


**ID:** 829688
**Sample Name:** foxhAjDt.elf
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 21:15:10
**Date:** 18/03/2023
**Version:** 37.0.0 Beryl

# Table of Contents

# Linux Analysis Report

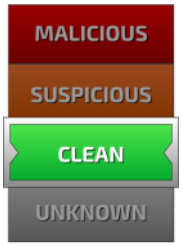
## foxhAjDt.elf

## Overview

### General Information

| | |
|---|---|
| Sample Name: | foxhAjDt.elf |
| Analysis ID: | 829688 |
| MD5: | 7de222fa7927d.. |
| SHA1: | 15404b19eda9... |
| SHA256: | d9bd1932dad0... |
| Tags: | elf |
| Infos: | |

### Detection

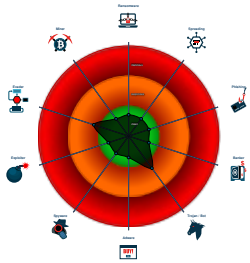



| | |
|---|---|
| Score: | 2 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- 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...

### 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: | 37.0.0 Beryl |
| Analysis ID: | 829688 |
| Start date and time: | 2023-03-18 21:15:10 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 8s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| 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 |
| Sample file name: | foxhAjDt.elf |
| Detection: | CLEAN |
| Classification: | clean2.linELF@0/0@0/0 |

## Runtime Messages

| | |
|---|---|
| Command: | /tmp/foxhAjDt.elf |
| PID: | 6227 |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | |
| Standard Error: | |

## Process Tree

- **system is lnxubuntu20**
- foxhAjDt.elf (PID: 6227, Parent: 6126, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/foxhAjDt.elf
  - foxhAjDt.elf New Fork (PID: 6229, Parent: 6227)
- **cleanup**

