ID: 679622
Sample Name: BWfKcndJCz
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 06:56:04
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

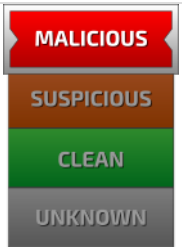
BWfKcndJCz

Overview

General Information

Sample Name:	BWfKcndJCz
Analysis ID:	679622
MD5:	00e2f1330f45468.
SHA1:	00562d888ec7a8..
SHA256:	febec5c5c4719c…
Tags:	32 elf mirai renesas
Infos:	

Detection



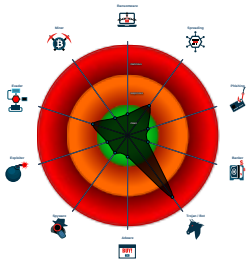
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- 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…
- Tries to connect to HTTP servers, b…
- 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.

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

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679622
Start date and time: 06/08/202206:56:04	2022-08-06 06:56:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BWfKcndJCz
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:	mal68.troj.lin@0/0@54/0

Warnings

Runtime Messages

Command:	/tmp/BWfKcndJCz
PID:	6270
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- BWfKcndJCz (PID: 6270, Parent: 6124, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/BWfKcndJCz
  - BWfKcndJCz New Fork (PID: 6272, Parent: 6270)
  - BWfKcndJCz New Fork (PID: 6273, Parent: 6270)
  - BWfKcndJCz New Fork (PID: 6275, Parent: 6270)
  - BWfKcndJCz New Fork (PID: 6277, Parent: 6270)
    - BWfKcndJCz New Fork (PID: 6281, Parent: 6277)
      - BWfKcndJCz New Fork (PID: 6368, Parent: 6281)
    - BWfKcndJCz New Fork (PID: 6282, Parent: 6277)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
BWfKcndJCz	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
6368.1.00007f2810400000.00007f2810414000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6282.1.00007f2810400000.00007f2810414000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6270.1.00007f2810400000.00007f2810414000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

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

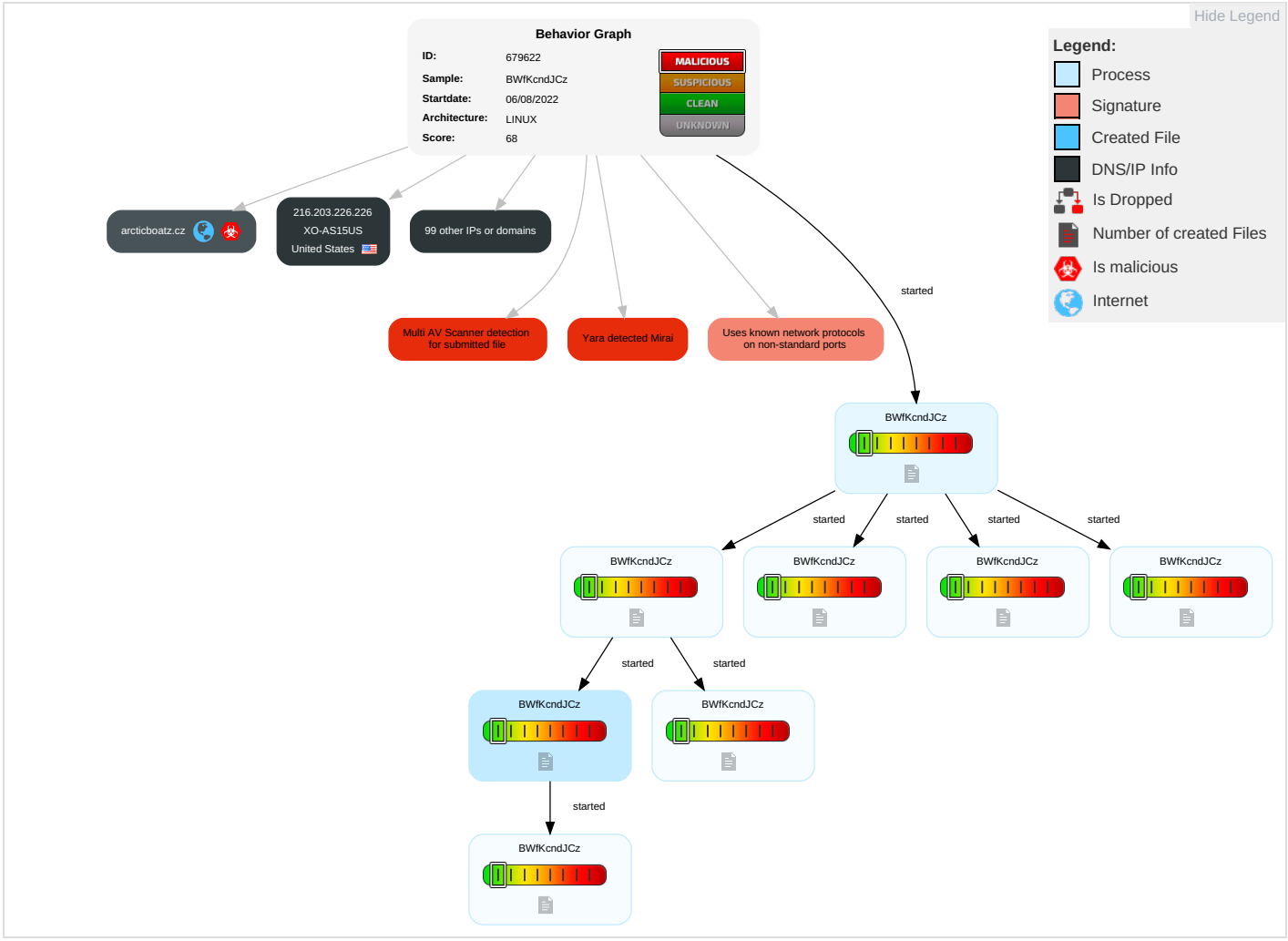
Mitre Att&ck Matrix

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
BWfKcndJCz	41%	Virustotal		Browse
BWfKcndJCz	40%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

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

URLs

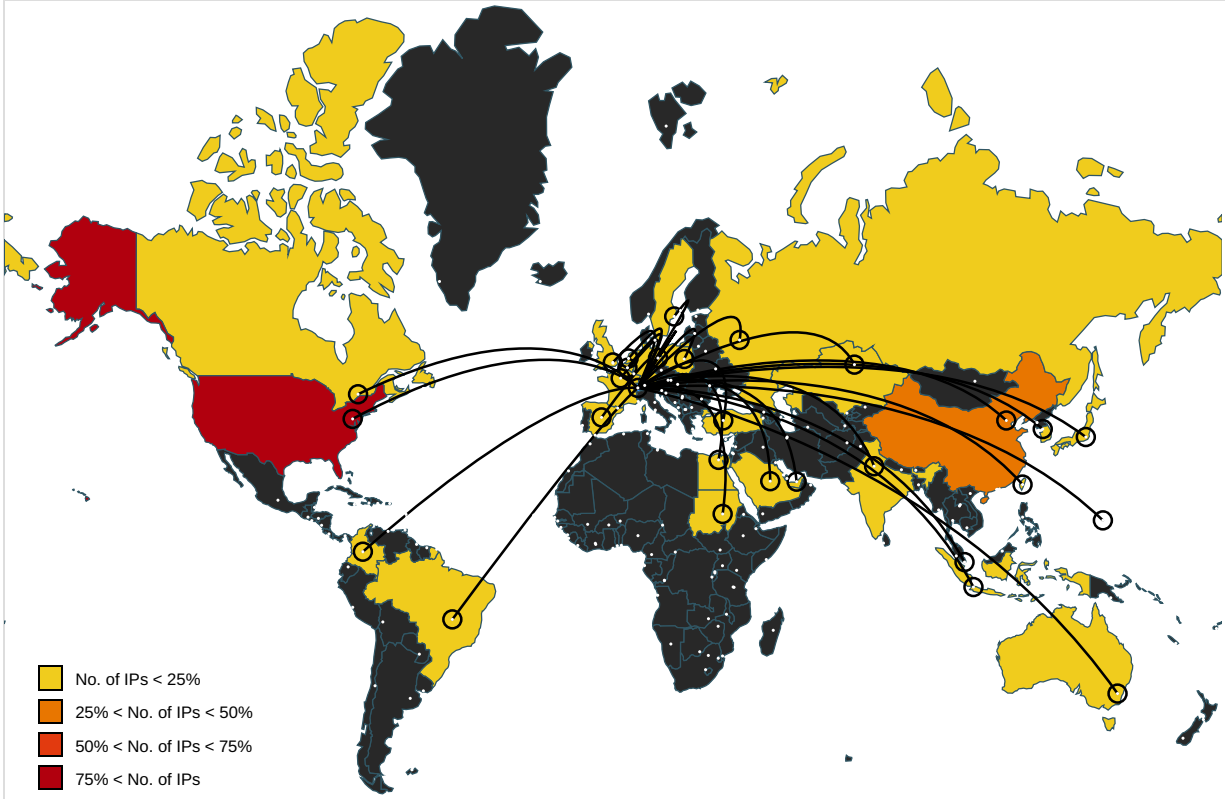
No Antivirus matches

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
126.10.188.201	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
191.134.140.164	unknown	Brazil		26615	TIMSABR	false
168.185.112.82	unknown	United States		2386	INS-ASUS	false
116.169.60.178	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
186.181.146.219	unknown	Colombia		27831	ColombiaMovilCO	false
157.203.50.1	unknown	United Kingdom		21369	SEMA-UK-ASGB	false
222.80.178.18	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
73.253.134.102	unknown	United States		7922	COMCAST-7922US	false
42.79.216.60	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
176.16.193.37	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
77.23.0.57	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
181.154.149.91	unknown	Colombia		26611	COMCELSACO	false
113.42.126.196	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
27.175.240.67	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
87.208.121.118	unknown	Netherlands		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
199.96.158.138	unknown	United States		22062	GEOSTARUS	false
121.86.7.47	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
155.121.107.248	unknown	United States		11003	PANDGUS	false
136.119.6.47	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
114.201.214.133	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
250.16.193.230	unknown	Reserved		unknown	unknown	false
164.213.14.108	unknown	United States		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
222.144.23.95	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
163.181.147.225	unknown	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
252.47.3.232	unknown	Reserved		unknown	unknown	false
5.107.206.60	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
94.254.235.80	unknown	Poland		39603	P4NETP4UMTSoperatorinPolandPL	false
155.48.25.197	unknown	United States		16481	BABSON-GNETUS	false
145.85.43.211	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
96.170.253.129	unknown	United States		7922	COMCAST-7922US	false
218.167.76.255	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
24.85.18.231	unknown	Canada		6327	SHAWCA	false
20.34.247.98	unknown	United States		8070	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
4.177.46.104	unknown	United States		3356	LEVEL3US	false
8.187.66.174	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
158.128.175.63	unknown	Canada		721	DNIC-ASBLK-00721-00726US	false
66.33.146.154	unknown	United States		7270	NET2PHONEUS	false
8.128.253.249	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
202.128.70.152	unknown	Guam		3605	ERX-KUENTOS-ASGuamCablevisionLLCGU	false
39.240.223.214	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
245.70.135.90	unknown	Reserved		unknown	unknown	false
110.76.113.93	unknown	Korea Republic of		7622	ASN-KAIST-SALKoreaAdvancedInstituteofScienceandTechno	false
248.241.213.22	unknown	Reserved		unknown	unknown	false
191.8.139.153	unknown	Brazil		27699	TELEFONICABRASILSABR	false
68.177.52.155	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
166.212.225.201	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
65.90.237.12	unknown	United States		3356	LEVEL3US	false
163.98.17.196	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
112.36.133.70	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
171.57.98.160	unknown	India		9874	STARHUB-MOBILEStarHubLtdSG	false
12.4.247.94	unknown	United States		7018	ATT-INTERNET4US	false
65.154.209.218	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
216.44.168.165	unknown	United States		22691	ISPNET-1US	false
40.225.230.46	unknown	United States		4249	LILLY-ASUS	false
113.6.156.29	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
18.50.108.142	unknown	United States		3	MIT-GATEWAYSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
249.178.22.21	unknown	Reserved		unknown	unknown	false
53.252.78.216	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
74.97.179.131	unknown	United States		701	UUNETUS	false
114.199.124.33	unknown	Indonesia		24525	SAP-AS-IDPTSolusiAksesindoPratamaID	false
20.65.181.143	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
187.75.183.70	unknown	Brazil		27699	TELEFONICABRASILSABR	false
112.27.106.149	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
2.78.125.73	unknown	Kazakhstan		29355	KCELL-ASKZ	false
245.183.87.51	unknown	Reserved		unknown	unknown	false
37.132.200.12	unknown	Spain		12479	UNI2-ASES	false
181.156.78.251	unknown	Colombia		26611	COMCELSACO	false
252.168.83.157	unknown	Reserved		unknown	unknown	false
122.195.233.191	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
255.220.26.136	unknown	Reserved		unknown	unknown	false
105.200.15.254	unknown	Egypt		36992	ETISALAT-MISREG	false
197.251.97.122	unknown	Sudan		37197	SUDRENSD	false
104.244.106.21	unknown	United States		4922	SHENTELUS	false
46.221.241.210	unknown	Turkey		15897	VODAFONETURKEYTR	false
106.82.15.179	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
39.149.103.74	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
207.206.52.98	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
94.121.41.190	unknown	Turkey		12978	DOGAN-ONLINETR	false
71.52.220.24	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
216.203.226.226	unknown	United States		2828	XO-AS15US	false
243.64.140.165	unknown	Reserved		unknown	unknown	false
125.197.52.84	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
169.81.211.206	unknown	United States		37611	AfrihostZA	false
87.255.170.252	unknown	Sweden		206114	HOFORSSE	false
121.217.223.251	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
86.15.30.45	unknown	United Kingdom		5089	NTLGB	false
198.134.219.204	unknown	Canada		393348	SUC-CORP1US	false
102.22.168.62	unknown	unknown		36924	GVA-CanalboxBJ	false
81.246.236.121	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
70.230.219.202	unknown	United States		7018	ATT-INTERNET4US	false
5.227.152.67	unknown	Russian Federation		8580	SANDYNizhnyNovgorodRussiaRU	false
146.217.84.168	unknown	United States		20478	GENMILLSUS	false
133.137.4.39	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
135.94.207.158	unknown	United States		29705	MOTIVE-COMMUNICATIONS-INCORPORATEDUS	false
101.16.254.242	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
217.187.39.197	unknown	Germany		6805	TDDE-ASN1DE	false
112.37.66.61	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
158.103.37.247	unknown	United States		33170	MORGAN-STATE-UNIVERSITYUS	false
163.84.28.196	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
81.6.84.77	unknown	Turkey		15897	VODAFONETURKEYTR	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 LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.835569254032797
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	BWfKcndJCz
File size:	83284
MD5:	00e2f1330f45468f78497ea8c73e0b3d
SHA1:	00562d888ec7a88f8023e8252aef1480234e7c06
SHA256:	febec5c5c4719ca23ad04e2f1b7ffe76b81035d5dd79d0eb1f61d9917886e022
SHA512:	36cb2b8f8078552a5601484acb176ec6854eafeb1b4b8df43619562944e11a38115e4d2aaf58af3686f7e2c994c142545f5133ad6a42139804f796e618989e52
SSDEEP:	1536:IF9a26mwt/KNb9REbQObIPs3NPXoKA/qUp8KJ8yK6BeCqJvf3JYoU/:IF9OmpNcbWP+NPoppjJtBeHf5XU/
TLSH:	D883BFB5C099ADA8C1484AB4BDA58F349313A90485A73EF6E794C35D940BEFDF6093F0
File Content Preview:	.ELF.....*.....@.4....C.....4. ...(.....@...@.p<..p<.....t<..t<B.t<B..... 3.....Q.td...../../"O.n.....#.*@.....#.*@L....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:	82884
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	0x11a60	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x411b40	0x11b40	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x411b64	0x11b64	0x210c	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x423c74	0x13c74	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x423c7c	0x13c7c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x423c88	0x13c88	0x6fc	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x424384	0x14384	0x2c10	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x14384	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	0x13c70	0x13c70	6.8757	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x13c74	0x423c74	0x423c74	0x710	0x3320	4.4046	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 06:56:50.035624027 CEST	192.168.2.23	8.8.8.8	0xf146	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:56:57.084233999 CEST	192.168.2.23	8.8.8.8	0xdd64	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:56:58.132563114 CEST	192.168.2.23	8.8.8.8	0x9804	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:02.187666893 CEST	192.168.2.23	8.8.8.8	0x8be8	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:07.234935045 CEST	192.168.2.23	8.8.8.8	0x431f	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 06:57:14.354414940 CEST	192.168.2.23	8.8.8.8	0x1113	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:15.402242899 CEST	192.168.2.23	8.8.8.8	0x7c9f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:17.449896097 CEST	192.168.2.23	8.8.8.8	0x63f0	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:20.496587992 CEST	192.168.2.23	8.8.8.8	0xc8ce	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:29.579412937 CEST	192.168.2.23	8.8.8.8	0xe1f2	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:30.639404058 CEST	192.168.2.23	8.8.8.8	0x2212	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:31.685211897 CEST	192.168.2.23	8.8.8.8	0x59b6	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:36.734404087 CEST	192.168.2.23	8.8.8.8	0xca8e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:39.782919884 CEST	192.168.2.23	8.8.8.8	0x1254	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:43.829257011 CEST	192.168.2.23	8.8.8.8	0x8f07	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:50.877547026 CEST	192.168.2.23	8.8.8.8	0xce8b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:56.963840961 CEST	192.168.2.23	8.8.8.8	0x3ad4	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:59.011733055 CEST	192.168.2.23	8.8.8.8	0x10b5	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:08.060539007 CEST	192.168.2.23	8.8.8.8	0x784f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:18.121064901 CEST	192.168.2.23	8.8.8.8	0x5b45	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:24.170289040 CEST	192.168.2.23	8.8.8.8	0x8e38	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:32.217387915 CEST	192.168.2.23	8.8.8.8	0x4ed6	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:39.265671015 CEST	192.168.2.23	8.8.8.8	0x51e9	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:45.311171055 CEST	192.168.2.23	8.8.8.8	0xe41b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:50.361099958 CEST	192.168.2.23	8.8.8.8	0x3e43	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:58.410478115 CEST	192.168.2.23	8.8.8.8	0xc396	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:02.457345009 CEST	192.168.2.23	8.8.8.8	0x54dc	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:03.506371021 CEST	192.168.2.23	8.8.8.8	0x182d	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:09.588334084 CEST	192.168.2.23	8.8.8.8	0x1ae8	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:10.634160042 CEST	192.168.2.23	8.8.8.8	0x5de8	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:12.701220036 CEST	192.168.2.23	8.8.8.8	0x83d3	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:19.747852087 CEST	192.168.2.23	8.8.8.8	0x2e36	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:21.797305107 CEST	192.168.2.23	8.8.8.8	0x16b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:30.845122099 CEST	192.168.2.23	8.8.8.8	0x9567	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:38.923134089 CEST	192.168.2.23	8.8.8.8	0xf027	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:39.379580975 CEST	192.168.2.23	8.8.8.8	0xf146	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:44.978177071 CEST	192.168.2.23	8.8.8.8	0x306a	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.427736044 CEST	192.168.2.23	8.8.8.8	0xdd64	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:47.476125002 CEST	192.168.2.23	8.8.8.8	0x9804	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:51.027462006 CEST	192.168.2.23	8.8.8.8	0x7c7	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 06:59:51.521742105 CEST	192.168.2.23	8.8.8.8	0x8be8	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:55.075078011 CEST	192.168.2.23	8.8.8.8	0xdb08	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:56.571420908 CEST	192.168.2.23	8.8.8.8	0x431f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:00.122791052 CEST	192.168.2.23	8.8.8.8	0xadd3	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:03.619024038 CEST	192.168.2.23	8.8.8.8	0x1113	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:04.664781094 CEST	192.168.2.23	8.8.8.8	0x7c9f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:06.173247099 CEST	192.168.2.23	8.8.8.8	0xaf08	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:06.712279081 CEST	192.168.2.23	8.8.8.8	0x63f0	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:09.772289991 CEST	192.168.2.23	8.8.8.8	0xc8ce	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:16.231467009 CEST	192.168.2.23	8.8.8.8	0x843e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:18.819293976 CEST	192.168.2.23	8.8.8.8	0xe1f2	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:19.869019032 CEST	192.168.2.23	8.8.8.8	0x2212	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:20.925767899 CEST	192.168.2.23	8.8.8.8	0x59b6	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:22.277837992 CEST	192.168.2.23	8.8.8.8	0x737b	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 06:56:50.054846048 CEST	8.8.8.8	192.168.2.23	0xf146	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:56:57.103171110 CEST	8.8.8.8	192.168.2.23	0xdd64	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:56:58.152157068 CEST	8.8.8.8	192.168.2.23	0x9804	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:02.206698895 CEST	8.8.8.8	192.168.2.23	0x8be8	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:07.254484892 CEST	8.8.8.8	192.168.2.23	0x431f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:14.373720884 CEST	8.8.8.8	192.168.2.23	0x1113	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:15.419578075 CEST	8.8.8.8	192.168.2.23	0x7c9f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:17.467223883 CEST	8.8.8.8	192.168.2.23	0x63f0	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:20.548434019 CEST	8.8.8.8	192.168.2.23	0xc8ce	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:29.596456051 CEST	8.8.8.8	192.168.2.23	0xe1f2	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:30.656332970 CEST	8.8.8.8	192.168.2.23	0x2212	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:31.704996109 CEST	8.8.8.8	192.168.2.23	0x59b6	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:36.753519058 CEST	8.8.8.8	192.168.2.23	0xca8e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:39.799984932 CEST	8.8.8.8	192.168.2.23	0x1254	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:43.848314047 CEST	8.8.8.8	192.168.2.23	0x8f07	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:50.896404028 CEST	8.8.8.8	192.168.2.23	0xce8b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:56.982877970 CEST	8.8.8.8	192.168.2.23	0x3ad4	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:57:59.031292915 CEST	8.8.8.8	192.168.2.23	0x10b5	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:08.092725039 CEST	8.8.8.8	192.168.2.23	0x784f	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 06:58:18.140161037 CEST	8.8.8.8	192.168.2.23	0x5b45	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:24.189546108 CEST	8.8.8.8	192.168.2.23	0x8e38	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:32.236618996 CEST	8.8.8.8	192.168.2.23	0x4ed6	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:39.282852888 CEST	8.8.8.8	192.168.2.23	0x51e9	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:45.330629110 CEST	8.8.8.8	192.168.2.23	0xe41b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:50.380206108 CEST	8.8.8.8	192.168.2.23	0x3e43	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:58:58.427586079 CEST	8.8.8.8	192.168.2.23	0xc396	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:02.477582932 CEST	8.8.8.8	192.168.2.23	0x54dc	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:03.559933901 CEST	8.8.8.8	192.168.2.23	0x182d	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:09.605597973 CEST	8.8.8.8	192.168.2.23	0x1ae8	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:10.653480053 CEST	8.8.8.8	192.168.2.23	0x5de8	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:12.718441963 CEST	8.8.8.8	192.168.2.23	0x83d3	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:19.766853094 CEST	8.8.8.8	192.168.2.23	0x2e36	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:21.816644907 CEST	8.8.8.8	192.168.2.23	0x16b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:30.864298105 CEST	8.8.8.8	192.168.2.23	0x9567	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:38.941890955 CEST	8.8.8.8	192.168.2.23	0xf027	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:39.398794889 CEST	8.8.8.8	192.168.2.23	0xf146	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:44.998653889 CEST	8.8.8.8	192.168.2.23	0x306a	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:46.446966887 CEST	8.8.8.8	192.168.2.23	0xdd64	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:47.492810011 CEST	8.8.8.8	192.168.2.23	0x9804	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:51.044807911 CEST	8.8.8.8	192.168.2.23	0x7c7	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:51.541069031 CEST	8.8.8.8	192.168.2.23	0x8be8	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:59:55.092355967 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 06:59:56.590563059 CEST	8.8.8.8	192.168.2.23	0x431f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:00.142249107 CEST	8.8.8.8	192.168.2.23	0xadd3	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:03.636152983 CEST	8.8.8.8	192.168.2.23	0x1113	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:04.682857037 CEST	8.8.8.8	192.168.2.23	0x7c9f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:06.190462112 CEST	8.8.8.8	192.168.2.23	0xaf08	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:06.743859053 CEST	8.8.8.8	192.168.2.23	0x63f0	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:09.790031910 CEST	8.8.8.8	192.168.2.23	0xc8ce	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:16.248883009 CEST	8.8.8.8	192.168.2.23	0x843e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:18.838740110 CEST	8.8.8.8	192.168.2.23	0xe1f2	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:19.887870073 CEST	8.8.8.8	192.168.2.23	0x2212	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:20.945054054 CEST	8.8.8.8	192.168.2.23	0x59b6	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:00:22.297184944 CEST	8.8.8.8	192.168.2.23	0x737b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: BWfKcndJCz PID: **6270**, Parent PID: **6124**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	/tmp/BWfKcndJCz
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: BWfKcndJCz PID: **6272**, Parent PID: **6270**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: BWfKcndJCz PID: **6273**, Parent PID: **6270**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: BWfKcndJCz PID: **6275**, Parent PID: **6270**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: BWfKcndJCz PID: **6277**, Parent PID: **6270**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: BWfKcndJCz PID: **6281**, Parent PID: **6277**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: BWfKcndJCz PID: **6368**, Parent PID: **6281**

General

Start time:	06:59:38
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: BWfKcndJCz PID: **6282**, Parent PID: **6277**

General

Start time:	06:56:48
Start date:	06/08/2022
Path:	/tmp/BWfKcndJCz
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9