Linux Analysis Report

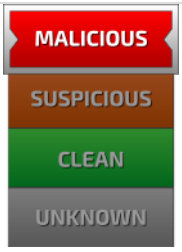
mips.nn.elf

Overview

General Information

Sample name:	mips.nn.elf
Analysis ID:	1575253
MD5:	2145cb16a925…
SHA1:	821c929b723b…
SHA256:	beeeaa8013f74..
Tags:	elf user-abuse_ch
Infos:	

Detection



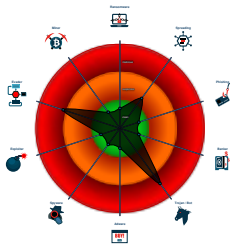
Mirai, Okiru

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…
- Found strings indicative of a multi-p…
- Sample contains strings indicative o…
- Sample has stripped symbol table
- Sample listens on a socket

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1575253
Start date and time:	2024-12-15 00:46:08 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 46s
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:	mips.nn.elf
Detection:	MAL
Classification:	mal76.troj.evad.linELF@0/2@0/0

Warnings

Runtime Messages

Command:	/tmp/mips.nn.elf
PID:	5433
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	The Gorilla Botnet Cats Came After You!
Standard Error:	

Process Tree

- **system is lnxubuntu20**

- mips.nn.elf (PID: 5433, Parent: 5357, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/mips.nn.elf
  - mips.nn.elf New Fork (PID: 5456, Parent: 5433)
    - mips.nn.elf New Fork (PID: 5459, Parent: 5456)
    - mips.nn.elf New Fork (PID: 5461, Parent: 5456)
    - mips.nn.elf New Fork (PID: 5470, Parent: 5456)
- udisksd New Fork (PID: 5443, Parent: 802)
- dumpe2fs (PID: 5443, Parent: 802, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- udisksd New Fork (PID: 5509, Parent: 802)
- dumpe2fs (PID: 5509, Parent: 802, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- udisksd New Fork (PID: 5532, Parent: 802)
- dumpe2fs (PID: 5532, Parent: 802, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- udisksd New Fork (PID: 5533, Parent: 802)
- dumpe2fs (PID: 5533, Parent: 802, MD5: 5c66f7d8f7681a40562cf049ad4b72b4) Arguments: dumpe2fs -h /dev/dm-0
- gnome-session-binary New Fork (PID: 5534, Parent: 1588)
- sh (PID: 5534, Parent: 1588, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 5534, Parent: 1588, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- udisksd New Fork (PID: 5538, Parent: 802)
- dumpe2fs (PID: 5538, Parent: 802, 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
mips.nn.elf	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	
mips.nn.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5433.1.00007fa4d0400000.00007fa4d0420000.r-x.sdmp	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	
5433.1.00007fa4d0400000.00007fa4d0420000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Process Memory Space: mips.nn.elf PID: 5433	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

