


**ID:** 557422
**Sample Name:** oTdXpH4hrI
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 04:26:28
**Date:** 21/01/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents

# Linux Analysis Report

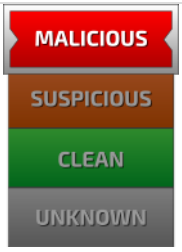
## oTdXpH4hrI

## Overview

### General Information

| | |
|---|---|
| Sample Name: | oTdXpH4hrI |
| Analysis ID: | 557422 |
| MD5: | 0dbe787e1b8ab7. |
| SHA1: | 0506160d345965. |
| SHA256: | d7d2cab6f55b5b.. |
| Tags: | 32 elf mips mirai |
| Infos: | |

### Detection



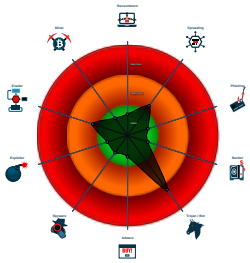

Mirai

| | |
|---|---|
| Score: | 64 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- 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 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: | 557422 |
| Start date: | 21.01.2022 |
| Start time: | 04:26:28 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 46s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | oTdXpH4hrI |
| 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: | mal64.troj.lin@0/0@0/0 |

## Warnings

### Runtime Messages

| | |
|---|---|
| Command: | /tmp/oTdXpH4hrI |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | DaddyL33T Infected Your Shit |

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

## Process Tree

- **system is lnxubuntu20**
- oTdXpH4hrl (PID: 5222, Parent: 5117, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/oTdXpH4hrl
  - oTdXpH4hrl New Fork (PID: 5224, Parent: 5222)
    - oTdXpH4hrl New Fork (PID: 5321, Parent: 5224)
    - oTdXpH4hrl New Fork (PID: 5323, Parent: 5224)
      - oTdXpH4hrl New Fork (PID: 5325, Parent: 5323)
        - oTdXpH4hrl New Fork (PID: 5338, Parent: 5325)
        - oTdXpH4hrl New Fork (PID: 5340, Parent: 5325)
      - oTdXpH4hrl New Fork (PID: 5327, Parent: 5323)
      - oTdXpH4hrl New Fork (PID: 5328, Parent: 5323)
    - oTdXpH4hrl New Fork (PID: 5225, Parent: 5222)
    - oTdXpH4hrl New Fork (PID: 5227, Parent: 5222)
      - oTdXpH4hrl New Fork (PID: 5230, Parent: 5227)
        - oTdXpH4hrl New Fork (PID: 5334, Parent: 5230)
        - oTdXpH4hrl New Fork (PID: 5336, Parent: 5230)
      - oTdXpH4hrl New Fork (PID: 5231, Parent: 5227)
      - oTdXpH4hrl New Fork (PID: 5233, Parent: 5227)
- **cleanup**

## Yara Overview

### PCAP (Network Traffic)

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| dump.pcap | JoeSecurity_Mirai_12 | Yara detected Mirai | Joe Security | |

