
**ID:** 511557
**Sample Name:** 3tgXa7CGc1
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 09:44:55
**Date:** 29/10/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

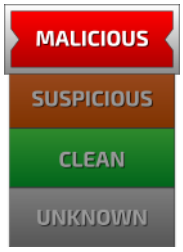
# Linux Analysis Report 3tgXa7CGc1

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 3tgXa7CGc1 |
| Analysis ID: | 511557 |
| MD5: | 3ca11c21956b7c… |
| SHA1: | d26f991c4df35a7.. |
| SHA256: | ddfb21fd0f3589e… |
| Tags: | 32 elf mips |
| Infos: | |

### Detection

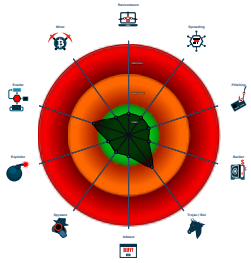



| | |
|---|---|
| Score: | 48 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Multi AV Scanner detection for subm…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- 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 only run correctly on MIPS or ARM architectures**

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

**Static ELF header machine description suggests that the sample might not execute correctly on this machine**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 511557 |
| Start date: | 29.10.2021 |
| Start time: | 09:44:55 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 4m 48s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 3tgXa7CGc1 |
| 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: | mal48.lin@0/0@0/0 |

## Process Tree

- **system is lnxubuntu20**
  - 3tgXa7CGc1 (PID: 5236, Parent: 5113, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/3tgXa7CGc1
    - 3tgXa7CGc1 New Fork (PID: 5238, Parent: 5236)
- **cleanup**