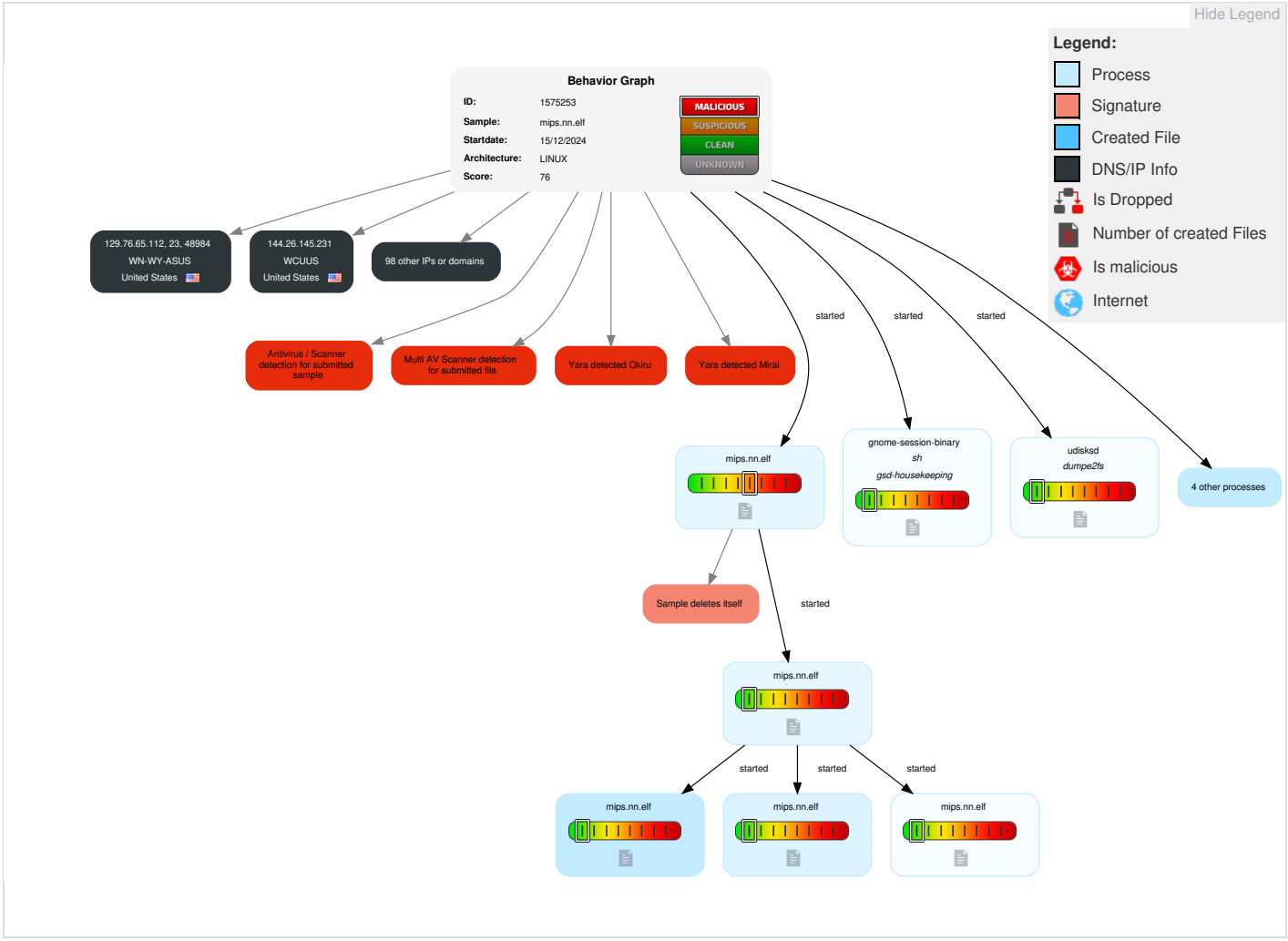
Mitre Att&ck Matrix

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 File Deletion	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Non-Standard Port	Exfiltration Over Other Network Medium	Abuse Accessibility Features

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
mips.nn.elf	42%	ReversingLabs	Linux.Backdoor.Mirai	
mips.nn.elf	100%	Avira	EXP/ELF.Mirai.W	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

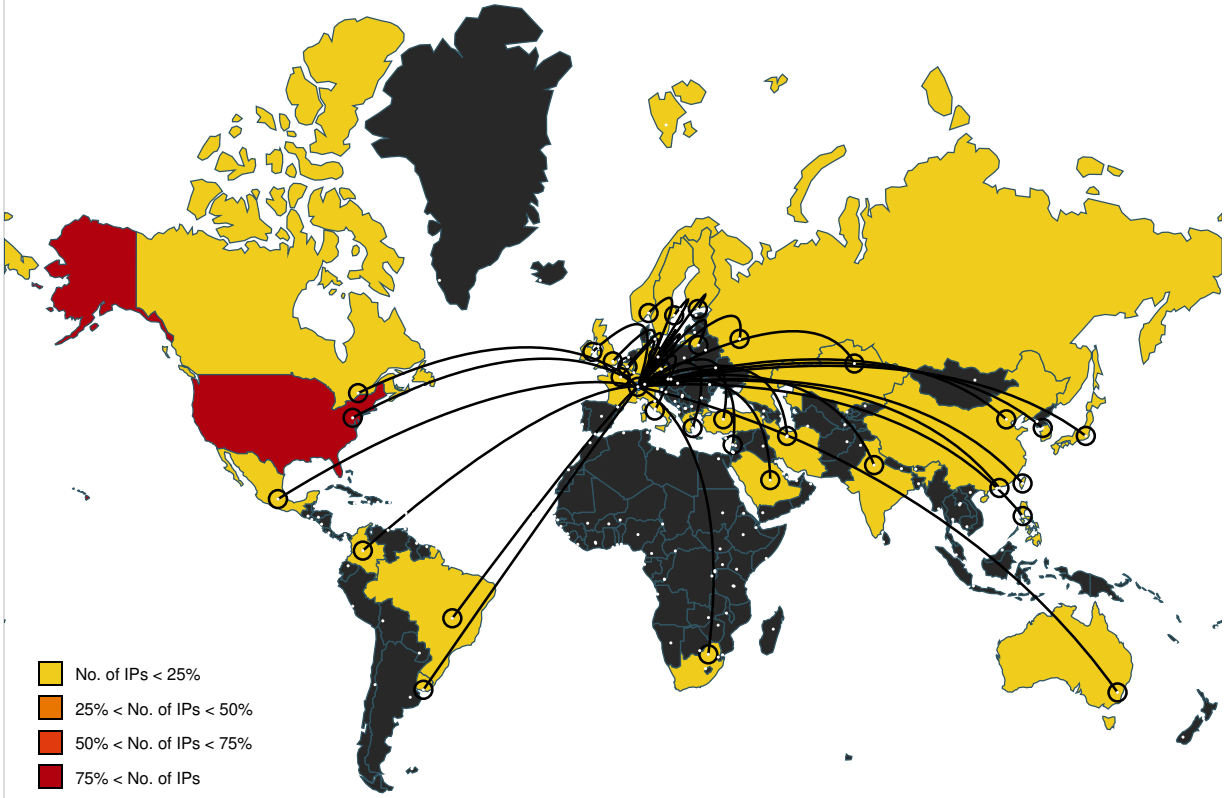
Domains and IPs

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
114.171.214.248	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
123.238.41.160	unknown	India		18101	RELIANCE-COMMUNICATIONS-INRelianceCommunicationsLtdDAKC	false
46.235.136.66	unknown	Italy		197589	ALFANEWSIT	false
162.16.207.15	unknown	United States		35893	ACPCA	false
25.95.13.157	unknown	United Kingdom		7922	COMCAST-7922US	false
79.230.205.174	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
106.171.143.33	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
92.103.218.129	unknown	France		12670	AS-COMPLETELFR	false
131.47.77.23	unknown	United States		409	AFCONC-BLOCK1-ASUS	false
176.158.31.11	unknown	France		5410	BOUYGTEL-ISPFR	false
16.92.248.169	unknown	United States		unknown	unknown	false
187.205.15.107	unknown	Mexico		8151	UninetSAdeCVMX	false
73.158.5.250	unknown	United States		7922	COMCAST-7922US	false
124.46.93.136	unknown	Korea Republic of		4668	LGNET-AS-KRLGCNSKR	false
207.73.92.61	unknown	United States		237	MERIT-AS-14US	false
193.0.152.73	unknown	Russian Federation		198758	ASTELEKRU	false
158.22.228.197	unknown	United States		1504	DNIC-AS-01504US	false
185.204.137.224	unknown	Ireland		199256	LTH-ASIE	false
212.138.90.110	unknown	Saudi Arabia		8895	ISUInternetServicesUnitISUSA	false
38.116.126.9	unknown	United States		174	COGENT-174US	false
89.234.28.7	unknown	United Kingdom		15395	RACKSPACE-LONGB	false
175.235.81.175	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
198.185.241.102	unknown	United States		394612	UPMC-PHSUS	false
40.4.203.143	unknown	United States		4249	LILLY-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.255.36.239	unknown	United States		1970	TAMUS-NETUS	false
85.71.211.239	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
179.225.107.21	unknown	Brazil		26599	TELEFONICABRASILSABR	false
21.127.118.106	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
134.49.149.213	unknown	United States		23138	FIRST-STEPUS	false
194.89.26.187	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
37.0.114.158	unknown	Germany		10780	PURE-STORAGEUS	false
148.221.95.25	unknown	Mexico		8151	UninetSAdeCVMX	false
100.61.74.33	unknown	United States		701	UUNETUS	false
142.188.170.28	unknown	Canada		577	BACOMCA	false
207.194.51.58	unknown	Canada		852	ASN852CA	false
38.177.215.166	unknown	United States		174	COGENT-174US	false
57.41.27.141	unknown	Belgium		2686	ATGS-MMD-ASUS	false
197.89.53.21	unknown	South Africa		10474	OPTINETZA	false
158.20.103.146	unknown	United States		1482	DNIC-AS-01482US	false
60.239.176.88	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
88.119.98.42	unknown	Lithuania		8764	TELIA-LIETUVALT	false
79.133.33.157	unknown	Germany		203833	AT-FIRSTCOLOAustriaAT	false
81.186.24.135	unknown	Greece		8248	GR-EDUNETGR	false
215.177.131.37	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
144.90.147.91	unknown	United States		6652	PIMA-COLLEGEUS	false
92.221.125.208	unknown	Norway		29695	ALTIBOX_ASNorwayNO	false
122.3.67.242	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
82.190.169.163	unknown	Italy		3269	ASN-IBSNAZIT	false
36.220.67.2	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
180.219.174.220	unknown	Hong Kong		17924	SMARTONE-MB-AS-APSmarToneMobileCommunicationsLtdHK	false
129.76.65.112	unknown	United States		2902	WN-WY-ASUS	false
173.104.161.185	unknown	United States		1239	SPRINTLINKUS	false
12.244.58.105	unknown	United States		7018	ATT-INTERNET4US	false
178.135.97.139	unknown	Lebanon		42003	OGERONETOGEROTelecomLB	false
215.3.75.75	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
65.185.252.214	unknown	United States		16787	CHARTER-16787-DCUS	false
46.62.214.21	unknown	Iran (ISLAMIC Republic Of)		16322	PARSONLINETehran-IRANIR	false
22.240.106.198	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
12.12.27.70	unknown	United States		32328	ALASCOM-IP-MANAGED-NETWORKUS	false
186.116.34.231	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
158.211.143.99	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
12.138.17.22	unknown	United States		7018	ATT-INTERNET4US	false
89.110.32.213	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
119.250.63.90	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
186.52.142.205	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
222.90.52.105	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
221.141.199.204	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.47.235.205	unknown	Japan		5501	FRAUNHOFER-CLUSTER-BWResearchInstitutesspreadalloverGe	false
193.42.34.225	unknown	Germany		3221	EENET-ASEE	false
46.196.44.254	unknown	Turkey		47524	TURKSAT-ASTR	false
37.151.174.83	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
155.145.125.114	unknown	United Kingdom		1221	ASN-TELSTRATelstraCorporationLtdAU	false
49.252.15.30	unknown	Japan		37903	EMOBILEYmobileCorporationJP	false
99.29.22.148	unknown	United States		7018	ATT-INTERNET4US	false
141.132.77.8	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
186.216.174.221	unknown	Brazil		262753	VOCETELECOMUNICACOESLTDABR	false
153.242.20.149	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
182.96.202.150	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
209.50.30.196	unknown	United States		15108	ALLO-COMMUS	false
93.37.49.195	unknown	Italy		12874	FASTWEBIT	false
215.235.57.72	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
132.15.117.214	unknown	United States		409	AFCONC-BLOCK1-ASUS	false
165.95.81.150	unknown	United States		1970	TAMUS-NETUS	false
202.145.152.143	unknown	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
44.194.239.200	unknown	United States		14618	AMAZON-AESUS	false
203.42.234.208	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
202.212.151.129	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
52.151.73.99	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
144.26.145.231	unknown	United States		29848	WCUUS	false
1.235.239.80	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
81.235.23.99	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
198.109.38.100	unknown	United States		237	MERIT-AS-14US	false
125.148.154.29	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
215.179.148.91	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
8.45.209.183	unknown	United States		30453	PATRICK-SOLUTIONS-INCUS	false
38.98.109.142	unknown	United States		18698	IAC-NYC-AS01US	false
20.181.7.34	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
171.93.229.84	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
204.208.92.154	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
11.120.224.250	unknown	United States		27651	ENTELCHILESACL	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.zlEnOZ (deleted)

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.712211284941116
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	mips.nn.elf
File size:	135'112 bytes
MD5:	2145cb16a925a273d569c25257eb701a
SHA1:	821c929b723b9c69683f96b921132e0ff98ac9a1
SHA256:	beeeaa8013f74e611c30f4a99aebe4f5e38f3403a3d8314379428ab0a1ddd244
SHA512:	b40814b92ba58edd3cf9814877ba6a9a3538fb2e748b18d49e731b9f7459ff1f3ed47b25781b82df8f61e51288cfd956a0138e71f8aa75f3c9893a8676fd596c
SSDEEP:	3072:M1syNDJJX/gcGzGZsJs/3e+CjxshzgnnuKCXO:osyNDJJX/gclK2mxRC+
TLSH:	A2D3D71E6E318F6DF769C33947B78A20979837C627D0C685D27CE9211E6034E641FBA8
File Content Preview:	.ELF.....@.`...4.....4. ...(.....@...@.....E...E.....1(.....dt.Q.....<...'..L...!'.....<...'..(...!.. ....'9... ..... <...'.....!.....'9.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3

ELF header	
Section Header Offset:	134552
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

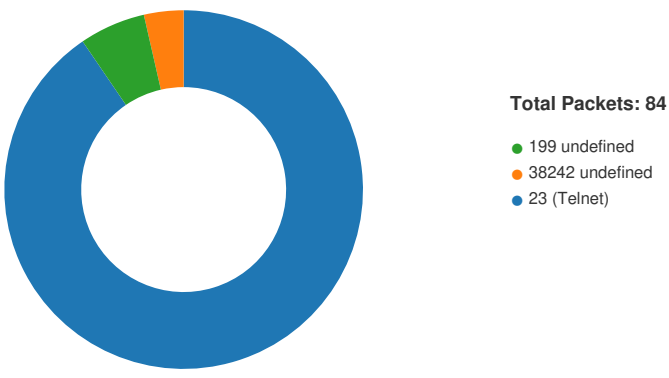
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x1cd00	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x41ce20	0x1ce20	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x41ce80	0x1ce80	0x3010	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x45fe94	0x1fe94	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x45fe9c	0x1fe9c	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x45fea8	0x1fea8	0x138	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x45ffe0	0x1ffe0	0x610	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4605f0	0x205f0	0x744	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x460d34	0x20d34	0x20	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x460d60	0x20d34	0x225c	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0xdec	0x20d34	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x20d34	0x64	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x1fe90	0x1fe90	5.7248	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1fe94	0x45fe94	0x45fe94	0xea0	0x3128	4.4252	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: mips.nn.elf PID: 5433, Parent PID: 5357

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/tmp/mips.nn.elf
Arguments:	/tmp/mips.nn.elf
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

- File Deleted
- File Read
- File Written
- Directory Enumerated
- Symbolic Link Created

Analysis Process: mips.nn.elf PID: 5456, Parent PID: 5433

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/tmp/mips.nn.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: mips.nn.elf PID: 5459, Parent PID: 5456

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/tmp/mips.nn.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: mips.nn.elf PID: 5461, Parent PID: 5456

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/tmp/mips.nn.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

- File Read
- Directory Enumerated

Analysis Process: mips.nn.elf PID: 5470, Parent PID: 5456

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/tmp/mips.nn.elf

Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

Directory Enumerated

Analysis Process: udisksd PID: **5443**, Parent PID: **802**

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **5443**, Parent PID: **802**

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
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: **5509**, Parent PID: **802**

General

Start time (UTC):	23:46:55
Start date (UTC):	14/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **5509**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
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: **5532**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-

File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **5532**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
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: **5533**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **5533**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
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: **5534**, Parent PID: **1588**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
Path:	/usr/libexec/gnome-session-binary
Arguments:	-
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: **5534**, Parent PID: **1588**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
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: **5534**, Parent PID: **1588**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
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: **5538**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
Path:	/usr/lib/udisks2/udisksd
Arguments:	-
File size:	483056 bytes
MD5 hash:	1d7ae439cc3d82fa6b127671ce037a24

Analysis Process: dumpe2fs PID: **5538**, Parent PID: **802**

General

Start time (UTC):	23:46:56
Start date (UTC):	14/12/2024
Path:	/usr/sbin/dumpe2fs
Arguments:	dumpe2fs -h /dev/dm-0
File size:	31112 bytes
MD5 hash:	5c66f7d8f7681a40562cf049ad4b72b4

File Activities

File Read