## Jbx Signature Overview

### AV Detection

Multi AV Scanner detection for submitted file

### Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

### Stealing of Sensitive Information

Yara detected Mirai

### Remote Access Functionality

Yara detected Mirai

## Mitre Att&ck Matrix

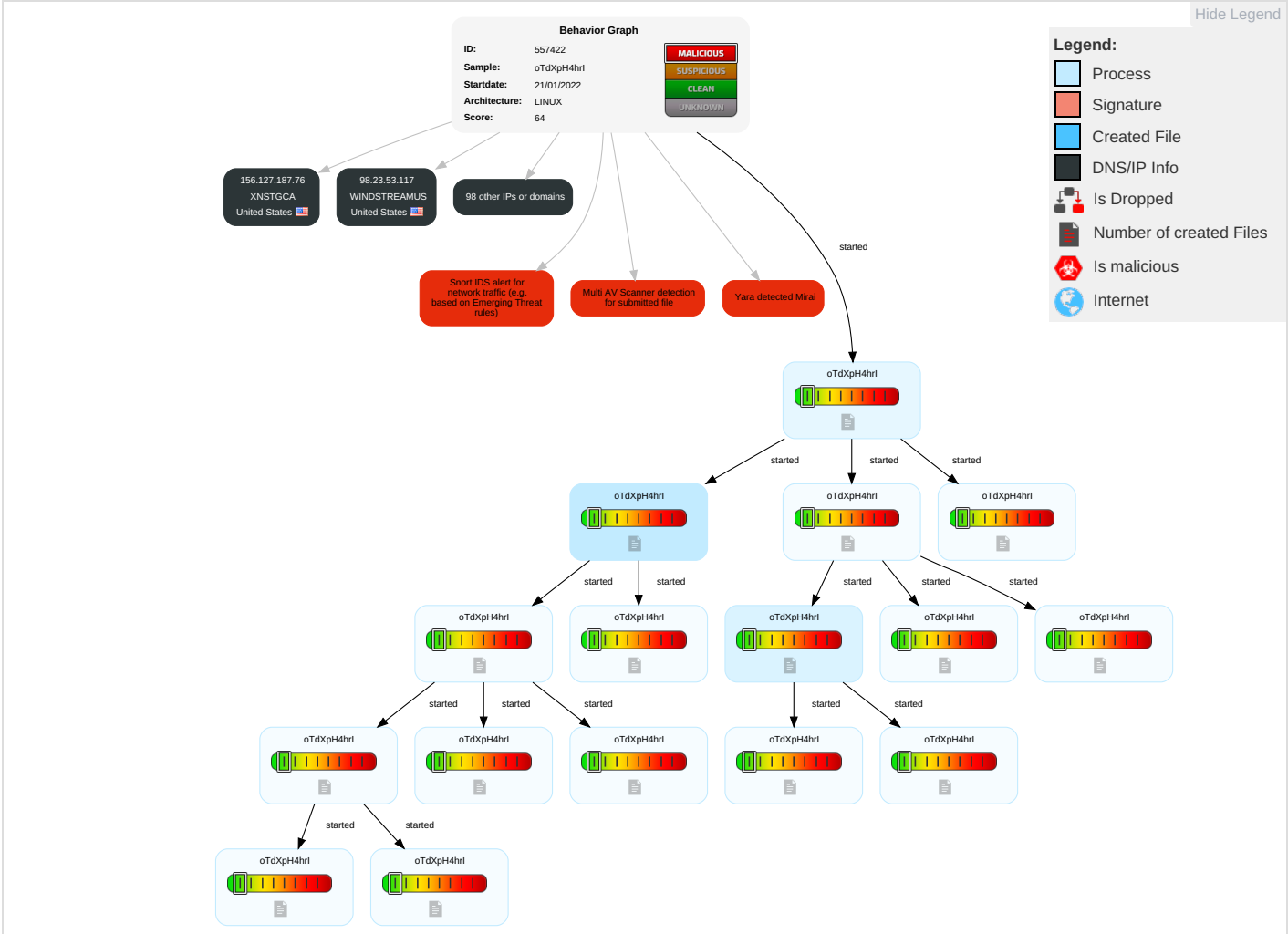
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| 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 |
|---|---|---|---|---|
| oTdXpH4hrI | 50% | Virustotal | | Browse |
| oTdXpH4hrI | 58% | ReversingLabs | Linux.Trojan.Mirai | |

## Dropped Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

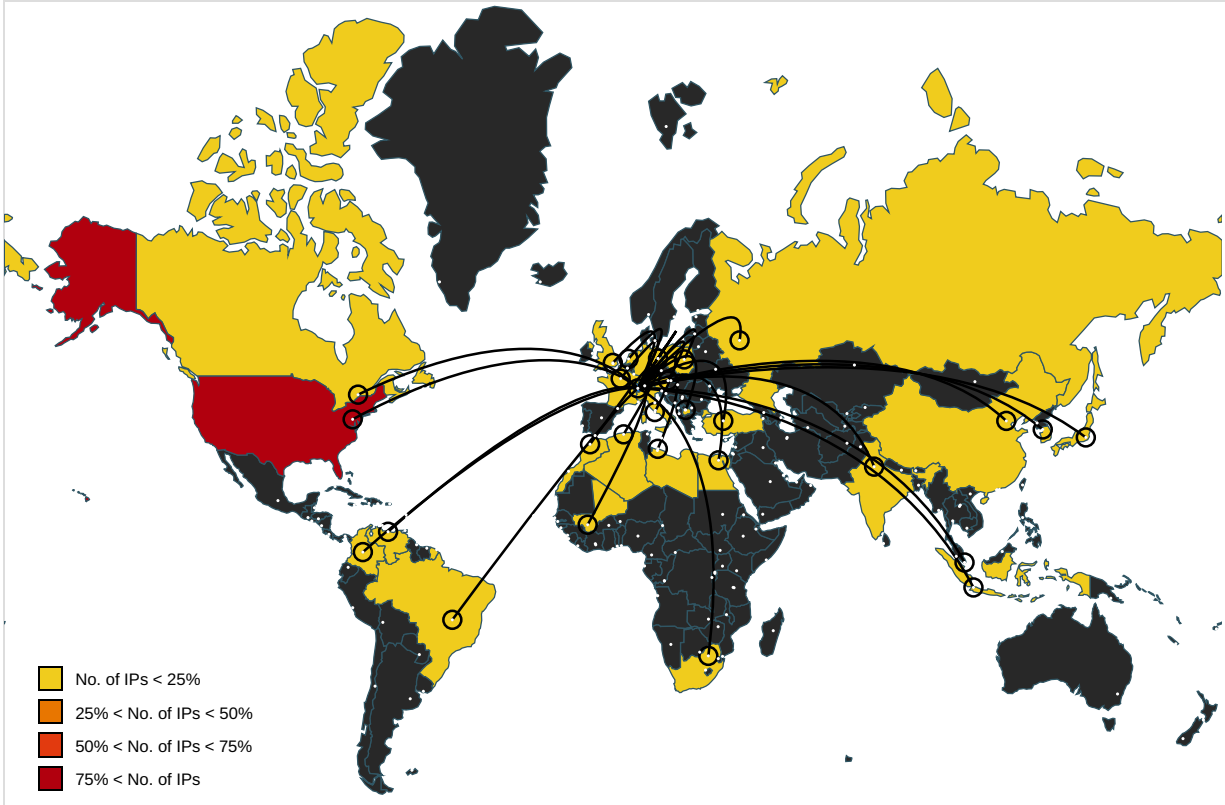
No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 248.18.203.183 | unknown | Reserved | | unknown | unknown | false |
| 97.208.122.175 | unknown | United States | | 6167 | CELLCO-PARTUS | false |
| 41.253.208.33 | unknown | Libyan Arab Jamahiriya | | 21003 | GPTC-ASLY | false |
| 157.51.180.43 | unknown | India | | 55836 | RELIANCEJIO-INRelianceJioInfocommLimitedIN | false |
| 146.35.146.91 | unknown | United States | | 197938 | TRAVIANGAMESDE | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 161.255.247.82 | unknown | Venezuela | | 25667 | HOME-SHOPPING-NETWORKUS | false |
| 2.239.41.68 | unknown | Italy | | 12874 | FASTWEBIT | false |
| 102.254.127.160 | unknown | South Africa | | 5713 | SAIX-NETZA | false |
| 208.117.171.2 | unknown | United States | | 32748 | STEADFASTUS | false |
| 117.238.129.163 | unknown | India | | 9829 | BSNL-NIBNationalInternetBackboneIN | false |
| 201.77.110.64 | unknown | unknown | | 265627 | NIDIXNETWORKSSADECVMX | false |
| 157.162.143.44 | unknown | Germany | | 22192 | SSHENETUS | false |
| 166.121.243.148 | unknown | Singapore | | 9911 | CONNECTPLUS-APSingaporeTelecomSG | false |
| 184.202.73.1 | unknown | United States | | 10507 | SPCSUS | false |
| 153.144.127.19 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 116.64.179.121 | unknown | Japan | | 9824 | JTCL-JP-ASJupiterTelecommunicationCoLtdJP | false |
| 179.133.103.140 | unknown | Brazil | | 26599 | TELEFONICABRASILSABR | false |
| 220.94.246.166 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 189.46.228.49 | unknown | Brazil | | 27699 | TELEFONICABRASILSABR | false |
| 156.127.187.76 | unknown | United States | | 393504 | XNSTGCA | false |
| 191.68.118.53 | unknown | Colombia | | 26611 | COMCELSACO | false |
| 156.24.81.178 | unknown | United States | | 29975 | VODACOM-ZA | false |
| 62.156.228.117 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 34.141.74.69 | unknown | United States | | 2686 | ATGS-MMD-ASUS | false |
| 154.118.174.227 | unknown | Mali | | 30985 | IKATELNETML | false |
| 17.83.16.172 | unknown | United States | | 714 | APPLE-ENGINEERINGUS | false |
| 19.35.34.22 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 219.43.181.12 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 206.155.137.26 | unknown | United States | | 3561 | CENTURYLINK-LEGACY-SAVVISUS | false |
| 119.98.22.197 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 250.139.144.230 | unknown | Reserved | | unknown | unknown | false |
| 160.63.37.99 | unknown | Switzerland | | 25031 | NOVARTIS-CH | false |
| 119.143.77.106 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 179.77.43.204 | unknown | Brazil | | 26615 | TIMSABR | false |
| 207.138.188.246 | unknown | United States | | 3549 | LVLT-3549US | false |
| 88.156.212.231 | unknown | Poland | | 29314 | VECTRANET-ASAlZwyciestwa25381-525GdyniaPolandPL | false |
| 39.237.94.34 | unknown | Indonesia | | 23693 | TELKOMSEL-ASN-IDPTTelekomunikasiSelularID | false |
| 71.118.210.182 | unknown | United States | | 701 | UUNETUS | false |
| 67.186.82.247 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 169.35.183.186 | unknown | Switzerland | | 37611 | AfrihostZA | false |
| 162.49.240.214 | unknown | United States | | 35893 | ACPCA | false |
| 176.25.33.205 | unknown | United Kingdom | | 5607 | BSKYB-BROADBAND-ASGB | false |
| 41.137.15.163 | unknown | Morocco | | 36884 | MAROCCONNECTMA | false |
| 46.183.211.230 | unknown | Poland | | 51996 | MICROSTRATEGY_POLAND-ASPL | false |
| 35.232.98.157 | unknown | United States | | 15169 | GOOGLEUS | false |
| 97.202.183.139 | unknown | United States | | 6167 | CELLCO-PARTUS | false |
| 115.44.238.221 | unknown | China | | 17962 | TOPWAY-NETShenZhenTopwayVideoCommunicationCoLtdCN | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 95.172.134.25 | unknown | Russian Federation | | 60879 | SYSTEMPROJECTS-ASKrasnoyarskRU | false |
| 141.55.19.217 | unknown | Germany | | 680 | DFNVereinzurFoerderungeinesDeutschenForschungsnetzese | false |
| 202.114.33.255 | unknown | China | | 4538 | ERX-CERNET-BKBChinaEducationandResearchNetworkCenter | false |
| 154.50.188.248 | unknown | United States | | 174 | COGENT-174US | false |
| 161.234.123.194 | unknown | Venezuela | | 396269 | BPL-ASNUS | false |
| 66.252.187.196 | unknown | United States | | 25606 | CPVCOMUS | false |
| 243.82.211.65 | unknown | Reserved | | unknown | unknown | false |
| 54.52.248.114 | unknown | United States | | 14618 | AMAZON-AESUS | false |
| 206.244.4.20 | unknown | United States | | 600 | OARNET-ASUS | false |
| 87.243.148.176 | unknown | Austria | | 35370 | AINET-ASAT | false |
| 157.203.98.74 | unknown | United Kingdom | | 1759 | TSF-IP-CORETeliaFinlandOyjEU | false |
| 95.156.28.222 | unknown | Macedonia | | 6821 | MT-AS-OWNbulOrceNikolovbbMK | false |
| 164.105.204.209 | unknown | United States | | 54060 | POUDRESCHOOLDISTRICTUS | false |
| 129.4.161.230 | unknown | United States | | 1906 | NORTHROP-GRUMMANUS | false |
| 197.204.101.18 | unknown | Algeria | | 36947 | ALGTEL-ASDZ | false |
| 113.122.67.53 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 250.197.76.186 | unknown | Reserved | | unknown | unknown | false |
| 79.19.233.101 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 190.84.94.126 | unknown | Colombia | | 10620 | TelmexColombiaSACO | false |
| 216.127.235.58 | unknown | United States | | 3356 | LEVEL3US | false |
| 98.23.53.117 | unknown | United States | | 7029 | WINDSTREAMUS | false |
| 32.212.93.213 | unknown | United States | | 46690 | SNET-FCCUS | false |
| 82.66.137.156 | unknown | France | | 12322 | PROXADFR | false |
| 142.130.66.40 | unknown | Canada | | 13576 | SDNW-13576US | false |
| 185.0.80.136 | unknown | unknown | | 5778 | CENTURYLINK-LEGACY-EMBARQ-RCMTUS | false |
| 43.87.148.114 | unknown | Japan | | 4249 | LILLY-ASUS | false |
| 182.83.127.87 | unknown | China | | 23771 | SXBCTV-APSXBCTVInternetServiceProviderCN | false |
| 84.190.75.150 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 44.52.114.166 | unknown | United States | | 7377 | UCSDUS | false |
| 31.145.206.225 | unknown | Turkey | | 15924 | BORUSANTELEKOM-ASTR | false |
| 129.7.118.186 | unknown | United States | | 7276 | UNIVERSITY-OF-HOUSTONUS | false |
| 182.101.237.254 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 119.219.228.191 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 156.215.116.37 | unknown | Egypt | | 8452 | TE-ASTE-ASEG | false |
| 62.233.213.0 | unknown | Poland | | 12741 | AS-NETIAWarszawa02-822PL | false |
| 173.249.196.174 | unknown | United States | | 11878 | TZULOUS | false |
| 198.227.253.234 | unknown | United States | | 18933 | USCC-MPLS01US | false |
| 99.145.18.237 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 76.134.26.255 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 59.211.133.118 | unknown | China | | 2516 | KDDIKDDICORPORATIONJP | false |
| 139.29.139.114 | unknown | Germany | | 8767 | MNET-ASGermanyDE | false |
| 65.85.104.218 | unknown | United States | | 18566 | MEGAPATH5-US | false |
| 38.79.169.249 | unknown | United States | | 174 | COGENT-174US | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 14.158.135.47 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 158.81.56.222 | unknown | United States | | 16746 | RELIANTENERGYUS | false |
| 217.96.200.70 | unknown | Poland | | 5617 | TPNETPL | false |
| 147.137.74.158 | unknown | United States | | 20214 | COMCAST-20214US | false |
| 45.239.81.192 | unknown | Brazil | | 268384 | JCTELECOMBR | false |
| 188.90.34.47 | unknown | Netherlands | | 31615 | TMO-NL-ASNL | false |
| 39.207.89.158 | unknown | Indonesia | | 23693 | TELKOMSEL-ASN-IDPTTelekomunikasiSelularID | false |
| 165.7.64.57 | unknown | United States | | 46512 | UT-MEDICAL-CENTERUS | false |
| 183.104.26.58 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 13.50.219.72 | unknown | United States | | 16509 | AMAZON-02US | false |

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped |
| Entropy (8bit): | 5.426622535894816 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | oTdXpH4hrl |
| File size: | 71528 |
| MD5: | 0dbe787e1b8ab7f004a55b418e3141c4 |
| SHA1: | 0506160d345965ffb7ffa6edb155ddfab10d1ae4 |
| SHA256: | d7d2cab6f55b5b9b2bbd12911c450981eb6d84da22ef13ae1cf9b2d31a336b2d |
| SHA512: | 9f79dd65e0beb8f8b18db5f19352e95c3bb0ca6aeebb55545b980f29f9b4d7dd76b2abefe84cc8a08db4d8cb650a0c25f6c8c7819bb08232ab9c3ca6ccd52942 |

| | |
|---|---|
| SSDEEP: | 768:JxNCJ0EYlDYhxD9ZbsFywLX3U6nFW9N6PNo0se15DSeue2qeNncoNjpkGUrXivM0:JxNCJBYld4ww/9wPqe1IT/qSnMhA5 |
| File Content Preview: | .ELF.....`.@.4...`.....4. ...(.....@...@.....E...E.....Q.td.....<...'!.....'.....<...'!... .....9'.. .....<...'!..... .9 |

## Static ELF Info

### ELF header

| | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, little endian |
| Version: | 1 (current) |
| Machine: | MIPS R3000 |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | UNIX - System V |
| ABI Version: | 0 |
| Entry Point Address: | 0x400260 |
| Flags: | 0x1007 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 71008 |
| Section Header Size: | 40 |
| Number of Section Headers: | 13 |
| Header String Table Index: | 12 |

### Sections

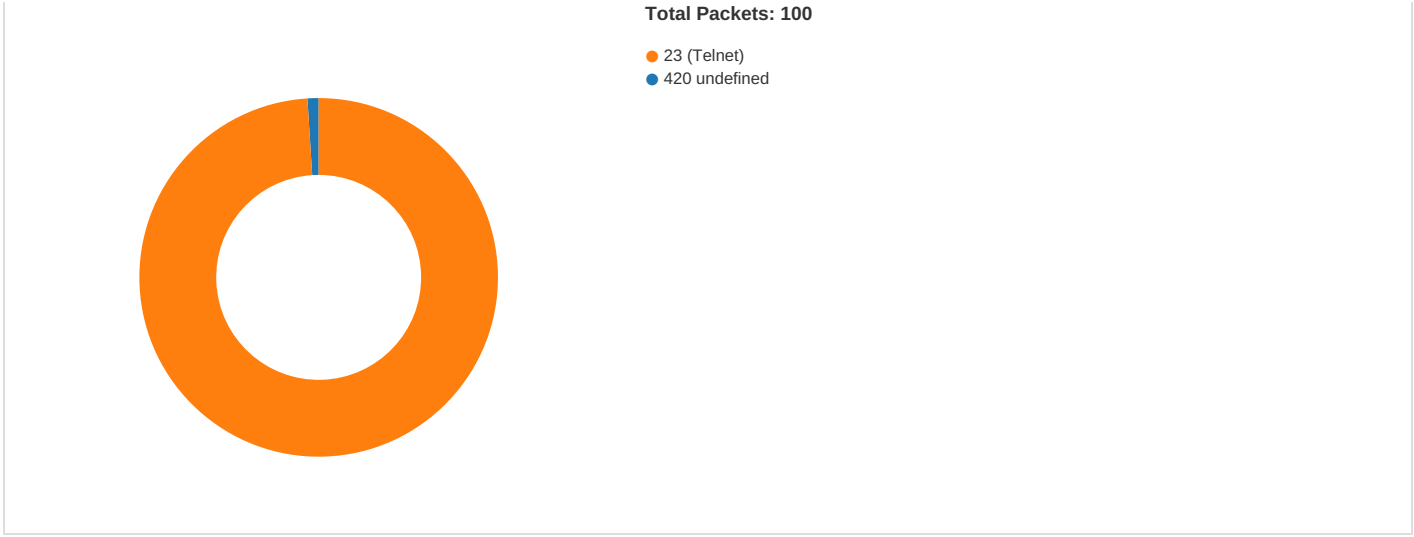
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x400094 | 0x94 | 0x8c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .text | PROGBITS | 0x400120 | 0x120 | 0x10670 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .fini | PROGBITS | 0x410790 | 0x10790 | 0x5c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .rodata | PROGBITS | 0x4107f0 | 0x107f0 | 0x610 | 0x0 | 0x2 | A | 0 | 0 | 16 |
| .ctors | PROGBITS | 0x451000 | 0x11000 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x451008 | 0x11008 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x451020 | 0x11020 | 0x190 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .got | PROGBITS | 0x4511b0 | 0x111b0 | 0x358 | 0x4 | 0x10000003 | WA | 0 | 0 | 16 |
| .sbss | NOBITS | 0x451508 | 0x11508 | 0x24 | 0x0 | 0x10000003 | WA | 0 | 0 | 4 |
| .bss | NOBITS | 0x451530 | 0x11508 | 0x2a0 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .mdebug.abi32 | PROGBITS | 0x654 | 0x11508 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 1 |
| .shstrtab | STRTAB | 0x0 | 0x11508 | 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 | 0x10e00 | 0x10e00 | 3.3549 | 0x5 | R E | 0x10000 | | .init .text .fini .rodata |
| LOAD | 0x11000 | 0x451000 | 0x451000 | 0x508 | 0x7d0 | 2.0107 | 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: oTdXpH4hrl PID: 5222, Parent PID: 5117

#### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | /tmp/oTdXpH4hrl |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

#### File Activities

##### File Read

### Analysis Process: oTdXpH4hrl PID: 5224, Parent PID: 5222

#### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

#### File Activities

##### File Read

##### Directory Enumerated

### Analysis Process: oTdXpH4hrl PID: 5321, Parent PID: 5224

#### General

| | |
|---|---|
| Start time: | 04:30:02 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5323**, Parent PID: **5224**

### General

| | |
|---|---|
| Start time: | 04:30:02 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5325**, Parent PID: **5323**

### General

| | |
|---|---|
| Start time: | 04:30:02 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5338**, Parent PID: **5325**

### General

| | |
|---|---|
| Start time: | 04:30:07 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5340**, Parent PID: **5325**

### General

| | |
|---|---|
| Start time: | 04:30:07 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5327**, Parent PID: **5323**

### General

| | |
|---|---|
| Start time: | 04:30:02 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5328**, Parent PID: **5323**

### General

| | |
|---|---|
| Start time: | 04:30:02 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5225**, Parent PID: **5222**

### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5227**, Parent PID: **5222**

### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5230**, Parent PID: **5227**

### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: oTdXpH4hrl PID: **5334**, Parent PID: **5230**

### General

| | |
|---|---|
| Start time: | 04:30:03 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5336**, Parent PID: **5230**

### General

| | |
|---|---|
| Start time: | 04:30:03 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5231**, Parent PID: **5227**

### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |

| | |
|---|---|
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |

## Analysis Process: oTdXpH4hrl PID: **5233**, Parent PID: **5227**

### General

| | |
|---|---|
| Start time: | 04:27:12 |
| Start date: | 21/01/2022 |
| Path: | /tmp/oTdXpH4hrl |
| Arguments: | n/a |
| File size: | 5773336 bytes |
| MD5 hash: | 0d6f61f82cf2f781c6eb0661071d42d9 |