## Yara Signatures

**No yara matches**

## Snort Signatures

**No Snort rule has matched**

## Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

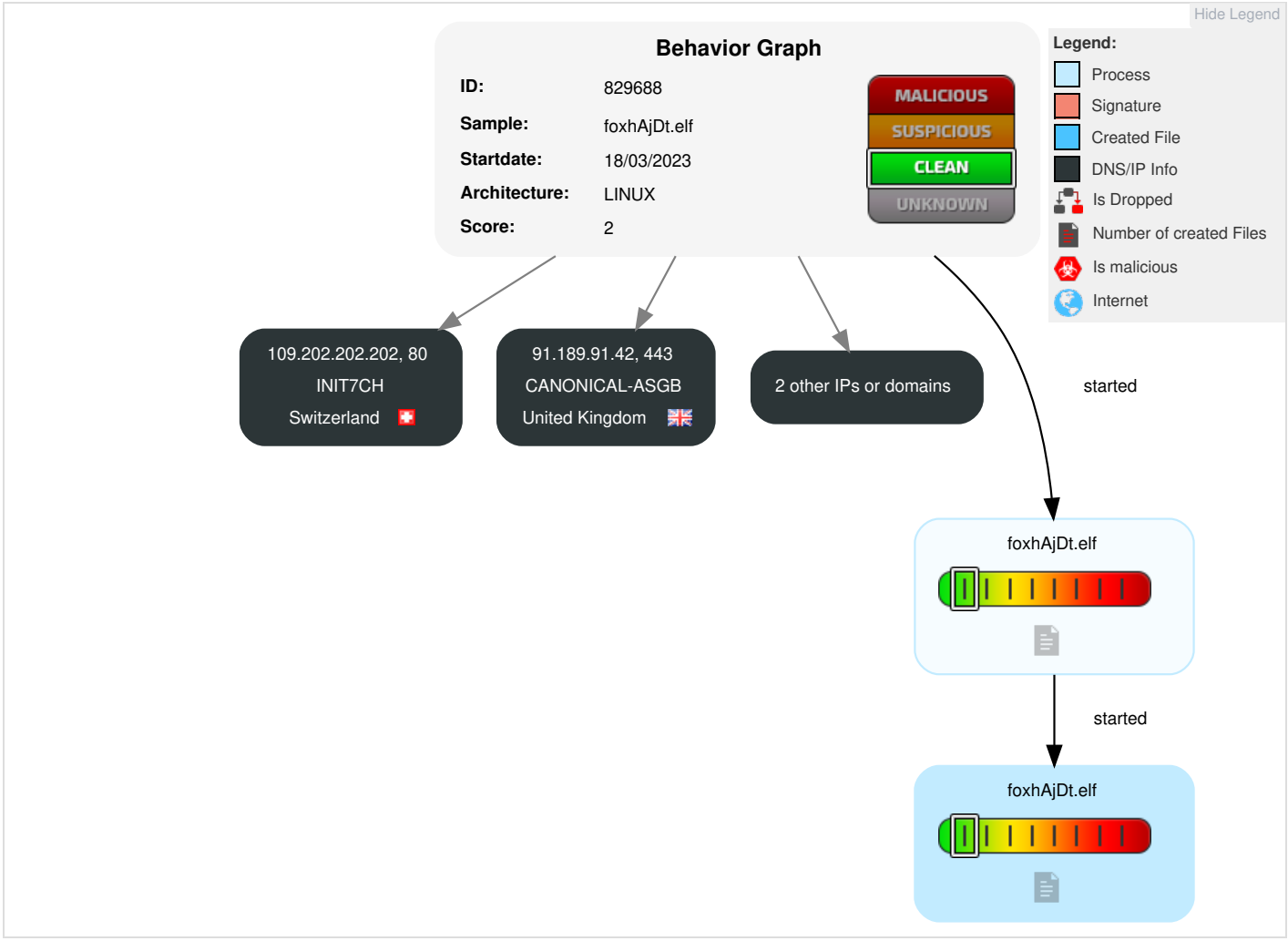
## Mitre Att&ck Matrix

| 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 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 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |

## Malware Configuration

**No configs have been found**

## Behavior Graph




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| foxhAjDt.elf | 3% | ReversingLabs | Linux.Malware.Bot Attack | |
| foxhAjDt.elf | 7% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

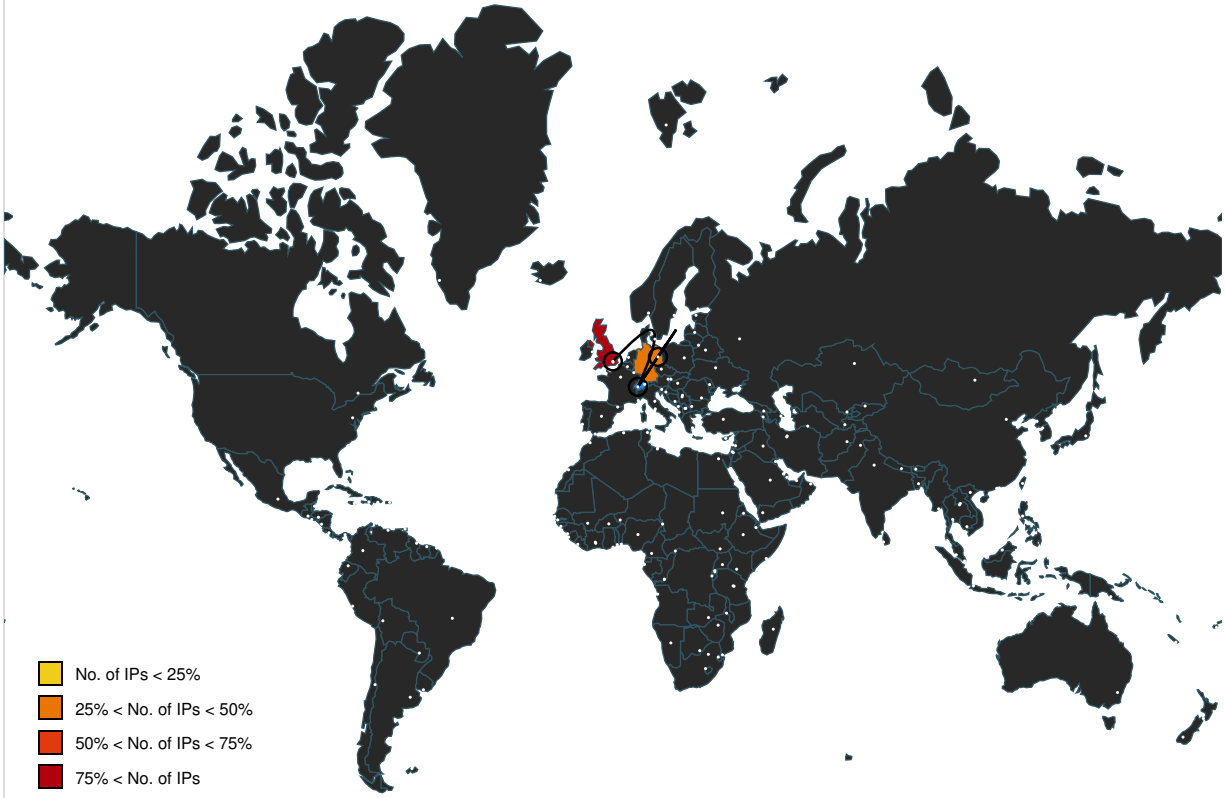
## Domains and IPs

### Contacted Domains

No contacted domains info

## URLs from Memory and Binaries

## World Map of Contacted IPs




### Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 109.202.202.202 | unknown | Switzerland | | 13030 | INIT7CH | false |
| 193.35.18.163 | unknown | Germany | | 41865 | BIALLNET-ASPL | false |
| 91.189.91.43 | unknown | United Kingdom | | 41231 | CANONICAL-ASGB | false |
| 91.189.91.42 | unknown | United Kingdom | | 41231 | CANONICAL-ASGB | 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, EABI5 version 1 (SYSV), statically linked, for GNU/Linux 3.2.0, stripped |
| Entropy (8bit): | 6.043235002426273 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | foxhAjDt.elf |
| File size: | 1243604 |
| MD5: | 7de222fa7927d27a83d855608d8f9e6f |
| SHA1: | 15404b19eda9a90043316ba255811e84bbb221b8 |
| SHA256: | d9bd1932dad08061e9cfecdc42bc4cbb3eec506ab54f4d889d6ae523d8249324 |
| SHA512: | 98faa3fe286a0c0402e76b86ecad77391987557a93633cae3d13b608cf5b2f8eac168943b6878b8b734f4b2e6bc92269bd9bace136ba47df0aa8e2c508153290 |
| SSDEEP: | 24576:XdEysUzziBk0P5yfuwiP6qCU59WdTxDy8g:tVsUcgWu9 |
| TLSH: | 72452A4AF4819F65C9E536BBF25D478833461775C2EA220AAD2087343FDECAE0E79741 |
| File Content Preview: | .ELF.....(.....p]..4.....4. ...(. .....4...4...4...`...`.....d]..d].....p]..p]..p]...M...M.....7...7.....a.....8...p.....R.td..... |

### Static ELF Info

#### ELF header

| | |
|---|---|
| Class: | |
| Data: | |
| Version: | |
| Machine: | |
| Version Number: | |
| Type: | |
| OS/ABI: | |
| ABI Version: | |
| Entry Point Address: | |
| Flags: | |
| ELF Header Size: | |
| Program Header Offset: | |
| Program Header Size: | |
| Number of Program Headers: | |
| Section Header Offset: | |
| Section Header Size: | |
| Number of Section Headers: | |
| Header String Table Index: | |

### Sections

| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .note.ABI-tag | NOTE | 0x10194 | 0x194 | 0x20 | 0x0 | 0x2 | A | 0 | 0 | 4 |
| .ARM.exidx | ARM_EXIDX | 0x101b4 | 0x1b4 | 0x4228 | 0x0 | 0x82 | AL | 10 | 0 | 4 |
| .rel.dyn | REL | 0x143dc | 0x43dc | 0x8 | 0x8 | 0x42 | AI | 0 | 19 | 4 |
| .rodata | PROGBITS | 0x143e8 | 0x43e8 | 0x1c898 | 0x0 | 0x32 | AMS | 0 | 0 | 8 |
| .ARM.extab | PROGBITS | 0x30c80 | 0x20c80 | 0x4d34 | 0x0 | 0x2 | A | 0 | 0 | 4 |
| __libc_IO_vtables | PROGBITS | 0x359b4 | 0x259b4 | 0x39c | 0x0 | 0x2 | A | 0 | 0 | 4 |
| __libc_atexit | PROGBITS | 0x35d50 | 0x25d50 | 0x4 | 0x0 | 0x2 | A | 0 | 0 | 4 |
| .eh_frame_hdr | PROGBITS | 0x35d54 | 0x25d54 | 0xc | 0x0 | 0x2 | A | 0 | 0 | 4 |
| .eh_frame | PROGBITS | 0x35d60 | 0x25d60 | 0x4 | 0x0 | 0x2 | A | 0 | 0 | 4 |

