
**ID:** 679617
**Sample Name:** 9aDl048Kv4
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 06:33:44
**Date:** 06/08/2022
**Version:** 35.0.0 Citrine

# Table of Contents

# Linux Analysis Report

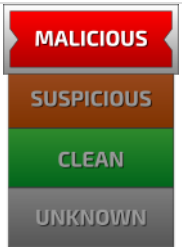
## 9aDl048Kv4

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 9aDl048Kv4 |
| Analysis ID: | 679617 |
| MD5: | a6d59f5e0ba33c.. |
| SHA1: | e54874d4f97c4e.. |
| SHA256: | 04dac155bac071.. |
| Tags: | 32 elf mips mirai |
| Infos: | |

### Detection



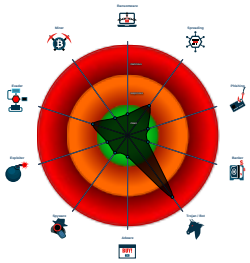

Mirai

| | |
|---|---|
| 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…
- 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…

### 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.**

**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: | 679617 |
| Start date and time: 06/08/202206:33:44 | 2022-08-06 06:33:44 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 41s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 9aDl048Kv4 |
| 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@54/0 |

## Warnings

### Runtime Messages

| | |
|---|---|
| Command: | /tmp/9aDl048Kv4 |
| PID: | 6230 |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | Connected To CNC |

| Standard Error: | |
|---|---|

## Process Tree

- **system is lnxubuntu20**
- 9aDl048Kv4 (PID: 6230, Parent: 6125, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/9aDl048Kv4
  - 9aDl048Kv4 New Fork (PID: 6233, Parent: 6230)
  - 9aDl048Kv4 New Fork (PID: 6234, Parent: 6230)
  - 9aDl048Kv4 New Fork (PID: 6235, Parent: 6230)
  - 9aDl048Kv4 New Fork (PID: 6237, Parent: 6230)
    - 9aDl048Kv4 New Fork (PID: 6242, Parent: 6237)
      - 9aDl048Kv4 New Fork (PID: 6330, Parent: 6242)
    - 9aDl048Kv4 New Fork (PID: 6243, Parent: 6237)
- **cleanup**

## Yara Signatures

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 9aDl048Kv4 | 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 |
|---|---|---|---|---|
| 6243.1.00007f96e8400000.00007f96e841b000.r-x.sdmp | JoeSecurity_Mirai_8 | Yara detected Mirai | Joe Security | |
| 6330.1.00007f96e8400000.00007f96e841b000.r-x.sdmp | JoeSecurity_Mirai_8 | Yara detected Mirai | Joe Security | |
| 6230.1.00007f96e8400000.00007f96e841b000.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

