ID: 679633
Sample Name: H9NSZqE1YV
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:40:13
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

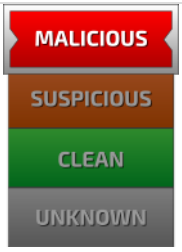
H9NSZqE1YV

Overview

General Information

Sample Name:	H9NSZqE1YV
Analysis ID:	679633
MD5:	58836131abfd48..
SHA1:	99834e69d8788d.
SHA256:	75197b35b16d26.
Tags:	32 elf mirai powerpc
Infos:	

Detection



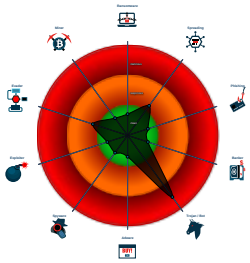
Mirai

Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on n…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket
- Sample tries to kill a process (SIGK…
- Sample contains strings indicative o…

Classification



Analysis Advice

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679633
Start date and time: 06/08/202207:40:13	2022-08-06 07:40:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	H9NSZqE1YV
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:	mal76.troj.lin@0/0@42/0

Warnings

Runtime Messages

Command:	/tmp/H9NSZqE1YV
PID:	6232
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- H9NSZqE1YV (PID: 6232, Parent: 6124, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/H9NSZqE1YV
  - H9NSZqE1YV New Fork (PID: 6234, Parent: 6232)
  - H9NSZqE1YV New Fork (PID: 6235, Parent: 6232)
  - H9NSZqE1YV New Fork (PID: 6237, Parent: 6232)
  - H9NSZqE1YV New Fork (PID: 6239, Parent: 6232)
    - H9NSZqE1YV New Fork (PID: 6242, Parent: 6239)
      - H9NSZqE1YV New Fork (PID: 6331, Parent: 6242)
    - H9NSZqE1YV New Fork (PID: 6244, Parent: 6239)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
H9NSZqE1YV	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
6232.1.00007fc154001000.00007fc154016000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6331.1.00007fc154001000.00007fc154016000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6244.1.00007fc154001000.00007fc154016000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

