ID: 679614
Sample Name: 7TgP3VbC81
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 06:20:08
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

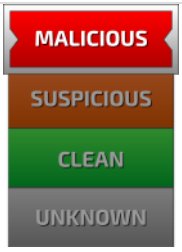
7TgP3VbC81

Overview

General Information

Sample Name:	7TgP3VbC81
Analysis ID:	679614
MD5:	6b953ba2d7e625.
SHA1:	8b40a086aab5a8.
SHA256:	f1385883753c29..
Tags:	32 elf mips mirai
Infos:	

Detection



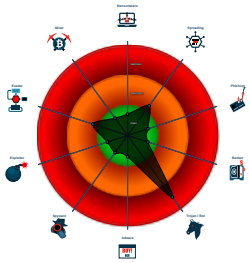
Mirai

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…
- 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.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679614
Start date and time: 06/08/202206:20:08	2022-08-06 06:20:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7TgP3VbC81
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@47/0

Warnings

Runtime Messages

Command:	/tmp/7TgP3VbC81
PID:	6227
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 7TgP3VbC81 (PID: 6227, Parent: 6119, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/7TgP3VbC81
  - 7TgP3VbC81 New Fork (PID: 6229, Parent: 6227)
  - 7TgP3VbC81 New Fork (PID: 6230, Parent: 6227)
  - 7TgP3VbC81 New Fork (PID: 6232, Parent: 6227)
  - 7TgP3VbC81 New Fork (PID: 6234, Parent: 6227)
    - 7TgP3VbC81 New Fork (PID: 6238, Parent: 6234)
      - 7TgP3VbC81 New Fork (PID: 6326, Parent: 6238)
    - 7TgP3VbC81 New Fork (PID: 6239, Parent: 6234)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
7TgP3VbC81	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
6227.1.00007f191c400000.00007f191c41c000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6326.1.00007f191c400000.00007f191c41c000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6239.1.00007f191c400000.00007f191c41c000.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