### 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

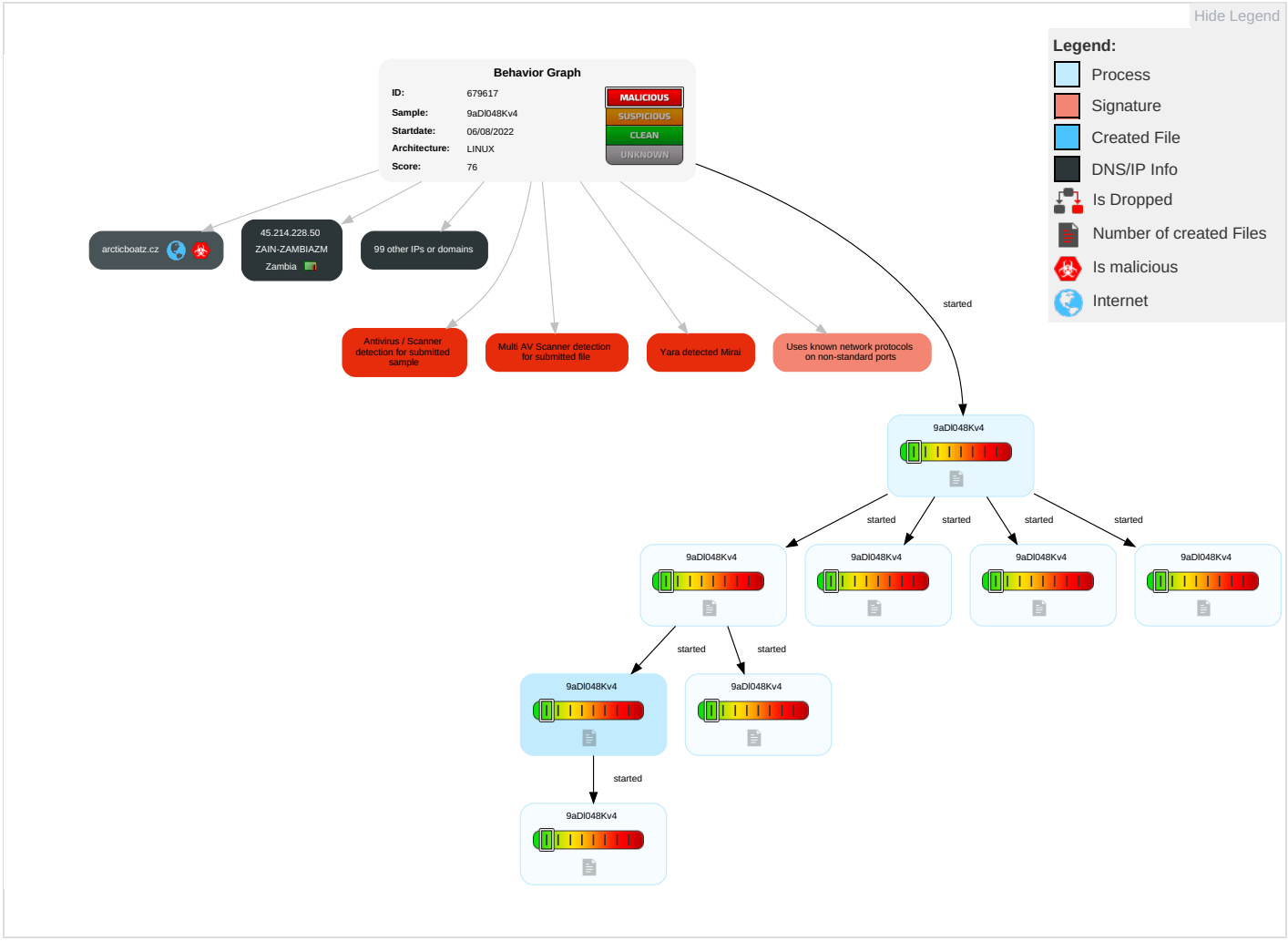
## Mitre Att&ck Matrix

| 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 |
|---|---|---|---|---|
| 9aDl048Kv4 | 56% | Virustotal | | Browse |
| 9aDl048Kv4 | 31% | Metadefender | | Browse |
| 9aDl048Kv4 | 69% | ReversingLabs | Linux.Trojan.Mirai | |
| 9aDl048Kv4 | 100% | Avira | LINUX/Mirai.ckhvs | |

### Dropped Files

No Antivirus matches

### Domains

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

### URLs

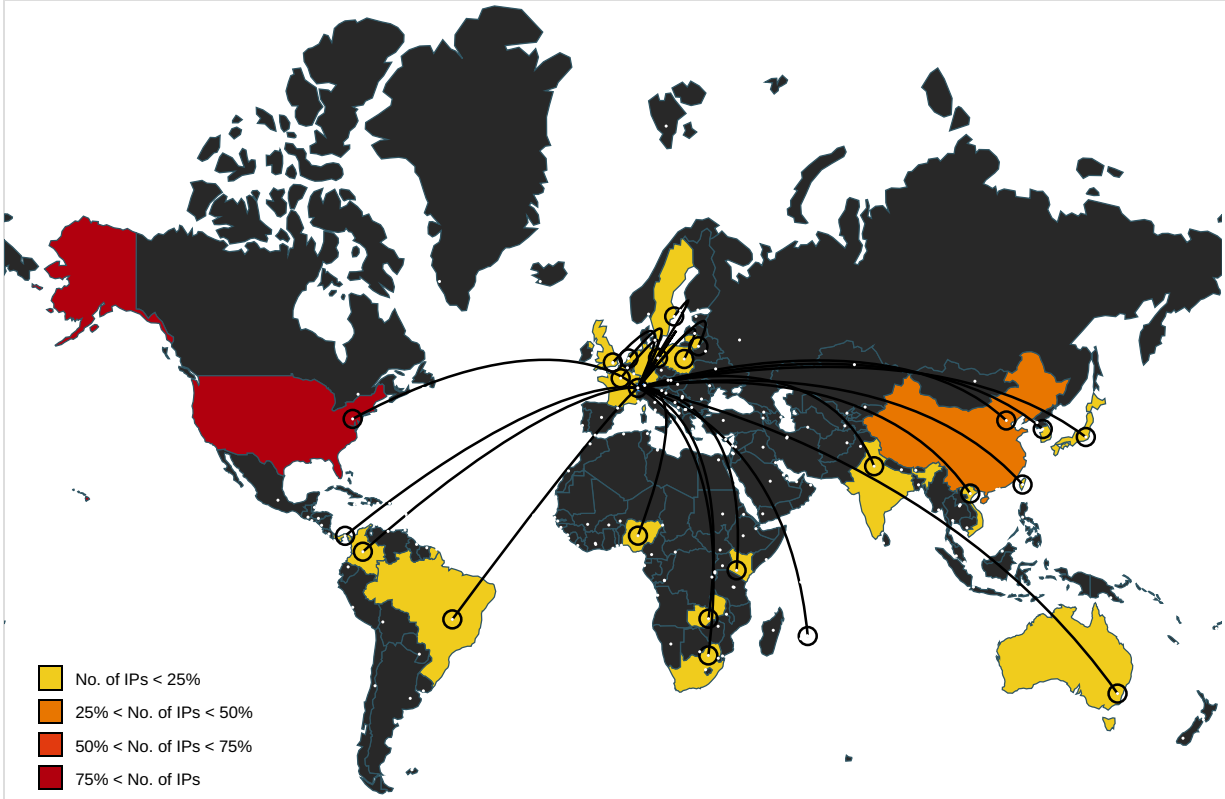
No Antivirus matches

## 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 |
|---|---|---|---|---|---|---|
| 112.38.81.126 | unknown | China | | 24444 | CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany | false |
| 209.188.192.80 | unknown | United States | | 2152 | CSUNET-NWUS | false |
| 31.119.143.132 | unknown | United Kingdom | | 12576 | EELtdGB | false |
| 168.142.106.78 | unknown | South Africa | | 3741 | ISZA | false |
| 241.238.198.119 | unknown | Reserved | | unknown | unknown | false |
| 71.207.101.131 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 243.94.91.52 | unknown | Reserved | | unknown | unknown | false |
| 82.134.138.59 | unknown | Netherlands | | 8542 | BKK-DIGITEK-AS8542NorwayNO | false |
| 103.207.37.116 | unknown | Viet Nam | | 45899 | VNPT-AS-VNVNPTCorpVN | false |
| 167.94.84.200 | unknown | United States | | 20278 | NEXEONUS | false |
| 71.234.44.99 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 20.136.114.213 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 92.173.69.212 | unknown | France | | 3215 | FranceTelecom-OrangeFR | false |
| 31.251.56.59 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 1.232.219.196 | unknown | Korea Republic of | | 9318 | SKB-ASSKBroadbandCoLtdKR | false |
| 8.85.206.249 | unknown | United States | | 3356 | LEVEL3US | false |
| 14.215.188.237 | unknown | China | | 58466 | CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN | false |
| 143.26.217.182 | unknown | United States | | 264008 | LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR | false |
| 69.71.53.125 | unknown | United States | | 12025 | IMDC-AS12025US | false |
| 133.42.124.105 | unknown | Japan | | 24248 | ASN-WADAI-UWakayamaUniversityJP | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 161.247.27.70 | unknown | United States | | 26539 | GIANT-FOOD-INCUS | false |
| 4.224.225.38 | unknown | United States | | 3356 | LEVEL3US | false |
| 99.32.231.102 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 178.192.103.30 | unknown | Switzerland | | 3303 | SWISSCOMSwisscomSwitzerlandLtdCH | false |
| 32.131.98.93 | unknown | United States | | 2686 | ATGS-MMD-ASUS | false |
| 41.115.224.79 | unknown | South Africa | | 16637 | MTNNS-ASZA | false |
| 45.214.228.50 | unknown | Zambia | | 37287 | ZAIN-ZAMBIAZM | false |
| 246.188.239.90 | unknown | Reserved | | unknown | unknown | false |
| 241.58.255.17 | unknown | Reserved | | unknown | unknown | false |
| 123.169.33.124 | unknown | China | | 4809 | CHINATELECOM-CORE-WAN-CN2ChinaTelecomNextGenerationCarr | false |
| 206.46.248.32 | unknown | United States | | 7021 | VRIS-7021US | false |
| 40.97.188.119 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 253.118.91.171 | unknown | Reserved | | unknown | unknown | false |
| 247.195.117.119 | unknown | Reserved | | unknown | unknown | false |
| 43.250.74.242 | unknown | China | | 40676 | AS40676US | false |
| 253.63.64.212 | unknown | Reserved | | unknown | unknown | false |
| 103.220.236.234 | unknown | India | | 139490 | ASPTNPL-AS-INAsptNetworksPvtLtdIN | false |
| 123.31.89.9 | unknown | Viet Nam | | 45899 | VNPT-AS-VNVNPTCorpVN | false |
| 166.148.219.208 | unknown | United States | | 22394 | CELLCOUS | false |
| 181.154.150.72 | unknown | Colombia | | 26611 | COMCELSACO | false |
| 59.128.228.32 | unknown | Japan | | 2516 | KDDIKDDICORPORATIONJP | false |
| 168.235.188.124 | unknown | United States | | 22925 | ALLIED-TELECOMUS | false |
| 217.98.115.142 | unknown | Poland | | 5617 | TPNETPL | false |
| 2.254.55.207 | unknown | Sweden | | 3301 | TELIANET-SWEDENTeliaCompanySE | false |
| 208.197.249.2 | unknown | United States | | 7029 | WINDSTREAMUS | false |
| 211.252.213.234 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 80.41.144.0 | unknown | United Kingdom | | 9105 | TISCALI-UKTalkTalkCommunicationsLimitedGB | false |
| 13.213.186.117 | unknown | United States | | 16509 | AMAZON-02US | false |
| 174.99.178.10 | unknown | United States | | 10796 | TWC-10796-MIDWESTUS | false |
| 96.132.30.42 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 174.228.87.35 | unknown | United States | | 22394 | CELLCOUS | false |
| 206.139.220.116 | unknown | United States | | 701 | UUNETUS | false |
| 180.222.63.58 | unknown | Japan | | 18371 | NCABLE-APNeighbourhoodCableAU | false |
| 201.53.53.71 | unknown | Brazil | | 28573 | CLAROSABR | false |
| 190.32.220.66 | unknown | Panama | | 11556 | CableWirelessPanamaPA | false |
| 9.193.186.225 | unknown | United States | | 3356 | LEVEL3US | false |
| 240.115.82.109 | unknown | Reserved | | unknown | unknown | false |
| 105.22.200.55 | unknown | Mauritius | | 37100 | SEACOM-ASMU | false |
| 150.115.207.2 | unknown | China | | 2516 | KDDIKDDICORPORATIONJP | false |
| 32.217.248.222 | unknown | United States | | 46690 | SNET-FCCUS | false |
| 247.116.205.32 | unknown | Reserved | | unknown | unknown | false |
| 81.98.166.242 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 165.96.21.17 | unknown | Japan | | 37053 | RSAWEB-ASZA | false |
| 122.41.44.128 | unknown | Korea Republic of | | 17858 | POWERVIS-AS-KRLGPOWERCOMMKR | false |
| 248.211.248.7 | unknown | Reserved | | unknown | unknown | false |
| 248.175.187.185 | unknown | Reserved | | unknown | unknown | false |
| 216.4.100.227 | unknown | United States | | 393577 | SCCNETUS | false |
| 219.130.114.139 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 8.196.29.161 | unknown | United States | | 3356 | LEVEL3US | false |
| 17.36.150.157 | unknown | United States | | 714 | APPLE-ENGINEERINGUS | false |
| 114.41.153.116 | unknown | Taiwan; Republic of China (ROC) | | 3462 | HINETDataCommunicationBusinessGroupTW | false |
| 247.209.22.244 | unknown | Reserved | | unknown | unknown | false |
| 194.61.190.0 | unknown | United Kingdom | | 24775 | AS24775GB | false |
| 148.11.87.103 | unknown | United States | | 394673 | 9408US | false |
| 196.40.197.88 | unknown | Nigeria | | 36974 | AFNET-ASCI | false |
| 99.123.148.139 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 204.66.36.171 | unknown | United States | | 1761 | TDIR-CAPNETUS | false |
| 187.126.17.235 | unknown | Brazil | | 7738 | TelemarNorteLesteSABR | false |
| 73.217.152.6 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 197.183.150.216 | unknown | Kenya | | 33771 | SAFARICOM-LIMITEDKE | false |
| 19.104.141.57 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 182.85.190.52 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 172.159.109.57 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 145.19.236.45 | unknown | Netherlands | | 1103 | SURFNET-NLSURFnetTheNetherlandsNL | false |
| 91.52.17.228 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 119.47.34.76 | unknown | Japan | | 7679 | QTNETQTnetIncJP | false |
| 12.77.56.175 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 183.238.72.237 | unknown | China | | 56040 | CMNET-GUANGDONG-APChinaMobilecommunicationscorporation | false |
| 19.113.192.29 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 114.183.221.23 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 217.227.178.81 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 191.210.231.186 | unknown | Brazil | | 26599 | TELEFONICABRASILSAB R | false |
| 163.123.126.190 | unknown | United States | | 1767 | ILIGHT-NETUS | false |
| 98.31.236.200 | unknown | United States | | 10796 | TWC-10796-MIDWESTUS | false |
| 121.246.90.149 | unknown | India | | 17908 | TCISLTataCommunications IN | false |
| 122.213.81.165 | unknown | Japan | | 17506 | UCOMARTERIANetworksCorporationJP | false |
| 175.172.190.121 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 175.37.77.244 | unknown | Australia | | 4804 | MPX-ASMicroplexPTYLTDAU | false |
| 222.209.131.130 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 213.197.169.187 | unknown | Lithuania | | 15440 | BALTNETACustomersASLT | false |

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped |
| Entropy (8bit): | 5.624887608307235 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | 9aDl048Kv4 |
| File size: | 114356 |
| MD5: | a6d59f5e0ba33c23089b0e8e5f33dc82 |
| SHA1: | e54874d4f97c4e80610ea3bb298eb9d912d30f65 |
| SHA256: | 04dac155bac0715d824c9f56aacd4148615bec0d761e7854da27f0fdeb827f95 |
| SHA512: | da0817d6f3b65997e197a9991938180e7a88e3b8ae89a835684a238fabf438c71f60316833377c24f354ed224bf699049397ad8a0c72ab454a305c7a80605530 |
| SSDEEP: | 1536:8RTc+b0cmOw9teplZ2axAzVQs842JnFhKeFuOg6HmG1eMEXSJYWsz0c2:2TRbnIyzVQs8XtFnFuOg6HmGWX8tsz0f |
| TLSH: | DAB3C71E3E218F7EF7ACC23847B74A21975923D527F0D185D16CE9015EA038E646FBA8 |
| File Content Preview: | .ELF.....@.`...4.....4. ...(.....@...@.....E...E..... ..8.....dt.Q.....<...'.6....!'.....<...'.6....!... ....'9... ..... <...'.6h...!.....'9. |

### Static ELF Info

#### ELF header

| | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, big 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: | 113796 |
| Section Header Size: | 40 |
| Number of Section Headers: | 14 |
| Header String Table Index: | 13 |

### Sections

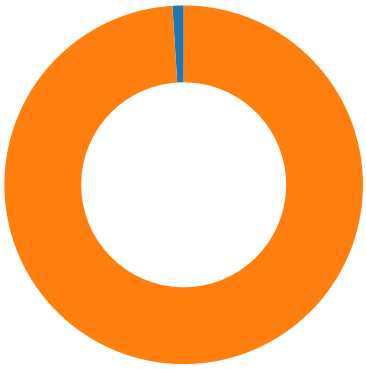
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x400094 | 0x94 | 0x8c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .text | PROGBITS | 0x400120 | 0x120 | 0x18a60 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .fini | PROGBITS | 0x418b80 | 0x18b80 | 0x5c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .rodata | PROGBITS | 0x418be0 | 0x18be0 | 0x22c0 | 0x0 | 0x2 | A | 0 | 0 | 16 |
| .ctors | PROGBITS | 0x45b000 | 0x1b000 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x45b008 | 0x1b008 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data.rel.ro | PROGBITS | 0x45b014 | 0x1b014 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x45b020 | 0x1b020 | 0x740 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .got | PROGBITS | 0x45b760 | 0x1b760 | 0x4c0 | 0x4 | 0x10000003 | WAp | 0 | 0 | 16 |
| .sbss | NOBITS | 0x45bc20 | 0x1bc20 | 0x24 | 0x0 | 0x10000003 | WAp | 0 | 0 | 4 |
| .bss | NOBITS | 0x45bc50 | 0x1bc20 | 0x2c40 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .mdebug.abi32 | PROGBITS | 0x936 | 0x1bc20 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 1 |
| .shstrtab | STRTAB | 0x0 | 0x1bc20 | 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 | 0x1aea0 | 0x1aea0 | 5.6407 | 0x5 | R E | 0x10000 | | .init .text .fini .rodata |
| LOAD | 0x1b000 | 0x45b000 | 0x45b000 | 0xc20 | 0x3890 | 4.7909 | 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



**Total Packets: 100**

- 23 (Telnet)
- 443 (HTTPS)

### TCP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Aug 6, 2022 06:34:30.984601974 CEST | 192.168.2.23 | 8.8.8.8 | 0x4c95 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:33.042846918 CEST | 192.168.2.23 | 8.8.8.8 | 0xa3ee | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:38.091512918 CEST | 192.168.2.23 | 8.8.8.8 | 0x41a | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:43.161137104 CEST | 192.168.2.23 | 8.8.8.8 | 0xfa2f | 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 06:34:50.209662914 CEST | 192.168.2.23 | 8.8.8.8 | 0x37e6 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:52.255748034 CEST | 192.168.2.23 | 8.8.8.8 | 0x5d33 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:02.321718931 CEST | 192.168.2.23 | 8.8.8.8 | 0xdfde | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:08.369952917 CEST | 192.168.2.23 | 8.8.8.8 | 0xf05a | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:13.417853117 CEST | 192.168.2.23 | 8.8.8.8 | 0x5135 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:16.467514992 CEST | 192.168.2.23 | 8.8.8.8 | 0x2756 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:18.513750076 CEST | 192.168.2.23 | 8.8.8.8 | 0xdf13 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:22.562899113 CEST | 192.168.2.23 | 8.8.8.8 | 0x8306 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:23.613262892 CEST | 192.168.2.23 | 8.8.8.8 | 0xe356 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:31.661303043 CEST | 192.168.2.23 | 8.8.8.8 | 0x5c | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:36.709366083 CEST | 192.168.2.23 | 8.8.8.8 | 0xca89 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:42.755481005 CEST | 192.168.2.23 | 8.8.8.8 | 0x83e8 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:52.801347017 CEST | 192.168.2.23 | 8.8.8.8 | 0xc49 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:02.850513935 CEST | 192.168.2.23 | 8.8.8.8 | 0xa4e2 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:07.915524960 CEST | 192.168.2.23 | 8.8.8.8 | 0x5e02 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:13.966692924 CEST | 192.168.2.23 | 8.8.8.8 | 0xd380 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:21.015851974 CEST | 192.168.2.23 | 8.8.8.8 | 0x991d | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:26.064208984 CEST | 192.168.2.23 | 8.8.8.8 | 0x5735 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:34.109294891 CEST | 192.168.2.23 | 8.8.8.8 | 0xbdab | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:39.158842087 CEST | 192.168.2.23 | 8.8.8.8 | 0x9986 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:42.231399059 CEST | 192.168.2.23 | 8.8.8.8 | 0xa808 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:43.279979944 CEST | 192.168.2.23 | 8.8.8.8 | 0xbbb9 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:50.325704098 CEST | 192.168.2.23 | 8.8.8.8 | 0xa579 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:51.374264002 CEST | 192.168.2.23 | 8.8.8.8 | 0xc2b8 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:59.423377991 CEST | 192.168.2.23 | 8.8.8.8 | 0x3c6 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:01.480495930 CEST | 192.168.2.23 | 8.8.8.8 | 0xdf0e | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:02.529299021 CEST | 192.168.2.23 | 8.8.8.8 | 0x7f1d | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:07.579133034 CEST | 192.168.2.23 | 8.8.8.8 | 0xb33d | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:13.629314899 CEST | 192.168.2.23 | 8.8.8.8 | 0xc8b | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:15.677565098 CEST | 192.168.2.23 | 8.8.8.8 | 0x3cb | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:18.500262976 CEST | 192.168.2.23 | 8.8.8.8 | 0x4c95 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:20.548906088 CEST | 192.168.2.23 | 8.8.8.8 | 0xa3ee | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:24.725655079 CEST | 192.168.2.23 | 8.8.8.8 | 0x2e44 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:25.595376015 CEST | 192.168.2.23 | 8.8.8.8 | 0x41a | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:30.642967939 CEST | 192.168.2.23 | 8.8.8.8 | 0xfa2f | 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 06:37:30.774873972 CEST | 192.168.2.23 | 8.8.8.8 | 0x8de6 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:32.823848963 CEST | 192.168.2.23 | 8.8.8.8 | 0x90a8 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:35.906585932 CEST | 192.168.2.23 | 8.8.8.8 | 0x8312 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:37.691096067 CEST | 192.168.2.23 | 8.8.8.8 | 0x37e6 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:39.741597891 CEST | 192.168.2.23 | 8.8.8.8 | 0x5d33 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:43.955291033 CEST | 192.168.2.23 | 8.8.8.8 | 0xb738 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:48.004853010 CEST | 192.168.2.23 | 8.8.8.8 | 0xfab1 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:48.789915085 CEST | 192.168.2.23 | 8.8.8.8 | 0xdfde | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:53.053350925 CEST | 192.168.2.23 | 8.8.8.8 | 0xf4b0 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:54.849728107 CEST | 192.168.2.23 | 8.8.8.8 | 0xf05a | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:59.908838987 CEST | 192.168.2.23 | 8.8.8.8 | 0x5135 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:02.978688002 CEST | 192.168.2.23 | 8.8.8.8 | 0x2756 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:03.101815939 CEST | 192.168.2.23 | 8.8.8.8 | 0xd947 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:05.055260897 CEST | 192.168.2.23 | 8.8.8.8 | 0xdf13 | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:05.150703907 CEST | 192.168.2.23 | 8.8.8.8 | 0x80 | 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 06:34:31.012761116 CEST | 8.8.8.8 | 192.168.2.23 | 0x4c95 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:33.062582970 CEST | 8.8.8.8 | 192.168.2.23 | 0xa3ee | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:38.110887051 CEST | 8.8.8.8 | 192.168.2.23 | 0x41a | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:43.178842068 CEST | 8.8.8.8 | 192.168.2.23 | 0xfa2f | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:50.227161884 CEST | 8.8.8.8 | 192.168.2.23 | 0x37e6 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:34:52.275523901 CEST | 8.8.8.8 | 192.168.2.23 | 0x5d33 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:02.341381073 CEST | 8.8.8.8 | 192.168.2.23 | 0xdfde | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:08.389444113 CEST | 8.8.8.8 | 192.168.2.23 | 0xf05a | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:13.437644005 CEST | 8.8.8.8 | 192.168.2.23 | 0x5135 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:16.485018015 CEST | 8.8.8.8 | 192.168.2.23 | 0x2756 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:18.533694029 CEST | 8.8.8.8 | 192.168.2.23 | 0xdf13 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:22.580888987 CEST | 8.8.8.8 | 192.168.2.23 | 0x8306 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:23.632677078 CEST | 8.8.8.8 | 192.168.2.23 | 0xe356 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:31.678518057 CEST | 8.8.8.8 | 192.168.2.23 | 0x5c | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:36.726804018 CEST | 8.8.8.8 | 192.168.2.23 | 0xca89 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:42.772620916 CEST | 8.8.8.8 | 192.168.2.23 | 0x83e8 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:35:52.820950031 CEST | 8.8.8.8 | 192.168.2.23 | 0xc49 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:02.868339062 CEST | 8.8.8.8 | 192.168.2.23 | 0xa4e2 | 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 06:36:07.935823917 CEST | 8.8.8.8 | 192.168.2.23 | 0x5e02 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:13.986347914 CEST | 8.8.8.8 | 192.168.2.23 | 0xd380 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:21.035554886 CEST | 8.8.8.8 | 192.168.2.23 | 0x991d | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:26.081285954 CEST | 8.8.8.8 | 192.168.2.23 | 0x5735 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:34.130255938 CEST | 8.8.8.8 | 192.168.2.23 | 0xbdab | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:39.176071882 CEST | 8.8.8.8 | 192.168.2.23 | 0x9986 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:42.251230955 CEST | 8.8.8.8 | 192.168.2.23 | 0xa808 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:43.297199965 CEST | 8.8.8.8 | 192.168.2.23 | 0xbbb9 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:50.345362902 CEST | 8.8.8.8 | 192.168.2.23 | 0xa579 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:51.394253969 CEST | 8.8.8.8 | 192.168.2.23 | 0xc2b8 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:36:59.451746941 CEST | 8.8.8.8 | 192.168.2.23 | 0x3c6 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:01.499841928 CEST | 8.8.8.8 | 192.168.2.23 | 0xdf0e | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:02.546760082 CEST | 8.8.8.8 | 192.168.2.23 | 0x7f1d | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:07.599052906 CEST | 8.8.8.8 | 192.168.2.23 | 0xb33d | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:13.648916006 CEST | 8.8.8.8 | 192.168.2.23 | 0xc8b | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:15.697153091 CEST | 8.8.8.8 | 192.168.2.23 | 0x3cb | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:18.517447948 CEST | 8.8.8.8 | 192.168.2.23 | 0x4c95 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:20.566694021 CEST | 8.8.8.8 | 192.168.2.23 | 0xa3ee | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:24.744548082 CEST | 8.8.8.8 | 192.168.2.23 | 0x2e44 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:25.612651110 CEST | 8.8.8.8 | 192.168.2.23 | 0x41a | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:30.661705971 CEST | 8.8.8.8 | 192.168.2.23 | 0xfa2f | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:30.794035912 CEST | 8.8.8.8 | 192.168.2.23 | 0x8de6 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:32.843652964 CEST | 8.8.8.8 | 192.168.2.23 | 0x90a8 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:35.926378012 CEST | 8.8.8.8 | 192.168.2.23 | 0x8312 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:37.710695028 CEST | 8.8.8.8 | 192.168.2.23 | 0x37e6 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:39.760700941 CEST | 8.8.8.8 | 192.168.2.23 | 0x5d33 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:43.974637032 CEST | 8.8.8.8 | 192.168.2.23 | 0xb738 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:48.024336100 CEST | 8.8.8.8 | 192.168.2.23 | 0xfab1 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:48.809528112 CEST | 8.8.8.8 | 192.168.2.23 | 0xdfde | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:53.073667049 CEST | 8.8.8.8 | 192.168.2.23 | 0xf4b0 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:54.871546030 CEST | 8.8.8.8 | 192.168.2.23 | 0xf05a | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:37:59.927725077 CEST | 8.8.8.8 | 192.168.2.23 | 0x5135 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:03.026779890 CEST | 8.8.8.8 | 192.168.2.23 | 0x2756 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:03.121298075 CEST | 8.8.8.8 | 192.168.2.23 | 0xd947 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |
| Aug 6, 2022 06:38:05.074727058 CEST | 8.8.8.8 | 192.168.2.23 | 0xdf13 | 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 06:38:05.167964935 CEST | 8.8.8.8 | 192.168.2.23 | 0x80 | No error (0) | arcticboatz.cz | | 46.23.109.40 | A (IP address) | IN (0x0001) |

## System Behavior

### Analysis Process: 9aDl048Kv4 PID: **6230**, Parent PID: **6125**

#### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | /tmp/9aDl048Kv4 |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

#### File Activities

**File Read**

### Analysis Process: 9aDl048Kv4 PID: **6233**, Parent PID: **6230**

#### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### Analysis Process: 9aDl048Kv4 PID: **6234**, Parent PID: **6230**

#### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### Analysis Process: 9aDl048Kv4 PID: **6235**, Parent PID: **6230**

#### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### Analysis Process: 9aDl048Kv4 PID: **6237**, Parent PID: **6230**

#### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

## Analysis Process: 9aDl048Kv4 PID: **6242**, Parent PID: **6237**

### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### File Activities

**File Read**

**Directory Enumerated**

## Analysis Process: 9aDl048Kv4 PID: **6330**, Parent PID: **6242**

### General

| | |
|---|---|
| Start time: | 06:37:17 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

## Analysis Process: 9aDl048Kv4 PID: **6243**, Parent PID: **6237**

### General

| | |
|---|---|
| Start time: | 06:34:29 |
| Start date: | 06/08/2022 |
| Path: | /tmp/9aDl048Kv4 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |