ID: 514677
Sample Name: HdZIgkO5be
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 14:34:03
Date: 03/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

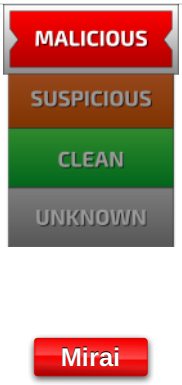
Linux Analysis Report HdZIgkO5be

Overview

General Information

Sample Name:	HdZIgkO5be
Analysis ID:	514677
MD5:	1b5dfd49454f3d7..
SHA1:	560ba6f16c235b2.
SHA256:	743ebdcaf8b0255.
Tags:	32 elf mirai renesas
Infos:	

Detection

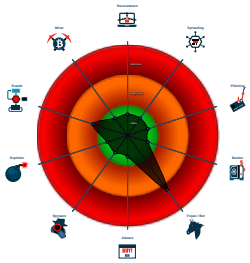


Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample has stripped symbol table
- Uses the "uname" system call to qu...
- Detected TCP or UDP traffic on non...
- Executes the "rm" command used to...
- Sample listens on a socket

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	514677
Start date:	03.11.2021
Start time:	14:34:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HdZIgkO5be
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:	mal64.troj.lin@0/1@0/0
Warnings:	Show All

Process Tree

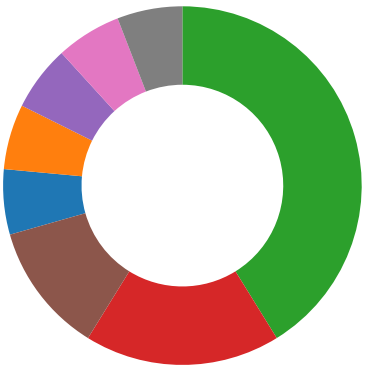
- **system is lnxubuntu20**
- HdZIgkO5be (PID: 5234, Parent: 5111, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/HdZIgkO5be
  - HdZIgkO5be New Fork (PID: 5237, Parent: 5234)
  - HdZIgkO5be New Fork (PID: 5238, Parent: 5234)
    - HdZIgkO5be New Fork (PID: 5241, Parent: 5238)
    - HdZIgkO5be New Fork (PID: 5242, Parent: 5238)
- dash New Fork (PID: 5257, Parent: 4335)
- cat (PID: 5257, Parent: 4335, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.H4Yec3gXhs
- dash New Fork (PID: 5258, Parent: 4335)
- head (PID: 5258, Parent: 4335, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5259, Parent: 4335)
- tr (PID: 5259, Parent: 4335, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5260, Parent: 4335)
- cut (PID: 5260, Parent: 4335, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5261, Parent: 4335)
- cat (PID: 5261, Parent: 4335, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.H4Yec3gXhs
- dash New Fork (PID: 5262, Parent: 4335)
- head (PID: 5262, Parent: 4335, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5263, Parent: 4335)
- tr (PID: 5263, Parent: 4335, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5264, Parent: 4335)
- cut (PID: 5264, Parent: 4335, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5265, Parent: 4335)
- rm (PID: 5265, Parent: 4335, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.H4Yec3gXhs /tmp/tmp.fjoJ0veOxV /tmp/tmp.nPTMpkeekC
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



AV Detection
Compliance
Networking
System Summary
Persistence and Installation Behavior
Malware Analysis System Evasion
Stealing of Sensitive Information
Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

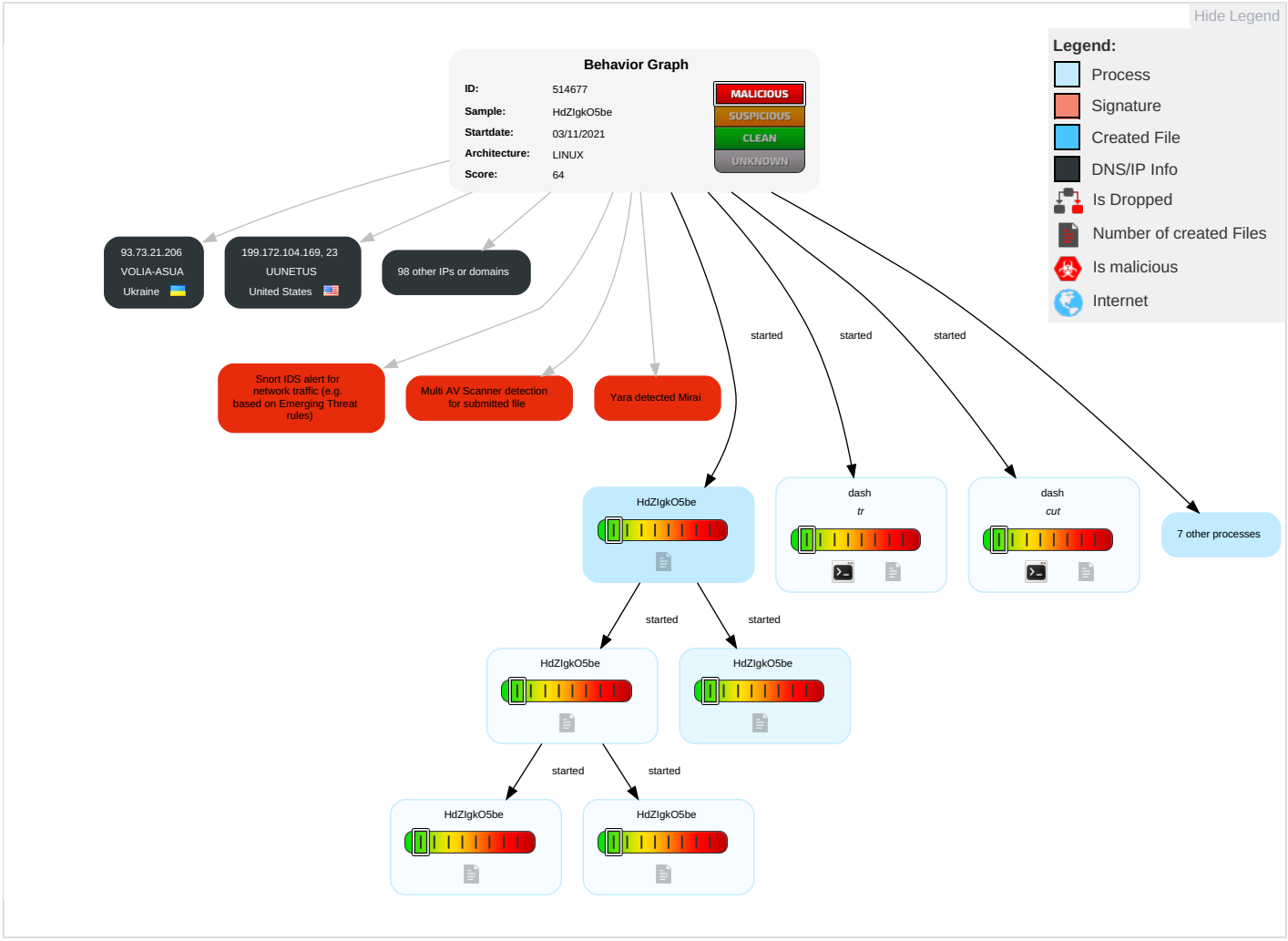
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	File Deletion 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HdZIgkO5be	51%	Virustotal		Browse
HdZIgkO5be	49%	ReversingLabs	Linux.Trojan.Mirai	

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

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.133.121.28	unknown	United States		1239	SPRINTLINKUS	false
110.4.132.88	unknown	Japan		4685	ASAHI-NETAsahiNetJP	false
192.20.120.87	unknown	United States		14153	EDGECAST-IRUS	false
13.163.22.158	unknown	United States		7018	ATT-INTERNET4US	false
48.76.175.244	unknown	United States		2686	ATGS-MMD-ASUS	false
64.155.235.85	unknown	United States		3356	LEVEL3US	false
206.141.247.32	unknown	United States		7132	SBIS-ASUS	false
42.128.68.101	unknown	China		4249	LILLY-ASUS	false
131.22.137.74	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
42.30.112.85	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
80.138.21.138	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
74.39.79.11	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
106.146.245.154	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
140.246.119.194	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
156.152.214.245	unknown	United States		71	HP-INTERNET-ASUS	false
45.220.66.178	unknown	Seychelles		22769	DDOSING-BGP-NETWORKUS	false
59.146.137.204	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
54.209.193.64	unknown	United States		14618	AMAZON-AESUS	false
57.75.159.6	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
139.34.57.100	unknown	United States		9905	LINKNET-ID-APLinknetASNID	false
88.39.187.28	unknown	Italy		3269	ASN-IBSNAZIT	false
109.49.71.237	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
178.201.60.193	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
98.55.87.226	unknown	United States		7922	COMCAST-7922US	false
108.163.174.131	unknown	Canada		32613	IWEB-ASCA	false
209.158.237.86	unknown	United States		701	UUNETUS	false
211.80.251.197	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
103.227.88.150	unknown	Hong Kong		134078	NETPLUZ-AS-APNETPLUZHOLDINGSPRIVATELIMITEDSG	false
80.247.97.154	unknown	Russian Federation		21365	INTELECA-ASRussiaBarnaulRU	false
97.211.140.133	unknown	United States		6167	CELLCO-PARTUS	false
37.2.172.136	unknown	Sweden		1257	TELE2EU	false
153.176.2.177	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
153.173.231.69	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
77.179.253.44	unknown	Germany		6805	TDDE-ASN1DE	false
206.24.109.11	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
192.227.172.222	unknown	United States		36352	AS-COLOCROSSINGUS	false
42.180.134.40	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
134.218.234.55	unknown	United States		22586	AS22586US	false
97.185.107.185	unknown	United States		6167	CELLCO-PARTUS	false
42.54.69.60	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
2.53.80.24	unknown	Israel		12400	PARTNER-ASIL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
17.125.181.191	unknown	United States		714	APPLE-ENGINEERINGUS	false
138.118.91.230	unknown	Brazil		262485	SCRIOTELECOMUNICACOESEINFORMATICALTDABR	false
96.43.47.102	unknown	United States		23404	RITTERNETUS	false
5.55.222.216	unknown	Greece		3329	HOL-GRAthensGreeceGR	false
12.139.76.108	unknown	United States		7018	ATT-INTERNET4US	false
66.40.171.253	unknown	Canada		13768	COGECO-PEER1CA	false
119.161.182.40	unknown	China		23724	CHINANET-IDC-BJ-APIDCChinaTelecommunicationsCorporation	false
45.53.108.14	unknown	United States		5650	FRONTIER-FRTRUS	false
121.165.152.110	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
139.34.113.220	unknown	United States		9905	LINKNET-ID-APLinknetASNID	false
40.151.134.6	unknown	United States		4249	LILLY-ASUS	false
2.53.79.49	unknown	Israel		12400	PARTNER-ASIL	false
25.94.196.216	unknown	United Kingdom		7922	COMCAST-7922US	false
51.110.38.67	unknown	United Kingdom		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
63.43.226.219	unknown	United States		22394	CELLCOUS	false
43.52.108.99	unknown	Japan		4249	LILLY-ASUS	false
154.235.180.205	unknown	Cote D'ivoire		36974	AFNET-ASCI	false
13.209.107.25	unknown	United States		16509	AMAZON-02US	false
27.221.202.131	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
176.202.208.137	unknown	Qatar		8781	QA-ISPQA	false
38.31.207.157	unknown	United States		174	COGENT-174US	false
134.158.112.54	unknown	France		789	IN2P3IN2P3AutonomousSystemEU	false
82.116.89.3	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
63.88.124.112	unknown	United States		701	UUNETUS	false
13.181.20.246	unknown	United States		7018	ATT-INTERNET4US	false
159.15.172.185	unknown	United Kingdom		8897	KCOM-SPNService-ProviderNetworkex-MistralGB	false
174.126.143.65	unknown	United States		11492	CABLEONEUS	false
61.38.180.140	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
204.216.163.145	unknown	United States		4544	CONXION-AUS	false
206.74.116.46	unknown	United States		12208	TRUVISTAUS	false
13.106.20.155	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
67.28.217.149	unknown	United States		202818	LEVEL3COMMUNICATIONSFR	false
123.143.60.52	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
93.73.21.206	unknown	Ukraine		25229	VOLIA-ASUA	false
67.219.84.252	unknown	United States		11492	CABLEONEUS	false
103.101.14.43	unknown	China		23734	NETROUTINGINC-AS-APNetroutingIncUS	false
52.233.156.230	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
34.60.165.23	unknown	United States		2686	ATGS-MMD-ASUS	false
138.7.41.118	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
113.236.231.12	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
88.125.199.114	unknown	France		12322	PROXADFR	false
117.35.190.95	unknown	China		4835	CHINANET-IDC-SNChinaTelecomGroupCN	false
87.198.85.91	unknown	Ireland		34245	MAGNET-ASIE	false
44.140.71.217	unknown	United States		1653	SUNETSUNETSwedishUniversityNetworkEU	false
195.231.25.126	unknown	Italy		202242	ARUBA-CLOUDIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
118.28.235.118	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
73.37.39.244	unknown	United States		7922	COMCAST-7922US	false
89.41.195.75	unknown	Iran (ISLAMIC Republic Of)		57218	RIGHTELIR	false
106.252.34.137	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
162.237.151.226	unknown	United States		7018	ATT-INTERNET4US	false
51.108.249.23	unknown	United Kingdom		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
168.11.100.139	unknown	United States		3480	PEACHNET-AS2US	false
199.172.104.169	unknown	United States		701	UUNETUS	false
46.63.231.119	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
120.99.177.30	unknown	Taiwan; Republic of China (ROC)		17716	NTU-TWNationalTaiwanUniversityTW	false
132.28.253.212	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
94.184.96.7	unknown	Iran (ISLAMIC Republic Of)		6736	IRANET-IPMInstituteforResearchinFundamentalSciencesI	false
44.25.148.202	unknown	United States		63479	HAMWANUS	false
76.15.160.88	unknown	United States		12271	TWC-12271-NYCUS	false

Runtime Messages

Command:	/tmp/HdZIgkO5be
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	JEW was here lol
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.179.253.44	4eB1luja0v	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASAHI-NETAsahiNetJP	x86-20211103-0152	Get hash	malicious	Browse	• 14.3.193.10
	Z7QqCH0bak	Get hash	malicious	Browse	• 157.107.185.94
	32UX3eB2m0	Get hash	malicious	Browse	• 118.243.197.144
	jJ6GK5qbZt	Get hash	malicious	Browse	• 219.121.22.130
	en94piXmL6	Get hash	malicious	Browse	• 118.243.197.109
	g22kPe2LIc	Get hash	malicious	Browse	• 210.253.240.200
	jvilYCvWBc	Get hash	malicious	Browse	• 14.3.144.55
	b3astmode.arm	Get hash	malicious	Browse	• 118.243.197.105
	x86	Get hash	malicious	Browse	• 157.107.79.209
	jpVQoYXUk7	Get hash	malicious	Browse	• 183.77.123.110
	UniRHdW5VC	Get hash	malicious	Browse	• 157.107.79.213

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VdhQknQq9e	Get hash	malicious	Browse	• 138.64.186.255
	o4wjsQMo7q	Get hash	malicious	Browse	• 118.243.14 9.203
	cvWFjfKtdH	Get hash	malicious	Browse	• 122.249.14 4.105
	SecuriteInfo.com.Linux.BackDoor.Fgt.1541.29094.31457	Get hash	malicious	Browse	• 14.3.193.20
	LsgCcJSqnz	Get hash	malicious	Browse	• 118.243.31.64
	sora.arm	Get hash	malicious	Browse	• 203.189.62.96
	eVtKZt4DLL	Get hash	malicious	Browse	• 111.234.20 5.167
	22693dBj8t	Get hash	malicious	Browse	• 14.3.120.82
	mirai.x86	Get hash	malicious	Browse	• 110.5.0.124
SPRINTLINKUS	cavEG2l8fj	Get hash	malicious	Browse	• 63.185.84.36
	arm-20211102-0937	Get hash	malicious	Browse	• 204.104.13 1.234
	arm5-20211102-0937	Get hash	malicious	Browse	• 63.178.243.141
	dUW6YG1Tdv	Get hash	malicious	Browse	• 63.175.225.90
	Ko84iLip1u	Get hash	malicious	Browse	• 65.173.0.172
	t7WU0JjLAR	Get hash	malicious	Browse	• 204.122.86.139
	FGVOkw9did	Get hash	malicious	Browse	• 204.180.4.59
	mxHkqAIYT0	Get hash	malicious	Browse	• 206.105.40.49
	swOGb2sZYt	Get hash	malicious	Browse	• 63.184.206.211
	V2WzER53Tt	Get hash	malicious	Browse	• 206.106.173.7
	a5nulABeSk	Get hash	malicious	Browse	• 63.178.243.137
	arm7	Get hash	malicious	Browse	• 173.107.83.131
	z0x3n.arm7	Get hash	malicious	Browse	• 173.148.20 6.146
	arm	Get hash	malicious	Browse	• 63.162.162.17
	QZ2CN6CUyv	Get hash	malicious	Browse	• 63.185.84.37
	Z7QqCH0bak	Get hash	malicious	Browse	• 144.243.45.220
	vEBWe85OY5	Get hash	malicious	Browse	• 63.162.162.61
	5mLAGfiGBf	Get hash	malicious	Browse	• 207.12.164.60
	x86_64	Get hash	malicious	Browse	• 63.177.253.255
	mdyu2wtnR8	Get hash	malicious	Browse	• 207.143.192.20

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/cache/motd-news	
Process:	/usr/bin/cut
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.515771857099866
Encrypted:	false
SSDEEP:	3:P2lnI+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn
MD5:	DD514F892B5F93ED615D366E58AC58AF
SHA1:	BA75EDB3C2232CC260BC187F604DC8F25AA72C11
SHA-256:	F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF
SHA-512:	9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACCDBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42A 2D0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	* Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation.