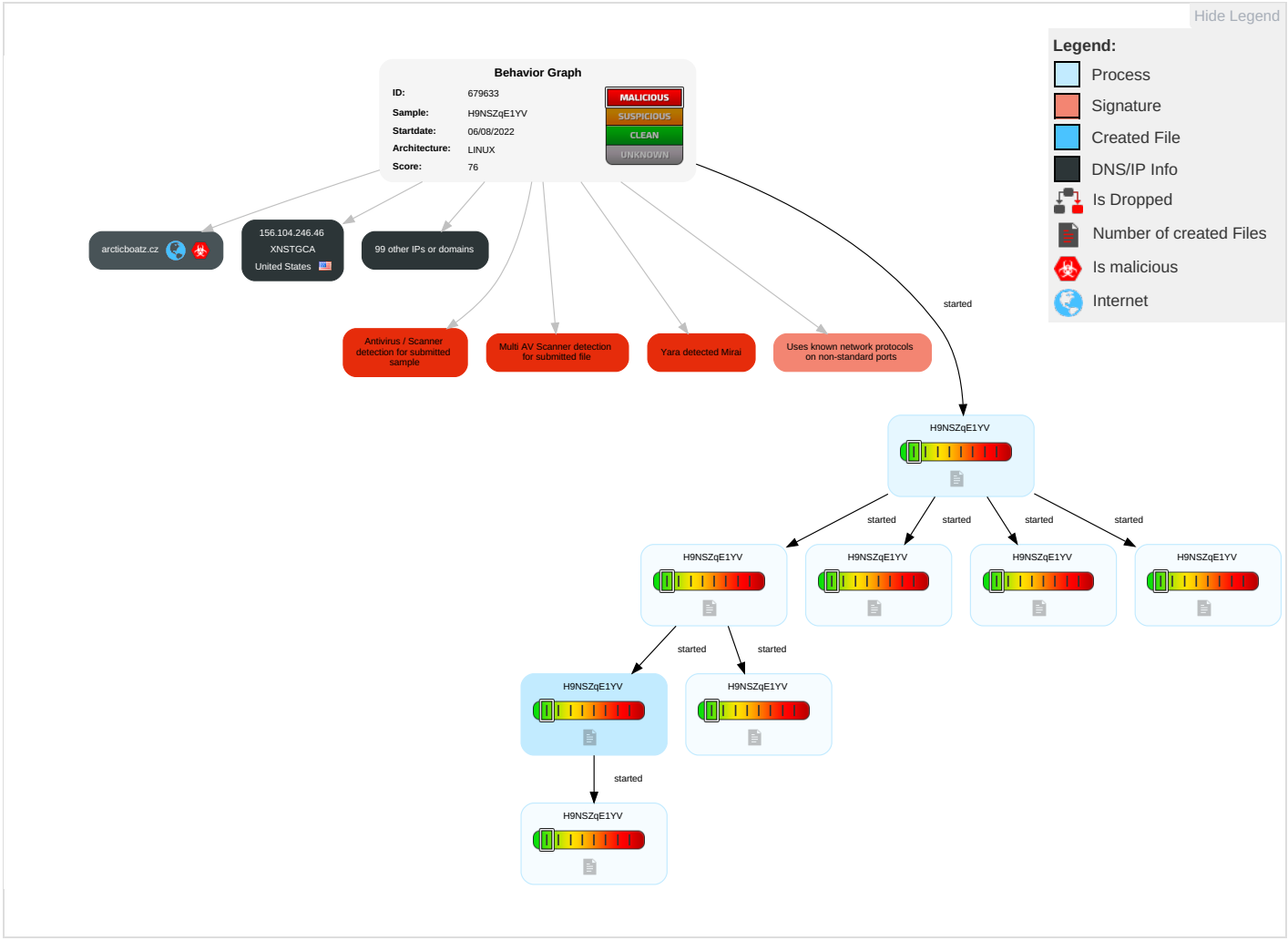
Mitre Att&ck Matrix

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	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	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	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
H9NSZqE1YV	50%	Virustotal		Browse
H9NSZqE1YV	31%	Metadefender		Browse
H9NSZqE1YV	62%	ReversingLabs	Linux.Trojan.Mirai	
H9NSZqE1YV	100%	Avira	LINUX/Mirai.ywooj	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
arcticboatz.cz	12%	Virustotal		Browse

URLs

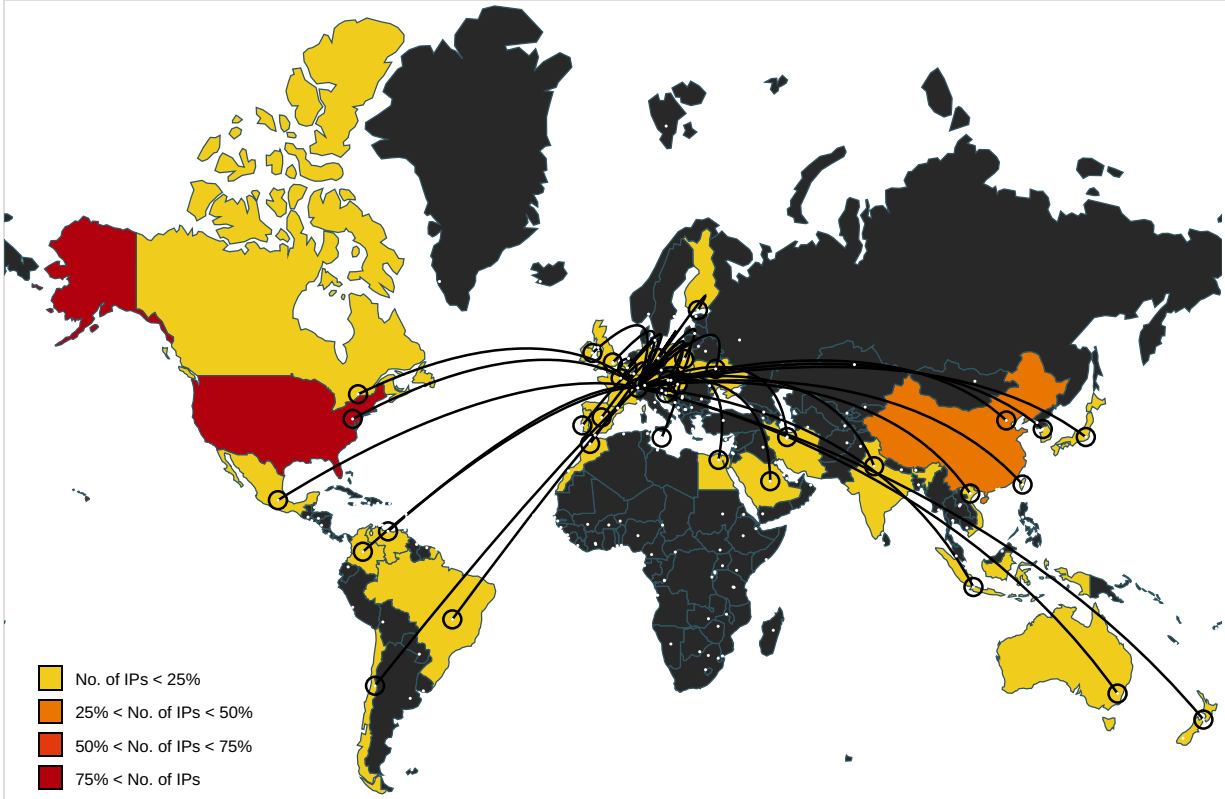
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
arcticboatz.cz	46.23.109.40	true	true	• 12%, Virustotal, Browse	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
155.109.221.154	unknown	United States		10273	FPLUS	false
181.135.48.207	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	false
14.165.112.96	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
220.110.11.185	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
118.48.135.48	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
223.89.203.166	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
85.156.76.78	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
152.173.70.221	unknown	Chile		7418	TELEFONICACHILESACL	false
218.158.128.63	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
62.201.85.237	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	false
17.62.173.148	unknown	United States		714	APPLE-ENGINEERINGUS	false
5.70.23.230	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
146.219.29.46	unknown	Spain		16153	SCS-ASES	false
247.47.97.152	unknown	Reserved		unknown	unknown	false
194.130.165.150	unknown	United Kingdom		702	UUNETUS	false
179.67.232.125	unknown	Brazil		7738	TelemarNorteLesteSABR	false
46.81.13.66	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
78.133.68.230	unknown	Malta		15735	DATASTREAM-NETMT	false
195.37.15.177	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
16.116.70.80	unknown	United States		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.213.34.200	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
156.104.246.46	unknown	United States		393504	XNSTGCA	false
241.154.209.12	unknown	Reserved		unknown	unknown	false
57.180.31.231	unknown	Belgium		2686	ATGS-MMD-ASUS	false
63.48.170.89	unknown	United States		701	UUNETUS	false
148.219.15.211	unknown	Mexico		8151	UninetSAdeCVMX	false
65.0.13.224	unknown	United States		16509	AMAZON-02US	false
190.143.63.123	unknown	Colombia		10620	TelmexColombiaSACO	false
19.247.181.236	unknown	United States		3	MIT-GATEWAYSUS	false
246.157.85.58	unknown	Reserved		unknown	unknown	false
116.118.24.28	unknown	Viet Nam		7602	SPT-AS-VNSaigonPostelCorporationVN	false
70.57.248.164	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
110.153.118.192	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
176.224.224.196	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
175.182.19.79	unknown	Taiwan; Republic of China (ROC)		4780	SEEDNETDigitalUnitedIncTW	false
78.123.223.255	unknown	France		8228	CEGETEL-ASFR	false
74.245.253.55	unknown	United States		7018	ATT-INTERNET4US	false
168.219.183.244	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
133.121.206.53	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
208.217.184.119	unknown	United States		701	UUNETUS	false
118.149.102.179	unknown	New Zealand		23655	SNAP-NZ-ASSnapInternetLimitedNZ	false
243.157.27.5	unknown	Reserved		unknown	unknown	false
115.247.124.226	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
70.53.130.250	unknown	Canada		577	BACOMCA	false
101.230.221.215	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
64.230.113.77	unknown	Canada		577	BACOMCA	false
54.120.7.252	unknown	United States		16509	AMAZON-02US	false
88.144.103.27	unknown	United Kingdom		12708	ONETEL-ASTalkTalkCommunicationsLimitedGB	false
202.147.239.4	unknown	Indonesia		18156	BITNET-ID-APBITNETISPASID	false
222.226.32.24	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
133.238.136.184	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
171.129.35.104	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
255.229.26.40	unknown	Reserved		unknown	unknown	false
111.160.230.225	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
252.233.82.244	unknown	Reserved		unknown	unknown	false
248.16.28.150	unknown	Reserved		unknown	unknown	false
59.44.8.235	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
158.54.95.144	unknown	Australia		11757	WHIRLPOOL-ASNUS	false
132.1.35.245	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
5.112.38.239	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
146.0.120.110	unknown	Germany		16097	HLKOMM04107LeipzigDE	false
246.229.188.175	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.58.199.215	unknown	Austria		199083	MP-ASAT	false
255.96.63.163	unknown	Reserved		unknown	unknown	false
76.221.46.250	unknown	United States		7018	ATT-INTERNET4US	false
177.10.52.215	unknown	Brazil		53232	BannerServicosdeTelecomeInternetLtdaBR	false
169.178.222.46	unknown	United States		37611	AfrihostZA	false
109.129.79.187	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
83.13.177.41	unknown	Poland		5617	TPNETPL	false
253.113.190.193	unknown	Reserved		unknown	unknown	false
40.132.109.158	unknown	United States		7029	WINDSTREAMUS	false
146.39.178.162	unknown	United States		197938	TRAVIANGAMESDE	false
184.38.86.27	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
99.223.182.92	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
41.179.108.50	unknown	Egypt		24863	LINKdotNET-ASEG	false
62.135.4.212	unknown	Egypt		24863	LINKdotNET-ASEG	false
249.239.255.162	unknown	Reserved		unknown	unknown	false
179.228.187.230	unknown	Brazil		27699	TELEFONICABRASILSABR	false
85.134.195.246	unknown	Ireland		24751	MULTIFI-ASFI	false
190.207.250.245	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
182.116.28.224	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
251.134.38.124	unknown	Reserved		unknown	unknown	false
9.254.40.126	unknown	United States		3356	LEVEL3US	false
120.195.48.62	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
124.182.10.211	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
93.140.61.197	unknown	Croatia (LOCAL Name: Hrvatska)		5391	T-HTCroatianTelecomIncHR	false
173.5.70.42	unknown	United States		10507	SPCSUS	false
86.172.120.247	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
197.129.211.25	unknown	Morocco		6713	IAM-ASMA	false
46.153.18.240	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
61.210.62.8	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
85.244.28.223	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
152.237.114.197	unknown	Brazil		7738	TelemarNorteLesteSABR	false
251.172.40.214	unknown	Reserved		unknown	unknown	false
205.201.209.63	unknown	United States		6653	FORETHOUGHTNETUS	false
68.254.240.31	unknown	United States		7018	ATT-INTERNET4US	false
77.121.20.57	unknown	Ukraine		25229	VOLIA-ASUA	false
240.5.72.95	unknown	Reserved		unknown	unknown	false
184.225.78.253	unknown	United States		10507	SPCSUS	false
147.202.174.64	unknown	United States		19149	TEAMTECH-DSMUS	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

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.326713846296607
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	H9NSZqE1YV
File size:	87104
MD5:	58836131abfd4884cee3a45e82344236
SHA1:	99834e69d8788d276f63ee5968256cb84d3dc1c4
SHA256:	75197b35b16d2668bf3c9437ac9e29f2287db5b1f0839acc4f6dbcf7bca02ae2
SHA512:	1be5bcee9ef566a1300adf0e16d464dfd605ce09dc05a828733477c01370d8c261ef9beaffec24ba270cd68bba8f1cbb47c564fb50701a337d2e1bf45ad2f012
SSDEEP:	1536:npY0t1K/BFgpPidJ+bWxGcRy1A8dF67dGhY8CpSw5NJYPpo:oBFaPidI58mFtYZSubgpo
TLSH:	CC835C02B318094BF5E61DF0393F1BE193AFE98020F0B6C9690EE7499276E725546FD9
File Content Preview:	.ELF.....4..R`.....4. ...(.....J...J.....J...J...J.....3 .....dt.Q.....!..|.....$H...H.(5...$8!. |...N.. .!..|.....?.....R...../...@..\?.....K..+../...A..$8...})....K.N..

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x100001f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	86624

ELF header

Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

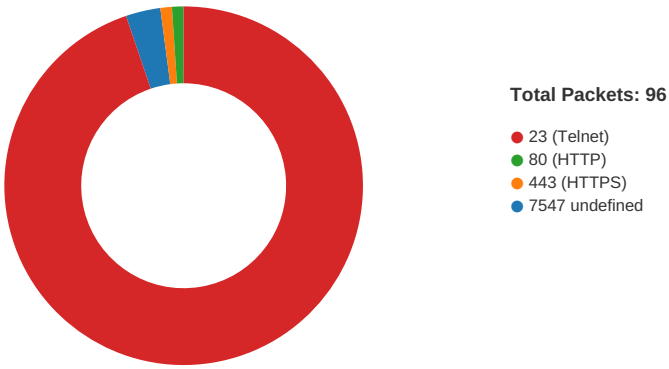
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0x1288c	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x10012944	0x12944	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x10012968	0x12968	0x2190	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x10024afc	0x14afc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x10024b04	0x14b04	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x10024b10	0x14b10	0x6b8	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x100251c8	0x151c8	0x4c	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x10025214	0x15214	0x90	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x100252a4	0x15214	0x2b78	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x15214	0x4b	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	0x10000000	0x10000000	0x14af8	0x14af8	6.3516	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x14afc	0x10024afc	0x10024afc	0x718	0x3320	4.4934	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 07:41:01.116614103 CEST	192.168.2.23	8.8.8.8	0xdb08	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:09.165544033 CEST	192.168.2.23	8.8.8.8	0xbb1e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 07:41:12.213207960 CEST	192.168.2.23	8.8.8.8	0xe192	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:21.259176970 CEST	192.168.2.23	8.8.8.8	0x770f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:25.307424068 CEST	192.168.2.23	8.8.8.8	0xf37b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:32.422629118 CEST	192.168.2.23	8.8.8.8	0x5c25	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:41.507055998 CEST	192.168.2.23	8.8.8.8	0xc3eb	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:50.554505110 CEST	192.168.2.23	8.8.8.8	0xe50d	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:52.602288961 CEST	192.168.2.23	8.8.8.8	0xdb3f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:01.654665947 CEST	192.168.2.23	8.8.8.8	0x3446	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:09.704438925 CEST	192.168.2.23	8.8.8.8	0xacc5	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:11.751385927 CEST	192.168.2.23	8.8.8.8	0x38cd	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:17.802405119 CEST	192.168.2.23	8.8.8.8	0x8340	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:20.852332115 CEST	192.168.2.23	8.8.8.8	0xc617	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:28.902182102 CEST	192.168.2.23	8.8.8.8	0xc2a8	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:33.952630997 CEST	192.168.2.23	8.8.8.8	0x2d8b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:41.004432917 CEST	192.168.2.23	8.8.8.8	0x6751	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:47.074788094 CEST	192.168.2.23	8.8.8.8	0x4c77	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:56.123281002 CEST	192.168.2.23	8.8.8.8	0xe9cb	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:04.171331882 CEST	192.168.2.23	8.8.8.8	0x8817	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:11.220374107 CEST	192.168.2.23	8.8.8.8	0x72c2	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:12.270960093 CEST	192.168.2.23	8.8.8.8	0xf4e5	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:22.319828987 CEST	192.168.2.23	8.8.8.8	0xa83d	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:26.370374918 CEST	192.168.2.23	8.8.8.8	0xb9ae	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:36.420439959 CEST	192.168.2.23	8.8.8.8	0x9b73	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:42.501266003 CEST	192.168.2.23	8.8.8.8	0xfffa	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:48.786597013 CEST	192.168.2.23	8.8.8.8	0xdb08	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:51.552239895 CEST	192.168.2.23	8.8.8.8	0xc97a	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:54.600958109 CEST	192.168.2.23	8.8.8.8	0x91c0	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:56.834305048 CEST	192.168.2.23	8.8.8.8	0xbb1e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:59.882426023 CEST	192.168.2.23	8.8.8.8	0xe192	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:03.662785053 CEST	192.168.2.23	8.8.8.8	0xbc06	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:04.711616039 CEST	192.168.2.23	8.8.8.8	0xabc1	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:08.928091049 CEST	192.168.2.23	8.8.8.8	0x770f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:13.022116899 CEST	192.168.2.23	8.8.8.8	0xf37b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:14.806247950 CEST	192.168.2.23	8.8.8.8	0xd163	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:15.852396965 CEST	192.168.2.23	8.8.8.8	0x4dfc	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 07:44:17.901329041 CEST	192.168.2.23	8.8.8.8	0x4e79	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:20.114877939 CEST	192.168.2.23	8.8.8.8	0x5c25	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:27.949146986 CEST	192.168.2.23	8.8.8.8	0xb943	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:28.997534037 CEST	192.168.2.23	8.8.8.8	0xee1b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:29.172676086 CEST	192.168.2.23	8.8.8.8	0xc3eb	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 07:41:01.135778904 CEST	8.8.8.8	192.168.2.23	0xdb08	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:09.183168888 CEST	8.8.8.8	192.168.2.23	0xbb1e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:12.230926037 CEST	8.8.8.8	192.168.2.23	0xe192	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:21.278891087 CEST	8.8.8.8	192.168.2.23	0x770f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:25.325009108 CEST	8.8.8.8	192.168.2.23	0xf37b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:32.442219019 CEST	8.8.8.8	192.168.2.23	0x5c25	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:41.524699926 CEST	8.8.8.8	192.168.2.23	0xc3eb	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:50.571964979 CEST	8.8.8.8	192.168.2.23	0xe50d	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:41:52.621741056 CEST	8.8.8.8	192.168.2.23	0xdb3f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:01.674204111 CEST	8.8.8.8	192.168.2.23	0x3446	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:09.722086906 CEST	8.8.8.8	192.168.2.23	0xacc5	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:11.770395041 CEST	8.8.8.8	192.168.2.23	0x38cd	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:17.821860075 CEST	8.8.8.8	192.168.2.23	0x8340	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:20.871762037 CEST	8.8.8.8	192.168.2.23	0xc617	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:28.921660900 CEST	8.8.8.8	192.168.2.23	0xc2a8	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:33.972543001 CEST	8.8.8.8	192.168.2.23	0x2d8b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:41.024063110 CEST	8.8.8.8	192.168.2.23	0x6751	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:47.094512939 CEST	8.8.8.8	192.168.2.23	0x4c77	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:42:56.140731096 CEST	8.8.8.8	192.168.2.23	0xe9cb	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:04.190247059 CEST	8.8.8.8	192.168.2.23	0x8817	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:11.240196943 CEST	8.8.8.8	192.168.2.23	0x72c2	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:12.290678978 CEST	8.8.8.8	192.168.2.23	0xf4e5	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:22.339315891 CEST	8.8.8.8	192.168.2.23	0xa83d	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:26.389827967 CEST	8.8.8.8	192.168.2.23	0xb9ae	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:36.472057104 CEST	8.8.8.8	192.168.2.23	0x9b73	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:42.520622969 CEST	8.8.8.8	192.168.2.23	0xfffa	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:48.804306030 CEST	8.8.8.8	192.168.2.23	0xdb08	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:51.571899891 CEST	8.8.8.8	192.168.2.23	0xc97a	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 07:43:54.620553970 CEST	8.8.8.8	192.168.2.23	0x91c0	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:56.853245020 CEST	8.8.8.8	192.168.2.23	0xbb1e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:43:59.899748087 CEST	8.8.8.8	192.168.2.23	0xe192	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:03.682626963 CEST	8.8.8.8	192.168.2.23	0xbc06	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:04.731012106 CEST	8.8.8.8	192.168.2.23	0xabc1	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:08.947515965 CEST	8.8.8.8	192.168.2.23	0x770f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:13.041237116 CEST	8.8.8.8	192.168.2.23	0xf37b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:14.823204994 CEST	8.8.8.8	192.168.2.23	0xd163	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:15.871874094 CEST	8.8.8.8	192.168.2.23	0x4dfc	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:17.920802116 CEST	8.8.8.8	192.168.2.23	0x4e79	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:20.132091045 CEST	8.8.8.8	192.168.2.23	0x5c25	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:27.968497038 CEST	8.8.8.8	192.168.2.23	0xb943	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:29.015249014 CEST	8.8.8.8	192.168.2.23	0xee1b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:44:29.192786932 CEST	8.8.8.8	192.168.2.23	0xc3eb	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: H9NSZqE1YV PID: **6232**, Parent PID: **6124**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	/tmp/H9NSZqE1YV
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: H9NSZqE1YV PID: **6234**, Parent PID: **6232**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: H9NSZqE1YV PID: **6235**, Parent PID: **6232**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a

File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: H9NSZqE1YV PID: **6237**, Parent PID: **6232**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: H9NSZqE1YV PID: **6239**, Parent PID: **6232**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: H9NSZqE1YV PID: **6242**, Parent PID: **6239**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: H9NSZqE1YV PID: **6331**, Parent PID: **6242**

General

Start time:	07:43:48
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: H9NSZqE1YV PID: **6244**, Parent PID: **6239**

General

Start time:	07:41:00
Start date:	06/08/2022
Path:	/tmp/H9NSZqE1YV
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6