ID: 679625
Sample Name: dNLKZA6IVs
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:00:30
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

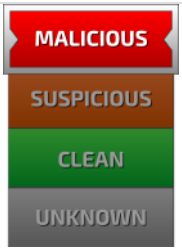
dNLKZA6IVs

Overview

General Information

Sample Name:	dNLKZA6IVs
Analysis ID:	679625
MD5:	407a38109a75cc..
SHA1:	d75de51babdf08..
SHA256:	6874279cf48edc…
Tags:	32 arm elf mirai
Infos:	

Detection



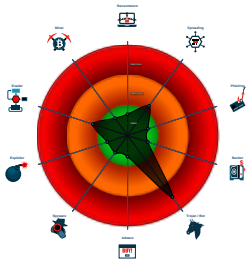
Mirai

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.

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:	679625
Start date and time: 06/08/202207:00:30	2022-08-06 07:00:30 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dNLKZA6IVs
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@46/0

Warnings

Runtime Messages

Command:	/tmp/dNLKZA6IVs
PID:	6231
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- dNLKZA6IVs (PID: 6231, Parent: 6125, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/dNLKZA6IVs
  - dNLKZA6IVs New Fork (PID: 6233, Parent: 6231)
  - dNLKZA6IVs New Fork (PID: 6234, Parent: 6231)
  - dNLKZA6IVs New Fork (PID: 6235, Parent: 6231)
  - dNLKZA6IVs New Fork (PID: 6238, Parent: 6231)
    - dNLKZA6IVs New Fork (PID: 6242, Parent: 6238)
      - dNLKZA6IVs New Fork (PID: 6329, Parent: 6242)
    - dNLKZA6IVs New Fork (PID: 6243, Parent: 6238)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
dNLKZA6IVs	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
6329.1.00007f5c4c017000.00007f5c4c02e000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6231.1.00007f5c4c017000.00007f5c4c02e000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6243.1.00007f5c4c017000.00007f5c4c02e000.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

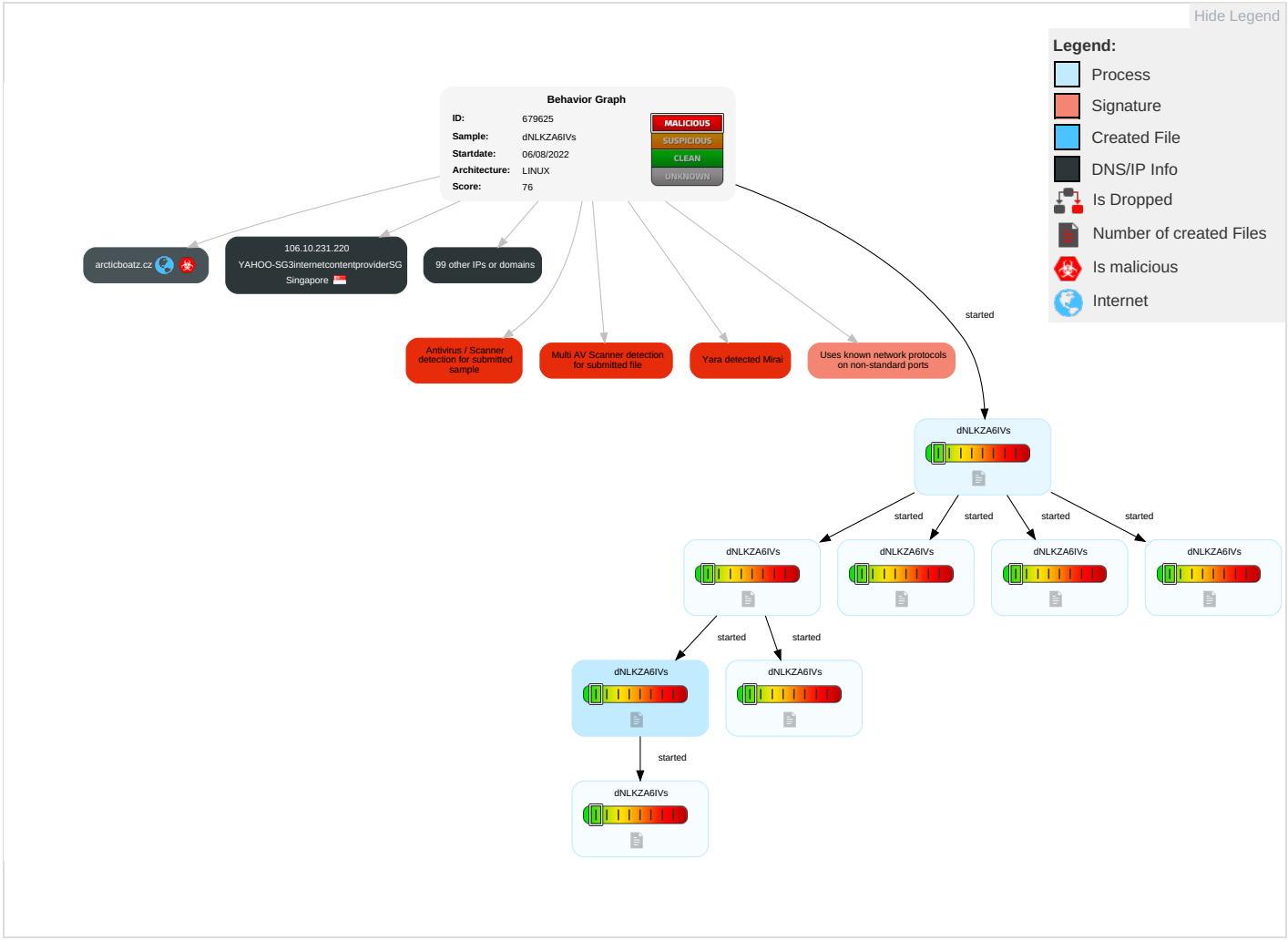
Mitre Att&ck Matrix

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
dNLKZA6IVs	44%	Virustotal		Browse
dNLKZA6IVs	34%	Metadefender		Browse
dNLKZA6IVs	73%	ReversingLabs	Linux.Trojan.Mirai	
dNLKZA6IVs	100%	Avira	LINUX/Mirai.krmnq	

Dropped Files

No Antivirus matches

Domains

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

URLs

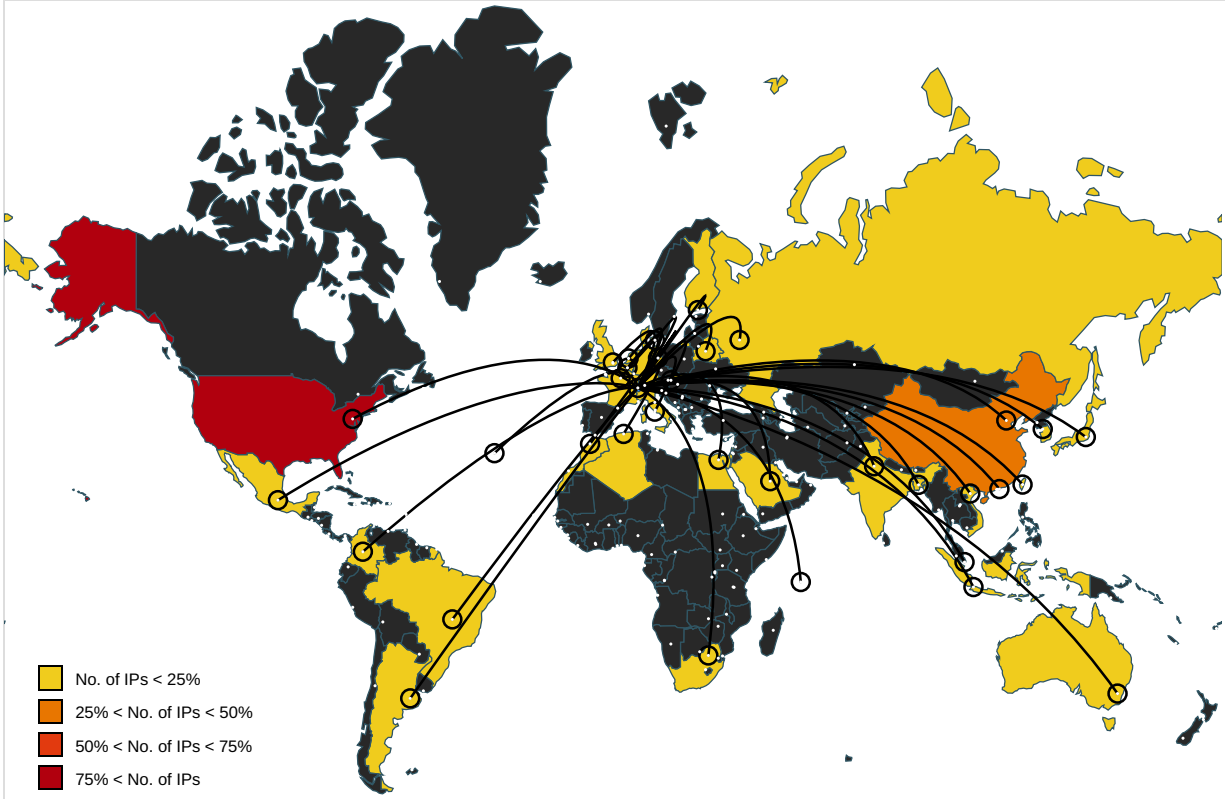
No Antivirus matches

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
140.245.130.189	unknown	United States		22488	CENGAGE-NYALBUS	false
179.99.190.111	unknown	Brazil		27699	TELEFONICABRASILSABR	false
160.177.155.129	unknown	Morocco		36903	MT-MPLSMA	false
163.39.57.194	unknown	United States		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
252.34.227.164	unknown	Reserved		unknown	unknown	false
116.100.223.37	unknown	Viet Nam		24086	VIETTEL-AS-VNViettelCorporationVN	false
157.117.193.135	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
147.196.107.48	unknown	France		2527	SO-NETSo-netEntertainmentCorporationJP	false
115.21.18.96	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
71.56.55.19	unknown	United States		7922	COMCAST-7922US	false
187.188.56.79	unknown	Mexico		22884	TOTALPLAYTELECOMUNICACIONESSADECVMX	false
42.25.215.245	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
104.156.153.64	unknown	United States		32391	SRCACCESSUS	false
95.106.170.150	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
84.35.150.57	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	false
40.220.55.208	unknown	United States		4249	LILLY-ASUS	false
124.207.149.250	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
125.193.114.56	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
253.132.90.144	unknown	Reserved		unknown	unknown	false
41.97.15.205	unknown	Algeria		36947	ALGTEL-ASDZ	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.101.21.217	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
200.164.68.140	unknown	Brazil		7738	TelemarNorteLesteSABR	false
216.107.146.42	unknown	United States		20278	NEXEONUS	false
106.10.231.220	unknown	Singapore		56173	YAHOO-SG3internetcontentproviderSG	false
248.239.3.124	unknown	Reserved		unknown	unknown	false
206.176.20.180	unknown	United States		22851	NSU-SDUS	false
178.178.13.56	unknown	Russian Federation		25159	SONICDUO-ASRU	false
221.4.223.185	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
149.109.163.226	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
54.44.2.152	unknown	United States		14618	AMAZON-AESUS	false
62.78.181.0	unknown	Finland		16086	DNAFI	false
154.91.52.21	unknown	Seychelles		62468	VPSQUANUS	false
163.151.39.94	unknown	United States		36161	WESTCHESTERCOUNTY-NYUS	false
181.152.32.197	unknown	Colombia		26611	COMCELSACO	false
108.28.236.149	unknown	United States		701	UUNETUS	false
111.6.69.172	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
78.93.243.132	unknown	Saudi Arabia		25233	AWALNET-ASNSA	false
60.87.12.18	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
119.107.244.169	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
18.163.241.145	unknown	United States		16509	AMAZON-02US	false
126.58.95.160	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
72.23.5.57	unknown	United States		27364	ACS-INTERNETUS	false
44.97.4.214	unknown	United States		7377	UCSDUS	false
45.244.146.89	unknown	Egypt		24863	LINKdotNET-ASEG	false
251.106.255.31	unknown	Reserved		unknown	unknown	false
65.67.37.241	unknown	United States		7018	ATT-INTERNET4US	false
253.194.92.93	unknown	Reserved		unknown	unknown	false
146.122.131.195	unknown	United States		22216	SIEMENS-PLMUS	false
193.89.106.134	unknown	Denmark		3292	TDCTDCASDK	false
23.54.60.124	unknown	United States		16625	AKAMAI-ASUS	false
27.193.150.188	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
200.246.226.12	unknown	Brazil		4230	CLAROSABR	false
187.123.171.57	unknown	Brazil		28573	CLAROSABR	false
81.221.46.157	unknown	Switzerland		1836	GREENgreenchAGAutonomousSystemEU	false
189.6.24.53	unknown	Brazil		28573	CLAROSABR	false
65.71.94.243	unknown	United States		7018	ATT-INTERNET4US	false
117.241.122.77	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
95.25.159.118	unknown	Russian Federation		3216	SOVAM-ASRU	false
36.228.128.198	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
158.193.226.165	unknown	Slovakia (SLOVAK Republic)		2607	SANETSlovakAcademicNetworkSK	false
12.122.193.204	unknown	United States		7018	ATT-INTERNET4US	false
92.29.42.240	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
2.46.240.136	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
124.20.249.100	unknown	China		7497	CSTNET-AS-APComputerNetworkInformationCenterCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.117.108.117	unknown	Bangladesh		137935	ILIS-AS-APILinkInternetServiceBD	false
36.73.61.185	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
80.178.27.50	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	false
163.52.238.118	unknown	unknown		2516	KDDIKDDICORPORATIONJP	false
203.198.234.145	unknown	Hong Kong		4760	HKTIMS-APHKTLimitedHK	false
201.103.48.20	unknown	Mexico		8151	UninetSAdeCVMX	false
57.46.12.214	unknown	Belgium		2686	ATGS-MMD-ASUS	false
36.70.155.73	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
78.200.186.78	unknown	France		12322	PROXADFR	false
162.5.107.138	unknown	United States		33348	PIERCE-COUNTYUS	false
20.35.186.177	unknown	United States		8070	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
178.122.24.177	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
162.97.87.246	unknown	United States		3356	LEVEL3US	false
41.145.10.73	unknown	South Africa		5713	SAIX-NETZA	false
155.244.147.141	unknown	United States		668	DNIC-AS-00668US	false
87.122.200.234	unknown	Germany		8881	VERSATELDE	false
121.17.44.98	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
136.104.45.67	unknown	United States		60311	ONEFMCH	false
242.147.54.104	unknown	Reserved		unknown	unknown	false
211.173.176.209	unknown	Korea Republic of		18313	PCN-AS-KRLGHelloVisionCorpKR	false
101.8.76.224	unknown	Taiwan; Republic of China (ROC)		701	UUNETUS	false
112.12.163.146	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
104.33.227.124	unknown	United States		20001	TWC-20001-PACWESTUS	false
17.205.243.220	unknown	United States		714	APPLE-ENGINEERINGUS	false
181.12.5.240	unknown	Argentina		7303	TelecomArgentinaSAAR	false
101.174.190.113	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
57.238.159.174	unknown	Belgium		2686	ATGS-MMD-ASUS	false
17.132.134.142	unknown	United States		714	APPLE-ENGINEERINGUS	false
120.171.58.235	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
124.115.165.91	unknown	China		4835	CHINANET-IDC-SNChinaTelecomGroupCN	false
178.107.239.74	unknown	United Kingdom		12576	EELtdGB	false
37.182.243.58	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
209.79.27.199	unknown	United States		32492	DANAUS	false
74.11.108.131	unknown	United States		7029	WINDSTREAMUS	false
37.113.150.151	unknown	Russian Federation		41661	ERTH-CHEL-ASRU	false
90.152.66.151	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.130935158584685
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	dNLKZA6lVs
File size:	95440
MD5:	407a38109a75cc3a5845952e359e2255
SHA1:	d75de51babdf08188f91d4e854160349e5c0185e
SHA256:	6874279cf48edce8cef28cce5c397462f5eadad07887dfabfb8caccf5899c436
SHA512:	291ef493c14caecfa5c2b69ebad48edc8df741f9c454562bc0e0322dc917c6d252672f116767f52f4d4a7dda299c260551decbd2f367531c16b9bbae3aa49a3e
SSDEEP:	1536:OM8MGxYUd9YdLabp+1xOOLnRVTSphZ6CqhaSbuqL3Csvc3JY4h:iBx/di6E6OLnbO3ohYE/c5vh
TLSH:	8E9349C1B881A626C6D152BBFF5F418C331697A8D2DA33128C295F61778E92F0E37749
File Content Preview:	.ELF...a.....(.....4...@s.....4. ...(.....k...k.....k...k...k.....$3.....Q.td.....-...L."...zR.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	95040

ELF header

Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

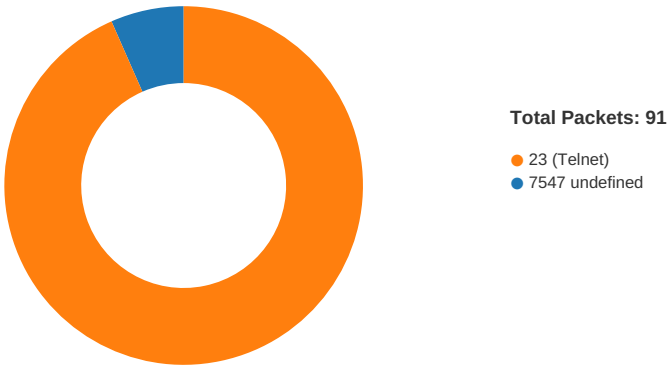
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x14a20	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1cad0	0x14ad0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1cae4	0x14ae4	0x2104	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x26bec	0x16bec	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x26bf4	0x16bf4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x26c00	0x16c00	0x700	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x27300	0x17300	0x2c10	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x17300	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	0x8000	0x8000	0x16be8	0x16be8	6.1474	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x16bec	0x26bec	0x26bec	0x714	0x3324	4.3733	0x6	RW	0x8000		.ctors .dtors .data .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
Aug 6, 2022 07:05:50.702507019 CEST	192.168.2.23	8.8.8.8	0x54be	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:05:54.752630949 CEST	192.168.2.23	8.8.8.8	0xfd19	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:04.801067114 CEST	192.168.2.23	8.8.8.8	0x7ed2	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:10.870327950 CEST	192.168.2.23	8.8.8.8	0x901	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 07:06:13.919563055 CEST	192.168.2.23	8.8.8.8	0x4d1d	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:23.967844963 CEST	192.168.2.23	8.8.8.8	0xc51e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:34.017163992 CEST	192.168.2.23	8.8.8.8	0x7948	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:41.095558882 CEST	192.168.2.23	8.8.8.8	0x3ffa	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:51.144331932 CEST	192.168.2.23	8.8.8.8	0x3dcb	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:00.192339897 CEST	192.168.2.23	8.8.8.8	0x4f47	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:08.239928961 CEST	192.168.2.23	8.8.8.8	0xb150	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:11.288945913 CEST	192.168.2.23	8.8.8.8	0x7f91	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:19.338779926 CEST	192.168.2.23	8.8.8.8	0xdeb1	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:27.385957003 CEST	192.168.2.23	8.8.8.8	0xbb86	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:28.435435057 CEST	192.168.2.23	8.8.8.8	0x1086	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:35.483746052 CEST	192.168.2.23	8.8.8.8	0x16d5	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:37.544806004 CEST	192.168.2.23	8.8.8.8	0x9c30	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:40.602895021 CEST	192.168.2.23	8.8.8.8	0xa552	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:44.651293039 CEST	192.168.2.23	8.8.8.8	0xb4cf	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:49.700762987 CEST	192.168.2.23	8.8.8.8	0x261b	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:59.748364925 CEST	192.168.2.23	8.8.8.8	0x4783	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:09.796504974 CEST	192.168.2.23	8.8.8.8	0xb28c	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:11.843915939 CEST	192.168.2.23	8.8.8.8	0x6c65	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:15.962863922 CEST	192.168.2.23	8.8.8.8	0x2e7	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:20.019285917 CEST	192.168.2.23	8.8.8.8	0x261c	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:21.067440033 CEST	192.168.2.23	8.8.8.8	0xe77a	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:29.115253925 CEST	192.168.2.23	8.8.8.8	0xd4bf	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:32.161578894 CEST	192.168.2.23	8.8.8.8	0x5241	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:39.616389990 CEST	192.168.2.23	8.8.8.8	0x54be	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:41.209120035 CEST	192.168.2.23	8.8.8.8	0x3989	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:43.674951077 CEST	192.168.2.23	8.8.8.8	0xfd19	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:49.257905006 CEST	192.168.2.23	8.8.8.8	0x4b22	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:52.303738117 CEST	192.168.2.23	8.8.8.8	0xcee4	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:53.720870018 CEST	192.168.2.23	8.8.8.8	0x7ed2	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:55.352310896 CEST	192.168.2.23	8.8.8.8	0xc7de	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:58.767436981 CEST	192.168.2.23	8.8.8.8	0x901	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:00.400082111 CEST	192.168.2.23	8.8.8.8	0x4610	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:01.827549934 CEST	192.168.2.23	8.8.8.8	0x4d1d	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:03.446547985 CEST	192.168.2.23	8.8.8.8	0xc471	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 07:09:07.495101929 CEST	192.168.2.23	8.8.8.8	0xf3b9	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:11.875713110 CEST	192.168.2.23	8.8.8.8	0xc51e	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:16.541476965 CEST	192.168.2.23	8.8.8.8	0x18f3	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:19.592694998 CEST	192.168.2.23	8.8.8.8	0xb147	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:21.966418028 CEST	192.168.2.23	8.8.8.8	0x7948	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:22.641074896 CEST	192.168.2.23	8.8.8.8	0x3f83	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:23.690777063 CEST	192.168.2.23	8.8.8.8	0x937d	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 07:05:50.719547033 CEST	8.8.8.8	192.168.2.23	0x54be	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:05:54.772036076 CEST	8.8.8.8	192.168.2.23	0xfd19	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:04.818865061 CEST	8.8.8.8	192.168.2.23	0x7ed2	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:10.890026093 CEST	8.8.8.8	192.168.2.23	0x901	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:13.938627958 CEST	8.8.8.8	192.168.2.23	0x4d1d	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:23.987060070 CEST	8.8.8.8	192.168.2.23	0xc51e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:34.037628889 CEST	8.8.8.8	192.168.2.23	0x7948	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:41.115243912 CEST	8.8.8.8	192.168.2.23	0x3ffa	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:06:51.163902998 CEST	8.8.8.8	192.168.2.23	0x3dcb	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:00.210024118 CEST	8.8.8.8	192.168.2.23	0x4f47	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:08.259632111 CEST	8.8.8.8	192.168.2.23	0xb150	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:11.308566093 CEST	8.8.8.8	192.168.2.23	0x7f91	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:19.356323004 CEST	8.8.8.8	192.168.2.23	0xdeb1	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:27.405544043 CEST	8.8.8.8	192.168.2.23	0xbb86	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:28.455080032 CEST	8.8.8.8	192.168.2.23	0x1086	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:35.504062891 CEST	8.8.8.8	192.168.2.23	0x16d5	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:37.573424101 CEST	8.8.8.8	192.168.2.23	0x9c30	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:40.622441053 CEST	8.8.8.8	192.168.2.23	0xa552	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:44.670378923 CEST	8.8.8.8	192.168.2.23	0xb4cf	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:49.720315933 CEST	8.8.8.8	192.168.2.23	0x261b	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:07:59.768058062 CEST	8.8.8.8	192.168.2.23	0x4783	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:09.814372063 CEST	8.8.8.8	192.168.2.23	0xb28c	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:11.875591993 CEST	8.8.8.8	192.168.2.23	0x6c65	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:15.982000113 CEST	8.8.8.8	192.168.2.23	0x2e7	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:20.038809061 CEST	8.8.8.8	192.168.2.23	0x261c	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:21.084737062 CEST	8.8.8.8	192.168.2.23	0xe77a	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 07:08:29.132872105 CEST	8.8.8.8	192.168.2.23	0xd4bf	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:32.180759907 CEST	8.8.8.8	192.168.2.23	0x5241	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:39.635659933 CEST	8.8.8.8	192.168.2.23	0x54be	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:41.228621960 CEST	8.8.8.8	192.168.2.23	0x3989	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:43.692435980 CEST	8.8.8.8	192.168.2.23	0xfd19	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:49.274925947 CEST	8.8.8.8	192.168.2.23	0x4b22	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:52.323026896 CEST	8.8.8.8	192.168.2.23	0xcee4	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:53.738450050 CEST	8.8.8.8	192.168.2.23	0x7ed2	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:55.369638920 CEST	8.8.8.8	192.168.2.23	0xc7de	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:08:58.795795918 CEST	8.8.8.8	192.168.2.23	0x901	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:00.417481899 CEST	8.8.8.8	192.168.2.23	0x4610	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:01.847336054 CEST	8.8.8.8	192.168.2.23	0x4d1d	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:03.466379881 CEST	8.8.8.8	192.168.2.23	0xc471	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:07.512717009 CEST	8.8.8.8	192.168.2.23	0xf3b9	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:11.894723892 CEST	8.8.8.8	192.168.2.23	0xc51e	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:16.560956955 CEST	8.8.8.8	192.168.2.23	0x18f3	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:19.612413883 CEST	8.8.8.8	192.168.2.23	0xb147	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:21.986105919 CEST	8.8.8.8	192.168.2.23	0x7948	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:22.660722971 CEST	8.8.8.8	192.168.2.23	0x3f83	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)
Aug 6, 2022 07:09:23.710640907 CEST	8.8.8.8	192.168.2.23	0x937d	No error (0)	arcticboatz.cz		46.23.109.40	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: dNLKZA6IVs PID: **6231**, Parent PID: **6125**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	/tmp/dNLKZA6IVs
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: dNLKZA6IVs PID: **6233**, Parent PID: **6231**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	n/a

File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: dNLKZA6IVs PID: **6234**, Parent PID: **6231**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: dNLKZA6IVs PID: **6235**, Parent PID: **6231**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: dNLKZA6IVs PID: **6238**, Parent PID: **6231**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: dNLKZA6IVs PID: **6242**, Parent PID: **6238**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: dNLKZA6IVs PID: **6329**, Parent PID: **6242**

General

Start time:	07:08:38
Start date:	06/08/2022
Path:	/tmp/dNLKZA6IVs
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: dNLKZA6IVs PID: **6243**, Parent PID: **6238**

General

Start time:	07:05:49
Start date:	06/08/2022
Path:	/tmp/dNLKZA6lVs
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1