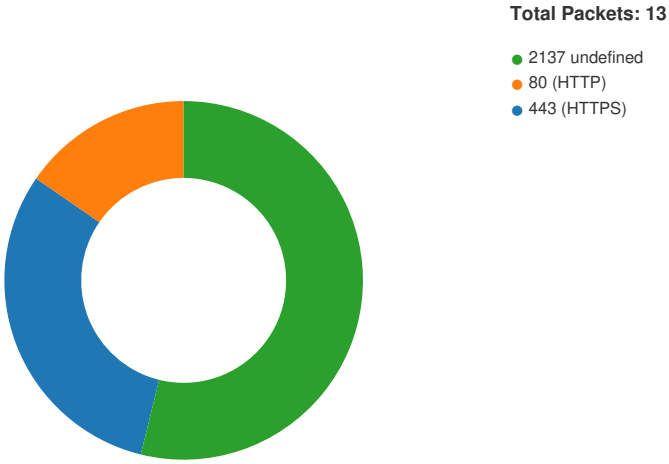
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| .text | PROGBITS | 0x45d70 | 0x25d70 | 0x104d64 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .init | PROGBITS | 0x14aad4 | 0x12aad4 | 0xc | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .fini | PROGBITS | 0x14aae0 | 0x12aae0 | 0x8 | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .iplt | PROGBITS | 0x14aaf0 | 0x12aaf0 | 0x10 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .tdata | PROGBITS | 0x15ab00 | 0x12ab00 | 0x38 | 0x0 | 0x403 | WAT | 0 | 0 | 4 |
| .tbss | NOBITS | 0x15ab38 | 0x12ab38 | 0x38 | 0x0 | 0x403 | WAT | 0 | 0 | 4 |
| .init_array | INIT_ARRAY | 0x15ab38 | 0x12ab38 | 0x28 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .fini_array | FINI_ARRAY | 0x15ab60 | 0x12ab60 | 0x8 | 0x4 | 0x3 | WA | 0 | 0 | 4 |
| .data.rel.ro | PROGBITS | 0x15ab68 | 0x12ab68 | 0x30e8 | 0x0 | 0x3 | WA | 0 | 0 | 8 |
| .got | PROGBITS | 0x15dc50 | 0x12dc50 | 0x648 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x16e298 | 0x12e298 | 0xeac | 0x0 | 0x3 | WA | 0 | 0 | 8 |
| .tm_clone_table | PROGBITS | 0x16f144 | 0x12f144 | 0x0 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .bss | NOBITS | 0x16f148 | 0x12f144 | 0x52c0 | 0x0 | 0x3 | WA | 0 | 0 | 8 |
| __libc_freeres_ptrs | NOBITS | 0x174408 | 0x12f144 | 0x1c | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .ARM.attributes | ARM_ATTRIBUTES | 0x0 | 0x12f144 | 0x2b | 0x0 | 0x0 | | 0 | 0 | 1 |
| .comment | PROGBITS | 0x0 | 0x12f16f | 0x50 | 0x1 | 0x30 | MS | 0 | 0 | 1 |
| .gnu.warning.pthread_attr_getstackaddr | PROGBITS | 0x0 | 0x12f1c0 | 0x52 | 0x0 | 0x0 | | 0 | 0 | 4 |
| .gnu.warning.pthread_attr_setstackaddr | PROGBITS | 0x0 | 0x12f214 | 0x52 | 0x0 | 0x0 | | 0 | 0 | 4 |
| .gnu.warning.sys_errlist | PROGBITS | 0x0 | 0x12f268 | 0x44 | 0x0 | 0x0 | | 0 | 0 | 4 |
| .gnu.warning.sys_nerr | PROGBITS | 0x0 | 0x12f2ac | 0x41 | 0x0 | 0x0 | | 0 | 0 | 4 |
| .gnu.warning.mktemp | PROGBITS | 0x0 | 0x12f2f0 | 0x44 | 0x0 | 0x0 | | 0 | 0 | 4 |
| .shstrtab | STRTAB | 0x0 | 0x12f334 | 0x1a0 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PHDR | 0x34 | 0x10034 | 0x10034 | 0x160 | 0x160 | 2.9369 | 0x4 | R | 0x4 | | |
| LOAD | 0x0 | 0x10000 | 0x10000 | 0x25d64 | 0x25d64 | 4.9877 | 0x4 | R | 0x10000 | | .note.ABI-tag .ARM.exidx .rel.dyn .rodata .ARM.extab __libc_IO_vtables __libc_atexit .eh_frame_hdr .eh_frame |
| LOAD | 0x25d70 | 0x45d70 | 0x45d70 | 0x104d90 | 0x104d90 | 6.0329 | 0x5 | R E | 0x10000 | | .text .init .fini .iplt |
| LOAD | 0x12ab00 | 0x15ab00 | 0x15ab00 | 0x3798 | 0x3798 | 4.7289 | 0x6 | RW | 0x10000 | | .tdata .tbss .init_array .fini_array .data.rel.ro .got |
| LOAD | 0x12e298 | 0x16e298 | 0x16e298 | 0xeac | 0x618c | 1.6272 | 0x6 | RW | 0x10000 | | .data .bss __libc_freeres_ptrs |
| TLS | 0x12ab00 | 0x15ab00 | 0x15ab00 | 0x38 | 0x70 | 3.1136 | 0x4 | R | 0x4 | | .tdata .tbss |
| GNU_RELRO | 0x12ab00 | 0x15ab00 | 0x15ab00 | 0x3798 | 0x4500 | 4.7289 | 0x4 | R | 0x1 | | .tdata .tbss .init_array .fini_array .data.rel.ro .got |
| GNU_EH_FRAME | 0x25d54 | 0x35d54 | 0x35d54 | 0xc | 0xc | 1.9473 | 0x4 | R | 0x4 | | .eh_frame_hdr |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x0 | | |
| NOTE | 0x194 | 0x10194 | 0x10194 | 0x20 | 0x20 | 1.5613 | 0x4 | R | 0x4 | | .note.ABI-tag |
| EXIDX | 0x1b4 | 0x101b4 | 0x101b4 | 0x4228 | 0x4228 | 5.1719 | 0x4 | R | 0x4 | | .ARM.exidx |

## Network Behavior

### Network Port Distribution




**TCP Packets**

## System Behavior

### Analysis Process: foxhAjDt.elf PID: 6227, Parent PID: 6126

**General**

| | |
|---|---|
| Start time: | 21:15:56 |
| Start date: | 18/03/2023 |
| Path: | /tmp/foxhAjDt.elf |
| Arguments: | /tmp/foxhAjDt.elf |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

**File Activities**

**File Read**

### Analysis Process: foxhAjDt.elf PID: 6229, Parent PID: 6227

**General**

| | |
|---|---|
| Start time: | 21:15:56 |
| Start date: | 18/03/2023 |
| Path: | /tmp/foxhAjDt.elf |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

**File Activities**

**File Read**

**Directory Enumerated**