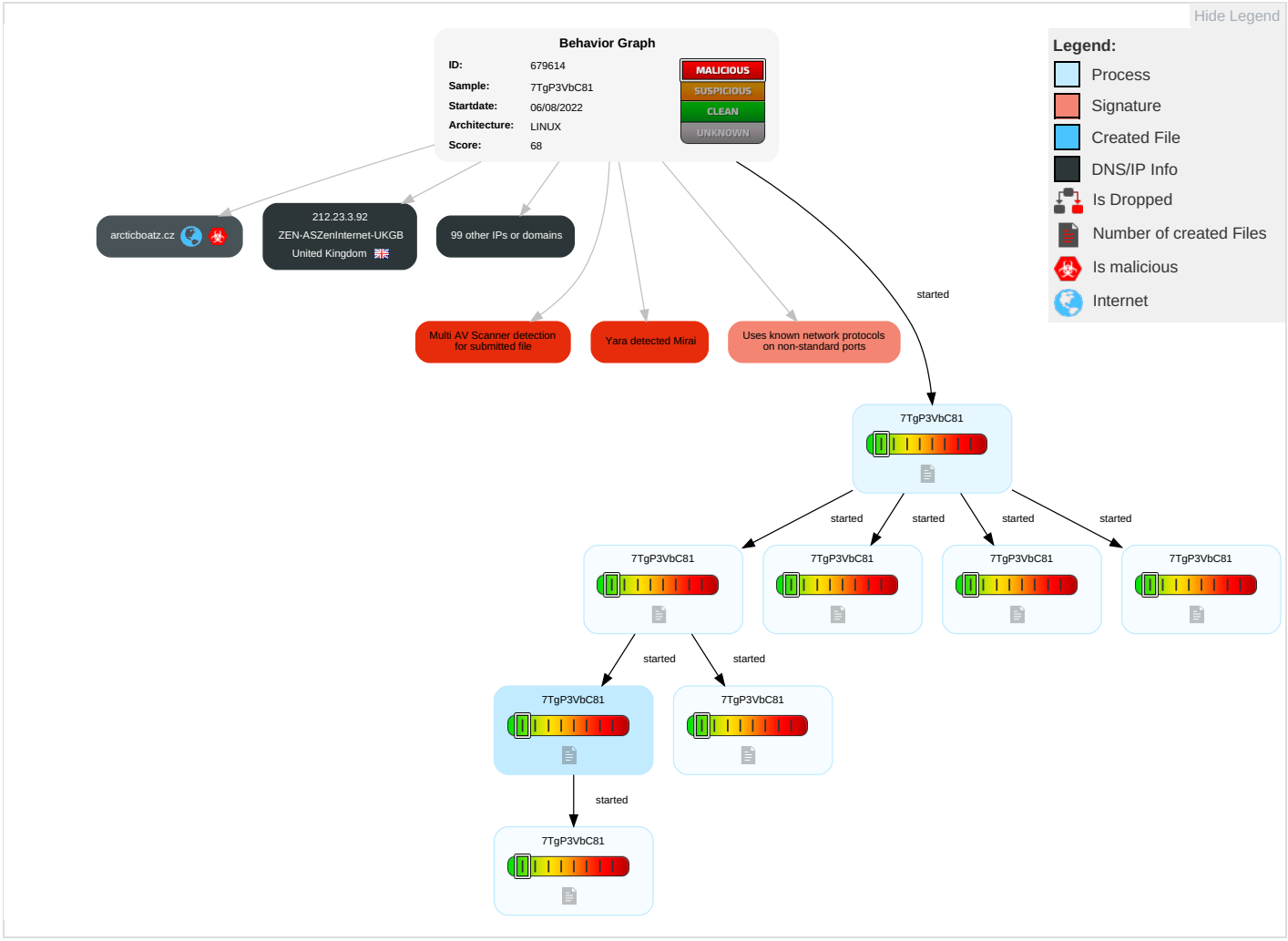
Mitre Att&ck Matrix

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
7TgP3VbC81	44%	Virustotal		Browse
7TgP3VbC81	42%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

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

URLs

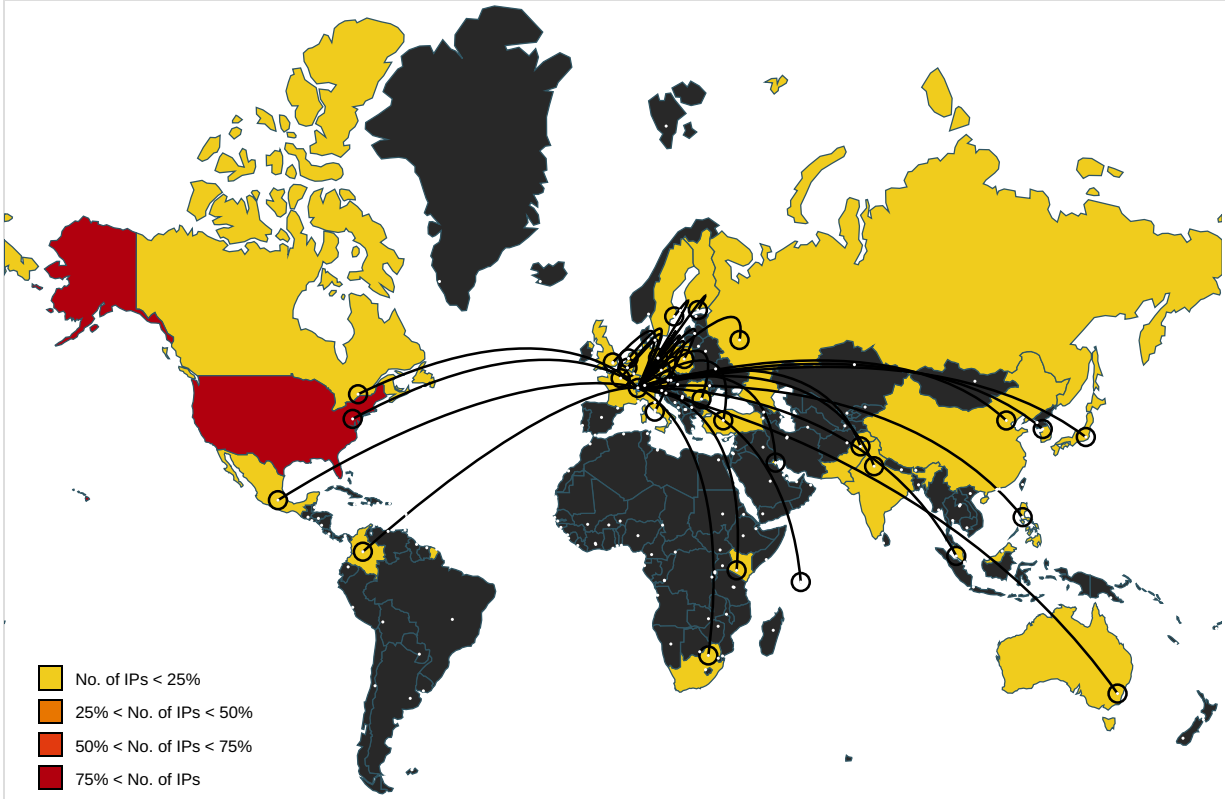
No Antivirus matches

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
17.159.246.11	unknown	United States		714	APPLE-ENGINEERINGUS	false
62.150.37.215	unknown	Kuwait		9155	QNETKuwaitKW	false
78.168.208.227	unknown	Turkey		9121	TTNETTR	false
77.204.100.77	unknown	France		15557	LDCOMNETFR	false
212.23.3.92	unknown	United Kingdom		13037	ZEN-ASZenInternet-UKGB	false
201.141.217.207	unknown	Mexico		28548	CablevisionSAdeCVMX	false
244.19.18.128	unknown	Reserved		unknown	unknown	false
223.162.231.54	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false
117.82.145.160	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
165.166.17.220	unknown	United States		2711	SPIRITTEL-ASUS	false
106.189.251.218	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
223.124.111.175	unknown	China		58453	CMI-INT-HKLevel30Tower1HK	false
86.75.116.7	unknown	France		15557	LDCOMNETFR	false
124.177.22.131	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
182.176.253.238	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
217.204.250.90	unknown	United Kingdom		4589	EASYNETEasynetGlobalServicesEU	false
169.115.139.77	unknown	United States		37611	AfrihostZA	false
13.241.78.232	unknown	United States		16509	AMAZON-02US	false
154.159.56.192	unknown	Kenya		36926	CKL1-ASNKE	false
57.72.103.249	unknown	Belgium		4862	EQUANT-ASIAOrangeBusinessASforAsiaHK	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.63.234.103	unknown	Sweden		8473	BAHNHOFhttpwwwbahnhofnetSE	false
94.82.90.48	unknown	Italy		3269	ASN-IBSNAZIT	false
212.246.13.206	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
48.205.4.172	unknown	United States		2686	ATGS-MMD-ASUS	false
67.36.232.196	unknown	United States		7018	ATT-INTERNET4US	false
152.78.134.107	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
60.14.98.46	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
59.33.173.191	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
175.233.21.253	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
107.239.190.125	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
206.33.161.60	unknown	United States		3356	LEVEL3US	false
45.133.252.66	unknown	Netherlands		39855	MOD-EUNL	false
201.233.213.59	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	false
66.199.253.54	unknown	United States		15149	EZZI-101-BGPUS	false
69.48.43.242	unknown	United States		7029	WINDSTREAMUS	false
196.19.248.151	unknown	Seychelles		134451	NME-INDONESIA-AS-APNewMediaExpressPteLtdID	false
205.126.90.244	unknown	United States		210	WEST-NET-WESTUS	false
167.247.32.221	unknown	United States		22808	RESOURCES-22808US	false
213.214.202.178	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
172.130.165.136	unknown	United States		7018	ATT-INTERNET4US	false
156.50.126.194	unknown	Australia		7474	OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU	false
70.19.140.120	unknown	United States		701	UUNETUS	false
222.77.88.125	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
70.9.41.41	unknown	United States		10507	SPCSUS	false
40.47.32.119	unknown	United States		4249	LILLY-ASUS	false
44.75.155.206	unknown	United States		7377	UCSDUS	false
84.14.172.232	unknown	France		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
173.206.218.17	unknown	Canada		6407	PRIMUS-AS6407CA	false
98.169.64.222	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
120.37.237.252	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
46.214.56.192	unknown	Romania		48161	NG-ASSosBucuresti-Ploiestinr42-44RO	false
202.218.0.138	unknown	Japan		4694	IDCFIDCFrontierIncJP	false
166.78.21.96	unknown	United States		33070	RMH-14US	false
149.182.164.178	unknown	United Kingdom		87	INDIANA-ASUS	false
172.199.5.143	unknown	Australia		18747	IFX18747US	false
71.170.191.70	unknown	United States		5650	FRONTIER-FRTRUS	false
152.10.107.193	unknown	United States		81	NCRENUS	false
160.218.217.91	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
138.196.204.99	unknown	United States		21727	HAMLINE-EDUUS	false
148.185.181.95	unknown	European Union		3423	ATTIS-ASN3423US	false
198.202.36.252	unknown	United States		19631	TRAVELPORTUS	false
121.213.76.151	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
120.49.195.34	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
159.140.225.110	unknown	United States		17264	CERNER-COMUS	false
19.30.101.119	unknown	United States		3	MIT-GATEWAYSUS	false
62.187.201.147	unknown	European Union		34456	RIALCOM-ASRU	false
146.175.71.245	unknown	Belgium		2611	BELNETBE	false
253.187.143.75	unknown	Reserved		unknown	unknown	false
99.190.37.164	unknown	United States		7018	ATT-INTERNET4US	false
107.38.10.186	unknown	United States		16567	NETRIX-16567US	false
95.225.107.143	unknown	Italy		3269	ASN-IBSNAZIT	false
82.139.56.71	unknown	Poland		29314	VECTRANET-ASAlZwyciestwa25381-525GdyniaPolandPL	false
80.146.251.45	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
119.93.5.1	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
148.251.220.122	unknown	Germany		24940	HETZNER-ASDE	false
59.170.157.125	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
18.73.47.59	unknown	United States		3	MIT-GATEWAYSUS	false
83.174.246.4	unknown	Russian Federation		28812	JSCBIS-ASRU	false
80.88.60.229	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
179.32.239.37	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
45.39.118.65	unknown	United States		18779	EGIHOSTINGUS	false
184.2.144.241	unknown	United States		14905	CENTURYLINK-LEGACY-EMBARQ-VACHVLUS	false
242.158.175.117	unknown	Reserved		unknown	unknown	false
62.40.163.77	unknown	Austria		8339	KABSI-ASAT	false
67.136.85.220	unknown	United States		7385	ALLSTREAMUS	false
66.96.2.234	unknown	United States		13337	EVWI-NET-01US	false
163.156.1.252	unknown	United Kingdom		9452	KUNET-ASKoreaUniversityKR	false
70.181.229.167	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
145.243.97.219	unknown	Germany		8792	ASVNETDE	false
142.151.26.153	unknown	Canada		239	UTORONTO-ASCA	false
196.161.183.190	unknown	South Africa		328065	Vast-Networks-ASZA	false
175.137.214.129	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
40.55.196.195	unknown	United States		4249	LILLY-ASUS	false
117.238.129.132	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
146.137.69.139	unknown	United States		683	ARGONNE-ASUS	false
94.142.228.118	unknown	Sweden		48994	GLOBALWIRESE	false
58.84.60.174	unknown	India		134343	OMSAI-ASOmSaiEntertainmentIN	false
208.3.184.76	unknown	United States		1239	SPRINTLINKUS	false
255.113.239.159	unknown	Reserved		unknown	unknown	false
246.241.203.232	unknown	Reserved		unknown	unknown	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.650969791181366
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	7TgP3VbC81
File size:	115828
MD5:	6b953ba2d7e62577777ffa13fda7672a
SHA1:	8b40a086aab5a866c9f003c9700cd24adb19d1c1
SHA256:	f1385883753c291d880e82d3abb6e91beaf067bc554da378e67a812fcd568b9e
SHA512:	e2bf853fc4d92b10dd543cba097c169759312eecb9c3d5c61d101f752b59486bbfd3bb612b7c3dce63c702f5a597e9ca2fe7e7d2e7d483bd3cd756378e7df01b
SSDEEP:	1536:B7R1XPLChIeGkhEVw27/TVsVB3qZBGaBlDRserWIHEJYvhZ/8:B7rXP2+WYjlluQyQh+
TLSH:	8FB3F806BF614FFBD85FDD3749EA1B0528DC590622A97B367674D418F28B20F0AE3864
File Content Preview:	.ELF.....`.@.4...D.....4. ...(.....@...@.....E...E.....8.....Q.td.....<|<.'!.....'.....<X<.'!... .....9'.. ..... <(<.'!.....0.9

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little 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
Section Header Offset:	115268

ELF header

Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

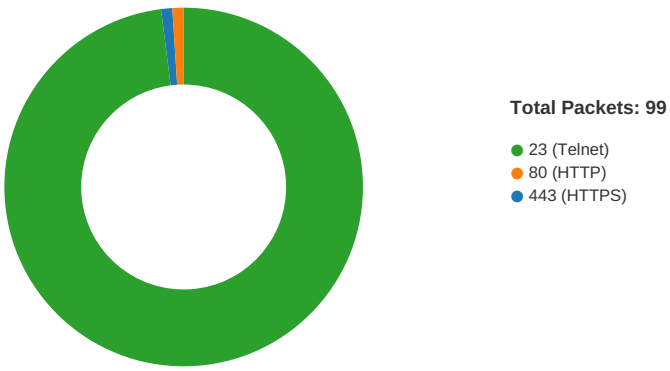
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x19180	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x4192a0	0x192a0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x419300	0x19300	0x22c0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x45b5c4	0x1b5c4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x45b5cc	0x1b5cc	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x45b5d8	0x1b5d8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x45b5e0	0x1b5e0	0x740	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x45bd20	0x1bd20	0x4c0	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x45c1e0	0x1c1e0	0x24	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x45c210	0x1c1e0	0x2c40	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x936	0x1c1e0	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x1c1e0	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	0x1b5c0	0x1b5c0	5.6526	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1b5c4	0x45b5c4	0x45b5c4	0xc1c	0x388c	4.7980	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

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 06:20:55.054124117 CEST	192.168.2.23	8.8.8.8	0xf9a3	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:01.118504047 CEST	192.168.2.23	8.8.8.8	0x4e48	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:10.168927908 CEST	192.168.2.23	8.8.8.8	0x40a1	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:12.227207899 CEST	192.168.2.23	8.8.8.8	0x48ed	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:22.275098085 CEST	192.168.2.23	8.8.8.8	0xdd4e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:27.322024107 CEST	192.168.2.23	8.8.8.8	0xcdb4	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:33.371695995 CEST	192.168.2.23	8.8.8.8	0x31b5	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:39.420341969 CEST	192.168.2.23	8.8.8.8	0x2599	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:42.488002062 CEST	192.168.2.23	8.8.8.8	0xa3ec	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:43.536468983 CEST	192.168.2.23	8.8.8.8	0xd48a	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:49.587800980 CEST	192.168.2.23	8.8.8.8	0xad34	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:58.636670113 CEST	192.168.2.23	8.8.8.8	0xf063	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:08.683094978 CEST	192.168.2.23	8.8.8.8	0x686c	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:14.733016968 CEST	192.168.2.23	8.8.8.8	0xde39	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:16.780201912 CEST	192.168.2.23	8.8.8.8	0xec17	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:17.827028036 CEST	192.168.2.23	8.8.8.8	0x356c	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:26.923281908 CEST	192.168.2.23	8.8.8.8	0xfec0	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:33.972594976 CEST	192.168.2.23	8.8.8.8	0x2f9	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:41.020912886 CEST	192.168.2.23	8.8.8.8	0x708a	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:49.069212914 CEST	192.168.2.23	8.8.8.8	0x485a	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:54.119970083 CEST	192.168.2.23	8.8.8.8	0x2eaf	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:58.203330994 CEST	192.168.2.23	8.8.8.8	0xcf8	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:08.251602888 CEST	192.168.2.23	8.8.8.8	0xbb27	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:12.299897909 CEST	192.168.2.23	8.8.8.8	0x7627	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:15.347408056 CEST	192.168.2.23	8.8.8.8	0xe0b7	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:23.402803898 CEST	192.168.2.23	8.8.8.8	0x3820	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:31.451904058 CEST	192.168.2.23	8.8.8.8	0x4f03	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:34.501224041 CEST	192.168.2.23	8.8.8.8	0xb85f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:39.549057961 CEST	192.168.2.23	8.8.8.8	0x1afe	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:40.597901106 CEST	192.168.2.23	8.8.8.8	0xbd4f	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:43.043684959 CEST	192.168.2.23	8.8.8.8	0xf9a3	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:47.644881964 CEST	192.168.2.23	8.8.8.8	0xb53b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:48.718522072 CEST	192.168.2.23	8.8.8.8	0x5fb	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:49.138235092 CEST	192.168.2.23	8.8.8.8	0x4e48	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:58.187613964 CEST	192.168.2.23	8.8.8.8	0x40a1	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 06:23:58.782862902 CEST	192.168.2.23	8.8.8.8	0x9d02	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:00.236366987 CEST	192.168.2.23	8.8.8.8	0x48ed	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:03.829914093 CEST	192.168.2.23	8.8.8.8	0x9a72	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:05.878206968 CEST	192.168.2.23	8.8.8.8	0x3442	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:10.285254955 CEST	192.168.2.23	8.8.8.8	0xdd4e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:10.924487114 CEST	192.168.2.23	8.8.8.8	0x1d92	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:11.969971895 CEST	192.168.2.23	8.8.8.8	0xbe30	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:15.337949991 CEST	192.168.2.23	8.8.8.8	0xcdb4	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:19.017915964 CEST	192.168.2.23	8.8.8.8	0xa87e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:21.390042067 CEST	192.168.2.23	8.8.8.8	0x31b5	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:26.094063997 CEST	192.168.2.23	8.8.8.8	0x911e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:27.439021111 CEST	192.168.2.23	8.8.8.8	0x2599	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 06:20:55.073971987 CEST	8.8.8.8	192.168.2.23	0xf9a3	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:01.137649059 CEST	8.8.8.8	192.168.2.23	0x4e48	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:10.188059092 CEST	8.8.8.8	192.168.2.23	0x40a1	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:12.246836901 CEST	8.8.8.8	192.168.2.23	0x48ed	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:22.292320967 CEST	8.8.8.8	192.168.2.23	0xdd4e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:27.341434002 CEST	8.8.8.8	192.168.2.23	0xcdb4	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:33.391268015 CEST	8.8.8.8	192.168.2.23	0x31b5	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:39.439193964 CEST	8.8.8.8	192.168.2.23	0x2599	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:42.507453918 CEST	8.8.8.8	192.168.2.23	0xa3ec	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:43.557682037 CEST	8.8.8.8	192.168.2.23	0xd48a	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:49.607022047 CEST	8.8.8.8	192.168.2.23	0xad34	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:21:58.654369116 CEST	8.8.8.8	192.168.2.23	0xf063	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:08.702673912 CEST	8.8.8.8	192.168.2.23	0x686c	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:14.750861883 CEST	8.8.8.8	192.168.2.23	0xde39	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:16.798026085 CEST	8.8.8.8	192.168.2.23	0xec17	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:17.846694946 CEST	8.8.8.8	192.168.2.23	0x356c	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:26.942719936 CEST	8.8.8.8	192.168.2.23	0xfec0	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:33.991853952 CEST	8.8.8.8	192.168.2.23	0x2f9	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:41.041075945 CEST	8.8.8.8	192.168.2.23	0x708a	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:49.088829994 CEST	8.8.8.8	192.168.2.23	0x485a	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:22:54.139631987 CEST	8.8.8.8	192.168.2.23	0x2eaf	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 06:22:58.222995996 CEST	8.8.8.8	192.168.2.23	0xcf8	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:08.271111965 CEST	8.8.8.8	192.168.2.23	0xbb27	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:12.317714930 CEST	8.8.8.8	192.168.2.23	0x7627	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:15.367042065 CEST	8.8.8.8	192.168.2.23	0xe0b7	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:23.422594070 CEST	8.8.8.8	192.168.2.23	0x3820	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:31.470913887 CEST	8.8.8.8	192.168.2.23	0x4f03	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:34.518801928 CEST	8.8.8.8	192.168.2.23	0xb85f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:39.568897963 CEST	8.8.8.8	192.168.2.23	0x1afe	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:40.615494013 CEST	8.8.8.8	192.168.2.23	0xbd4f	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:43.062648058 CEST	8.8.8.8	192.168.2.23	0xf9a3	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:47.664321899 CEST	8.8.8.8	192.168.2.23	0xb53b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:48.754725933 CEST	8.8.8.8	192.168.2.23	0x5fb	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:49.158003092 CEST	8.8.8.8	192.168.2.23	0x4e48	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:58.207087040 CEST	8.8.8.8	192.168.2.23	0x40a1	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:23:58.801214933 CEST	8.8.8.8	192.168.2.23	0x9d02	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:00.256150961 CEST	8.8.8.8	192.168.2.23	0x48ed	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:03.849462986 CEST	8.8.8.8	192.168.2.23	0x9a72	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:05.896336079 CEST	8.8.8.8	192.168.2.23	0x3442	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:10.304522038 CEST	8.8.8.8	192.168.2.23	0xdd4e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:10.941411972 CEST	8.8.8.8	192.168.2.23	0x1d92	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:11.989578009 CEST	8.8.8.8	192.168.2.23	0xbe30	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:15.358570099 CEST	8.8.8.8	192.168.2.23	0xcdb4	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:19.037736893 CEST	8.8.8.8	192.168.2.23	0xa87e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:21.409496069 CEST	8.8.8.8	192.168.2.23	0x31b5	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:26.113811016 CEST	8.8.8.8	192.168.2.23	0x911e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 06:24:27.456790924 CEST	8.8.8.8	192.168.2.23	0x2599	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: 7TgP3VbC81 PID: **6227**, Parent PID: **6119**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	/tmp/7TgP3VbC81
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: 7TgP3VbC81 PID: **6229**, Parent PID: **6227**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 7TgP3VbC81 PID: **6230**, Parent PID: **6227**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 7TgP3VbC81 PID: **6232**, Parent PID: **6227**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 7TgP3VbC81 PID: **6234**, Parent PID: **6227**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 7TgP3VbC81 PID: **6238**, Parent PID: **6234**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: 7TgP3VbC81 PID: **6326**, Parent PID: **6238**

General

Start time:	06:23:42
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 7TgP3VbC81 PID: **6239**, Parent PID: **6234**

General

Start time:	06:20:54
Start date:	06/08/2022
Path:	/tmp/7TgP3VbC81
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9