Static File Info

General

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.815905745089519
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	HdZIgkO5be
File size:	51924
MD5:	1b5dfd49454f3d7fe8e518f904c88bc7
SHA1:	560ba6f16c235b269669d8bb8c6367045e521617
SHA256:	743ebdcaf8b0255212578ac797f920df17daba5f8036fb2f6c942316a2524d22
SHA512:	9357c7595c8681f99a9821cd1de0451a06a9e4cae87343ab8a4766ec824d02063ae2b82af2257d2ac6b9838cd48499540c9d8df3e4c12593d1cb7bdf0b278b14
SSDEEP:	768:Er9Q6eGyC75erUUeOiwwtNp40ZdiWFyGoMuJLk3XCmlolN9aXCxw:EcdC753UlwtNFFyGoMD3X3qlGXCxw
File Content Preview:	.ELF.....*.....@.4...D.....4. ...(.....@...@.....A...A.(...<.....Q.td....././" O.n.....#.*@.....#.*@,....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	51524
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xbe40	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40bf20	0xbf20	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40bf44	0xbf44	0x794	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41c6dc	0xc6dc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41c6e4	0xc6e4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41c6f0	0xc6f0	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41c904	0xc904	0x314	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xc904	0x3e	0x0	0x0		0	0	1

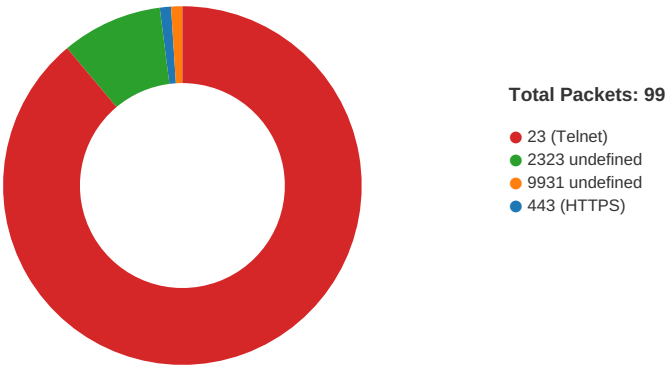
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0xc6d8	0xc6d8	4.7390	0x5	R E	0x10000		.init .text .fini .rodata

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0xc6dc	0x41c6dc	0x41c6dc	0x228	0x53c	1.5998	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: HdZIgkO5be PID: 5234 Parent PID: 5111

General

Start time:	14:34:48
Start date:	03/11/2021
Path:	/tmp/HdZIgkO5be
Arguments:	/tmp/HdZIgkO5be
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: HdZIgkO5be PID: 5237 Parent PID: 5234

General

Start time:	14:34:48
Start date:	03/11/2021
Path:	/tmp/HdZIgkO5be
Arguments:	n/a
File size:	4139976 bytes

MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: HdZIgkO5be PID: 5238 Parent PID: 5234

General

Start time:	14:34:48
Start date:	03/11/2021
Path:	/tmp/HdZIgkO5be
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: HdZIgkO5be PID: 5241 Parent PID: 5238

General

Start time:	14:34:48
Start date:	03/11/2021
Path:	/tmp/HdZIgkO5be
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: HdZIgkO5be PID: 5242 Parent PID: 5238

General

Start time:	14:34:48
Start date:	03/11/2021
Path:	/tmp/HdZIgkO5be
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: dash PID: 5257 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5257 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/cat

Arguments:	cat /tmp/tmp.H4Yec3gXhs
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5258 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5258 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5259 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5259 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5260 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5260 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5261 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5261 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.H4Yec3gXhs
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5262 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5262 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5263 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5263 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5264 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5264 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: dash PID: 5265 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5265 Parent PID: 4335

General

Start time:	14:35:11
Start date:	03/11/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.H4Yec3gXhs /tmp/tmp.fjoJ0veOxV /tmp/tmp.nPTMpkeekC
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read