## Yara Overview

**No yara matches**

## Jbx Signature Overview

- AV Detection
- Networking
- System Summary
- Malware Analysis System Evasion

Click to jump to signature section

**AV Detection:**

**Multi AV Scanner detection for submitted file**

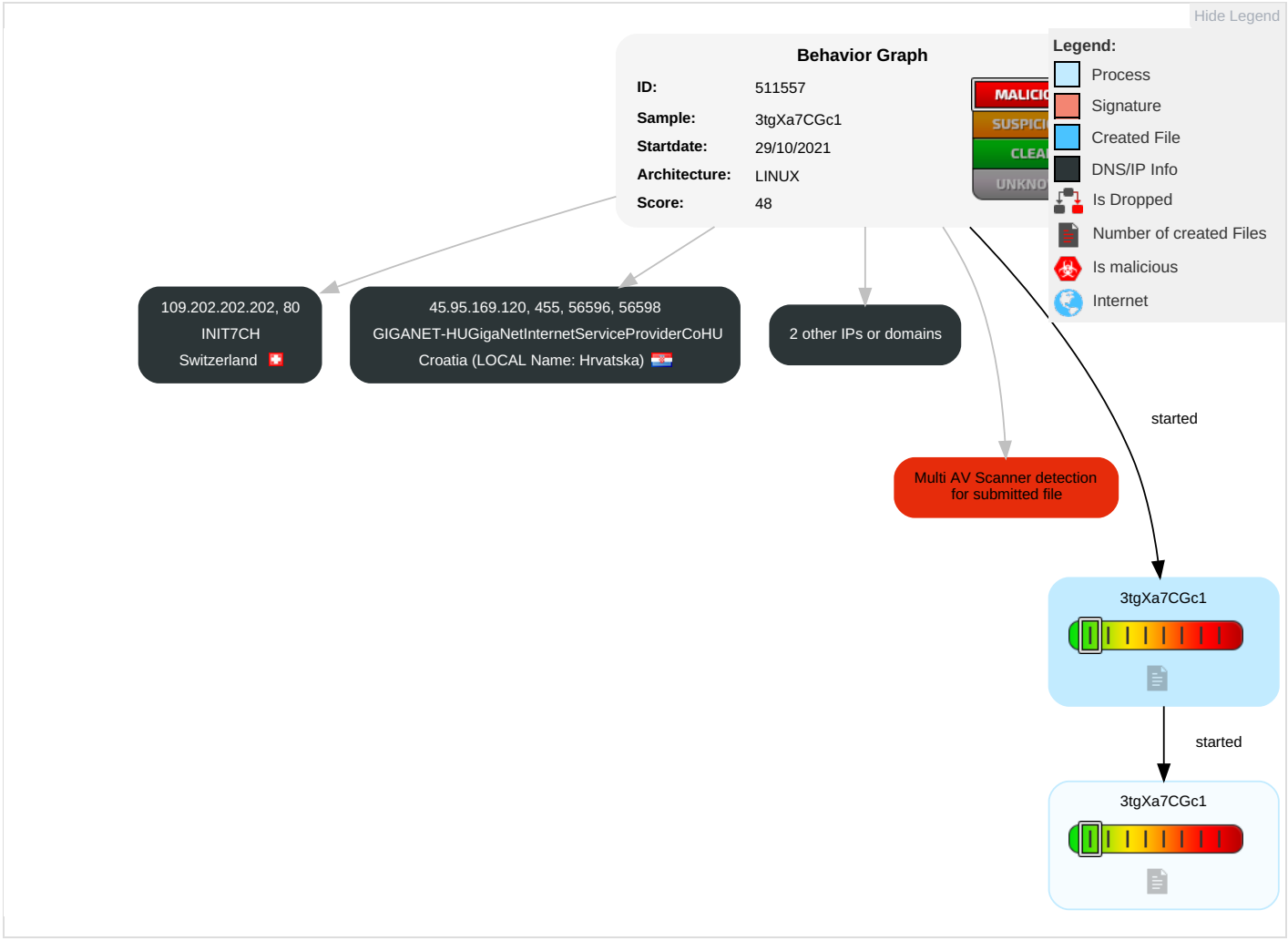
## Mitre Att&ck Matrix

| 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 | OS Credential Dumping | Security Software Discovery 1 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 1 | 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 | Non-Standard Port 1 | 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 | Application Layer Protocol 1 | 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 |
|---|---|---|---|---|
| 3tgXa7CGc1 | 25% | Virustotal | | Browse |
| 3tgXa7CGc1 | 27% | ReversingLabs | Linux.Trojan.Mirai | |

## Dropped Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 45.95.169.120 | unknown | Croatia (LOCAL Name: Hrvatska) | | 42864 | GIGANET-HUGigaNetInternetServiceProviderCoHU | false |
| 109.202.202.202 | unknown | Switzerland | | 13030 | INIT7CH | false |
| 91.189.91.43 | unknown | United Kingdom | | 41231 | CANONICAL-ASGB | false |
| 91.189.91.42 | unknown | United Kingdom | | 41231 | CANONICAL-ASGB | false |

## Runtime Messages

| | |
|---|---|
| Command: | /tmp/3tgXa7CGc1 |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | |
| Standard Error: | |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 45.95.169.120 | rijsTqU0lf | Get hash | malicious | Browse | |
| | csB31kWt10 | Get hash | malicious | Browse | |
| | QWg2NTuodY | Get hash | malicious | Browse | |
| | SL92Sz9pl2 | Get hash | malicious | Browse | |
| | YpKL484IG5 | Get hash | malicious | Browse | |
| | Y4W4j5QIqD | Get hash | malicious | Browse | |
| | 1TnmkstVG8 | Get hash | malicious | Browse | |
| | iksM5QEg2j | Get hash | malicious | Browse | |
| 109.202.202.202 | rijsTqU0lf | Get hash | malicious | Browse | |
| | csB31kWt10 | Get hash | malicious | Browse | |
| | QWg2NTuodY | Get hash | malicious | Browse | |
| | 6VLeGqFkPS | Get hash | malicious | Browse | |
| | DL5blLw1ly | Get hash | malicious | Browse | |
| | SL92Sz9pl2 | Get hash | malicious | Browse | |
| | YpKL484IG5 | Get hash | malicious | Browse | |
| | Y4W4j5QIqD | Get hash | malicious | Browse | |
| | 1TnmkstVG8 | Get hash | malicious | Browse | |
| | iksM5QEg2j | Get hash | malicious | Browse | |
| | lGJEkz80oe | Get hash | malicious | Browse | |
| | roV7kGaVr1 | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Linux.Siggen.4218.298.3210 | Get hash | malicious | Browse | |
| | uPOWBxniTA | Get hash | malicious | Browse | |
| | qy5unieRgR | Get hash | malicious | Browse | |
| | sAzPpn6mKZ | Get hash | malicious | Browse | |
| | AxadDC89j9 | Get hash | malicious | Browse | |
| | ZErnXU2XR1 | Get hash | malicious | Browse | |
| | sTHJvS5LPJ | Get hash | malicious | Browse | |
| | THzHjYQ4z6 | Get hash | malicious | Browse | |
| 91.189.91.43 | rijsTqU0lf | Get hash | malicious | Browse | |
| | csB31kWt10 | Get hash | malicious | Browse | |
| | QWg2NTuodY | Get hash | malicious | Browse | |
| | 6VLeGqFkPS | Get hash | malicious | Browse | |
| | DL5blLw1ly | Get hash | malicious | Browse | |
| | SL92Sz9pl2 | Get hash | malicious | Browse | |
| | YpKL484IG5 | Get hash | malicious | Browse | |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Y4W4j5QIqD | Get hash | malicious | Browse | |
| | 1TnmkstVG8 | Get hash | malicious | Browse | |
| | iksM5QEg2j | Get hash | malicious | Browse | |
| | lGJEkz80oe | Get hash | malicious | Browse | |
| | roV7kGaVr1 | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Linux.Siggen.4218.298.3210 | Get hash | malicious | Browse | |
| | uPOWBxniTA | Get hash | malicious | Browse | |
| | qy5unieRgR | Get hash | malicious | Browse | |
| | sAzPpn6mKZ | Get hash | malicious | Browse | |
| | AxadDC89j9 | Get hash | malicious | Browse | |
| | ZErnXU2XR1 | Get hash | malicious | Browse | |
| | sTHJvS5LPJ | Get hash | malicious | Browse | |
| | THzHjYQ4z6 | Get hash | malicious | Browse | |
| 91.189.91.42 | rijsTqU0lf | Get hash | malicious | Browse | |
| | csB31kWt10 | Get hash | malicious | Browse | |
| | QWg2NTuodY | Get hash | malicious | Browse | |
| | 6VLeGqFkPS | Get hash | malicious | Browse | |
| | DL5blLw1ly | Get hash | malicious | Browse | |
| | SL92Sz9pl2 | Get hash | malicious | Browse | |
| | YpKL484IG5 | Get hash | malicious | Browse | |
| | Y4W4j5QIqD | Get hash | malicious | Browse | |
| | 1TnmkstVG8 | Get hash | malicious | Browse | |
| | iksM5QEg2j | Get hash | malicious | Browse | |
| | lGJEkz80oe | Get hash | malicious | Browse | |
| | roV7kGaVr1 | Get hash | malicious | Browse | |
| | SecuriteInfo.com.Linux.Siggen.4218.298.3210 | Get hash | malicious | Browse | |
| | uPOWBxniTA | Get hash | malicious | Browse | |
| | qy5unieRgR | Get hash | malicious | Browse | |
| | sAzPpn6mKZ | Get hash | malicious | Browse | |
| | AxadDC89j9 | Get hash | malicious | Browse | |
| | ZErnXU2XR1 | Get hash | malicious | Browse | |
| | sTHJvS5LPJ | Get hash | malicious | Browse | |
| | THzHjYQ4z6 | Get hash | malicious | Browse | |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| CANONICAL-ASGB | rijsTqU0lf | Get hash | malicious | Browse | • 91.189.91.42 |
| | csB31kWt10 | Get hash | malicious | Browse | • 91.189.91.42 |
| | QWg2NTuodY | Get hash | malicious | Browse | • 91.189.91.42 |
| | 6VLeGqFkPS | Get hash | malicious | Browse | • 91.189.91.42 |
| | DL5blLw1ly | Get hash | malicious | Browse | • 91.189.91.42 |
| | SL92Sz9pl2 | Get hash | malicious | Browse | • 91.189.91.42 |
| | YpKL484IG5 | Get hash | malicious | Browse | • 91.189.91.42 |
| | Y4W4j5QIqD | Get hash | malicious | Browse | • 91.189.91.42 |
| | 1TnmkstVG8 | Get hash | malicious | Browse | • 91.189.91.42 |
| | iksM5QEg2j | Get hash | malicious | Browse | • 91.189.91.42 |
| | lGJEkz80oe | Get hash | malicious | Browse | • 91.189.91.42 |
| | roV7kGaVr1 | Get hash | malicious | Browse | • 91.189.91.42 |
| | SecuriteInfo.com.Linux.Siggen.4218.298.3210 | Get hash | malicious | Browse | • 91.189.91.42 |
| | uPOWBxniTA | Get hash | malicious | Browse | • 91.189.91.42 |
| | qy5unieRgR | Get hash | malicious | Browse | • 91.189.91.42 |
| | sAzPpn6mKZ | Get hash | malicious | Browse | • 91.189.91.42 |
| | AxadDC89j9 | Get hash | malicious | Browse | • 91.189.91.42 |
| | ZErnXU2XR1 | Get hash | malicious | Browse | • 91.189.91.42 |
| | sTHJvS5LPJ | Get hash | malicious | Browse | • 91.189.91.42 |
| | THzHjYQ4z6 | Get hash | malicious | Browse | • 91.189.91.42 |
| CANONICAL-ASGB | rijsTqU0lf | Get hash | malicious | Browse | • 91.189.91.42 |
| | csB31kWt10 | Get hash | malicious | Browse | • 91.189.91.42 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | QWg2NTuodY | Get hash | malicious | Browse | • 91.189.91.42 |
| | 6VLeGqFkPS | Get hash | malicious | Browse | • 91.189.91.42 |
| | DL5blLw1ly | Get hash | malicious | Browse | • 91.189.91.42 |
| | SL92Sz9pl2 | Get hash | malicious | Browse | • 91.189.91.42 |
| | YpKL484IG5 | Get hash | malicious | Browse | • 91.189.91.42 |
| | Y4W4j5QIqD | Get hash | malicious | Browse | • 91.189.91.42 |
| | 1TnmkstVG8 | Get hash | malicious | Browse | • 91.189.91.42 |
| | iksM5QEg2j | Get hash | malicious | Browse | • 91.189.91.42 |
| | lGJEkz80oe | Get hash | malicious | Browse | • 91.189.91.42 |
| | roV7kGaVr1 | Get hash | malicious | Browse | • 91.189.91.42 |
| | SecuriteInfo.com.Linux.Siggen.4218.298.3210 | Get hash | malicious | Browse | • 91.189.91.42 |
| | uPOWBxniTA | Get hash | malicious | Browse | • 91.189.91.42 |
| | qy5unieRgR | Get hash | malicious | Browse | • 91.189.91.42 |
| | sAzPpn6mKZ | Get hash | malicious | Browse | • 91.189.91.42 |
| | AxadDC89j9 | Get hash | malicious | Browse | • 91.189.91.42 |
| | ZErnXU2XR1 | Get hash | malicious | Browse | • 91.189.91.42 |
| | sTHJvS5LPJ | Get hash | malicious | Browse | • 91.189.91.42 |
| | THzHjYQ4z6 | Get hash | malicious | Browse | • 91.189.91.42 |
| GIGANET-HUGigaNetInternetServiceProviderCoHU | rijsTqU0lf | Get hash | malicious | Browse | • 45.95.169.120 |
| | csB31kWt10 | Get hash | malicious | Browse | • 45.95.169.120 |
| | QWg2NTuodY | Get hash | malicious | Browse | • 45.95.169.120 |
| | SL92Sz9pl2 | Get hash | malicious | Browse | • 45.95.169.120 |
| | YpKL484IG5 | Get hash | malicious | Browse | • 45.95.169.120 |
| | Y4W4j5QIqD | Get hash | malicious | Browse | • 45.95.169.120 |
| | 1TnmkstVG8 | Get hash | malicious | Browse | • 45.95.169.120 |
| | iksM5QEg2j | Get hash | malicious | Browse | • 45.95.169.120 |
| | RicwIfIHLK | Get hash | malicious | Browse | • 45.95.169.115 |
| | aIY7AxjUMc | Get hash | malicious | Browse | • 45.95.169.115 |
| | DtJmFQxtNC | Get hash | malicious | Browse | • 45.95.169.115 |
| | Wm4CzOCmNY | Get hash | malicious | Browse | • 45.95.169.115 |
| | vunWUzXJvC | Get hash | malicious | Browse | • 45.95.169.115 |
| | 52xhBHy9Wz | Get hash | malicious | Browse | • 45.95.169.115 |
| | YGvwG0iCDE | Get hash | malicious | Browse | • 45.95.169.115 |
| | dbd5O0RUTq | Get hash | malicious | Browse | • 45.95.169.115 |
| | fHVDVj0pzO | Get hash | malicious | Browse | • 45.95.169.115 |
| | eZPk7Fg5w7 | Get hash | malicious | Browse | • 45.95.169.115 |
| | ph5PjoFBpj | Get hash | malicious | Browse | • 45.95.169.115 |
| | xugAk5haat | Get hash | malicious | Browse | • 45.95.169.115 |
| INIT7CH | rijsTqU0lf | Get hash | malicious | Browse | • 109.202.202.202 |
| | csB31kWt10 | Get hash | malicious | Browse | • 109.202.202.202 |
| | QWg2NTuodY | Get hash | malicious | Browse | • 109.202.202.202 |
| | 6VLeGqFkPS | Get hash | malicious | Browse | • 109.202.202.202 |
| | DL5blLw1ly | Get hash | malicious | Browse | • 109.202.202.202 |
| | SL92Sz9pl2 | Get hash | malicious | Browse | • 109.202.202.202 |
| | YpKL484IG5 | Get hash | malicious | Browse | • 109.202.202.202 |
| | Y4W4j5QIqD | Get hash | malicious | Browse | • 109.202.202.202 |
| | 1TnmkstVG8 | Get hash | malicious | Browse | • 109.202.202.202 |
| | iksM5QEg2j | Get hash | malicious | Browse | • 109.202.202.202 |
| | lGJEkz80oe | Get hash | malicious | Browse | • 109.202.202.202 |
| | roV7kGaVr1 | Get hash | malicious | Browse | • 109.202.202.202 |
| | SecuriteInfo.com.Linux.Siggen.4218.298.3210 | Get hash | malicious | Browse | • 109.202.202.202 |
| | uPOWBxniTA | Get hash | malicious | Browse | • 109.202.202.202 |
| | qy5unieRgR | Get hash | malicious | Browse | • 109.202.202.202 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | sAzPpn6mKZ | Get hash | malicious | Browse | • 109.202.202.202 |
| | AxadDC89j9 | Get hash | malicious | Browse | • 109.202.202.202 |
| | ZErnXU2XR1 | Get hash | malicious | Browse | • 109.202.202.202 |
| | sTHJvS5LPJ | Get hash | malicious | Browse | • 109.202.202.202 |
| | THzHjYQ4z6 | Get hash | malicious | Browse | • 109.202.202.202 |

## 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): | 5.51303684741125 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | 3tgXa7CGc1 |
| File size: | 40824 |
| MD5: | 3ca11c21956b7c6a03ef4f48698c209e |
| SHA1: | d26f991c4df35a746a324129f588601fc105fd18 |
| SHA256: | ddfb21fd0f3589e3ecf1421d65941a8ff85e0e324e2b2149ce67e26727c5c97f |
| SHA512: | e49f2110dc9ec4867ac9962aea7eb1e8d814d45a143341873bacdd40588a3db975bbdc7f545cd546c1bc4477bffd721322fc2ccbb370154c698b081241433a2e |
| SSDEEP: | 768:nsILLLLLLLLiBnHd/lWMBYacrctZ2dqCUwr6ruD:Wbcdzr3 |
| File Content Preview: | .ELF.....@.`...4...p.....4. ...(.....@...@.....D...D.....D..%8.....dt.Q.....<..'..L...!'.....<...'..(...!... ....'9... .....<...'.....!... ....'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 |

### ELF header

| | |
|---|---|
| Number of Program Headers: | 3 |
| Section Header Offset: | 40304 |
| Section Header Size: | 40 |
| Number of Section Headers: | 13 |
| Header String Table Index: | 12 |

### Sections

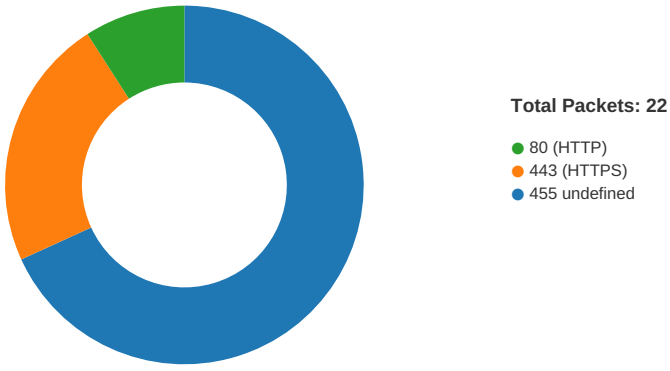
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x400094 | 0x94 | 0x8c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .text | PROGBITS | 0x400120 | 0x120 | 0x7e10 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .fini | PROGBITS | 0x407f30 | 0x7f30 | 0x5c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .rodata | PROGBITS | 0x407f90 | 0x7f90 | 0x640 | 0x0 | 0x2 | A | 0 | 0 | 16 |
| .ctors | PROGBITS | 0x4485d4 | 0x85d4 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x4485dc | 0x85dc | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x4485f0 | 0x85f0 | 0x1400 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .got | PROGBITS | 0x4499f0 | 0x99f0 | 0x328 | 0x4 | 0x10000003 | WA | 0 | 0 | 16 |
| .sbss | NOBITS | 0x449d18 | 0x9d18 | 0x18 | 0x0 | 0x10000003 | WA | 0 | 0 | 4 |
| .bss | NOBITS | 0x449d30 | 0x9d18 | 0xddc | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .mdebug.abi32 | PROGBITS | 0x5b2 | 0x9d18 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 1 |
| .shstrtab | STRTAB | 0x0 | 0x9d18 | 0x57 | 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 | 0x85d0 | 0x85d0 | 3.1410 | 0x5 | R E | 0x10000 | | .init .text .fini .rodata |
| LOAD | 0x85d4 | 0x4485d4 | 0x4485d4 | 0x1744 | 0x2538 | 2.1059 | 0x6 | RW | 0x10000 | | .ctors .dtors .data .got .sbss .bss |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

# Network Behavior

## Network Port Distribution




### TCP Packets

# System Behavior

## Analysis Process: 3tgXa7CGc1 PID: 5236 Parent PID: 5113

### General

| | |
|---|---|
| Start time: | 09:45:38 |
| Start date: | 29/10/2021 |
| Path: | /tmp/3tgXa7CGc1 |
| Arguments: | /tmp/3tgXa7CGc1 |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### File Activities

#### File Read

## Analysis Process: 3tgXa7CGc1 PID: 5238 Parent PID: 5236

### General

| | |
|---|---|
| Start time: | 09:45:38 |
| Start date: | 29/10/2021 |
| Path: | /tmp/3tgXa7CGc1 |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |