




**ID:** 626581
**Sample Name:** 63CYVWIouB
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 14:45:10
**Date:** 14/05/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents


Table of Contents 2
Linux Analysis Report 63CYVWIouB 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Warnings 3
Runtime Messages 3
Process Tree 4
Yara Signatures 4
PCAP (Network Traffic) 4
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Networking 4
Hooking and other Techniques for Hiding and Protection 4
Stealing of Sensitive Information 4
Remote Access Functionality 4
Mitre Att&ck Matrix 4
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 10
General 10
Static ELF Info 10
ELF header 10
Sections 10
Program Segments 10
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
System Behavior 11
Analysis Process: 63CYVWIouB PID: 6234, Parent PID: 6125 11
General 11
File Activities 11
File Deleted 11
Analysis Process: 63CYVWIouB PID: 6235, Parent PID: 6234 11
General 11
Analysis Process: 63CYVWIouB PID: 6236, Parent PID: 6235 11
General 11
Analysis Process: 63CYVWIouB PID: 6237, Parent PID: 6235 12
General 12
Analysis Process: 63CYVWIouB PID: 6238, Parent PID: 6235 12
General 12
File Activities 12
File Read 12
Directory Enumerated 12
Analysis Process: 63CYVWIouB PID: 6240, Parent PID: 6235 12
General 12
File Activities 12
Directory Enumerated 12

# Linux Analysis Report

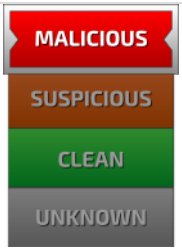
## 63CYVWIouB

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 63CYVWIouB |
| Analysis ID: | 626581 |
| MD5: | c43b1f7f5d82b0e.. |
| SHA1: | 1da4e06856562c.. |
| SHA256: | f403c4a3db6554.. |
| Tags: | 32 elf intel mirai |
| Infos: | |

### Detection



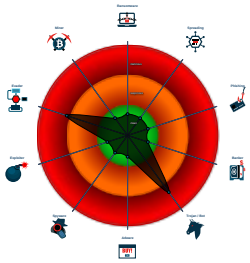

Mirai

| | |
|---|---|
| Score: | 68 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample deletes itself
- Uses known network protocols on n...
- Machine Learning detection for sam...
- Sample has stripped symbol table
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...
- Sample contains strings indicative o...

### Classification



### Analysis Advice

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

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 626581 |
| Start date and time: 14/05/202214:45:10 | 2022-05-14 14:45:10 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 7s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 63CYVWIouB |
| 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: | mal68.troj.evad.lin@0/0@0/0 |

## Warnings

## Runtime Messages

| | |
|---|---|
| Command: | /tmp/63CYVWIouB |
| PID: | 6234 |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | cronus |
| Standard Error: | |

Copyright Joe Security LLC 2022

## Process Tree

- **system is lnxubuntu20**
- 63CYVWIouB (PID: 6234, Parent: 6125, MD5: c43b1f7f5d82b0e0af11805d19221314) Arguments: /tmp/63CYVWIouB
  - 63CYVWIouB New Fork (PID: 6235, Parent: 6234)
    - 63CYVWIouB New Fork (PID: 6236, Parent: 6235)
    - 63CYVWIouB New Fork (PID: 6237, Parent: 6235)
    - 63CYVWIouB New Fork (PID: 6238, Parent: 6235)
    - 63CYVWIouB New Fork (PID: 6240, Parent: 6235)
- **cleanup**

## Yara Signatures

### PCAP (Network Traffic)

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

## Snort Signatures

**No Snort rule has matched**

## Joe Sandbox Signatures

### AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Networking



Uses known network protocols on non-standard ports

### Hooking and other Techniques for Hiding and Protection



Sample deletes itself

Uses known network protocols on non-standard ports

### Stealing of Sensitive Information



Yara detected Mirai

### Remote Access Functionality



Yara detected Mirai

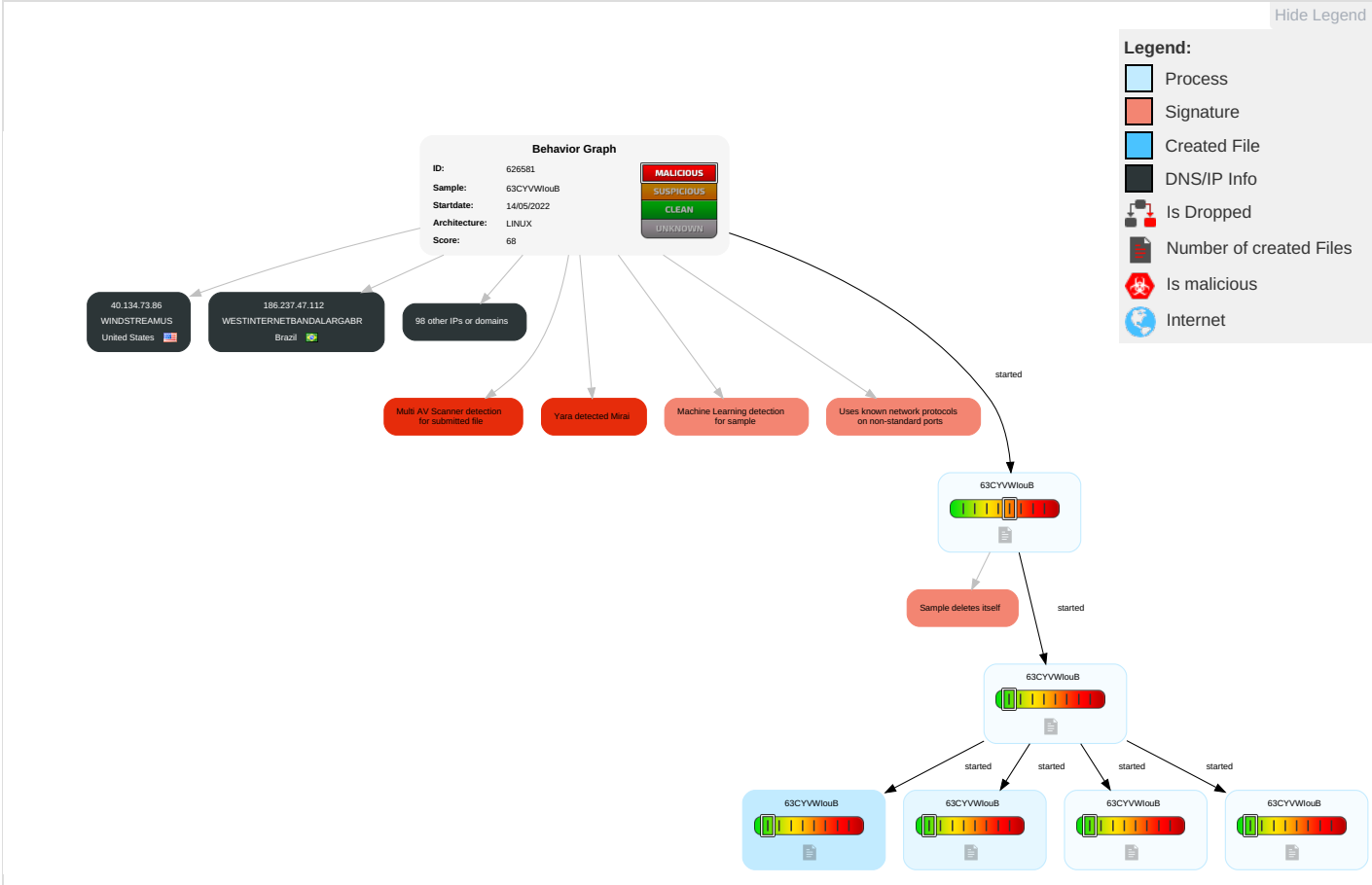
## Mitre Att&ck Matrix

| 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 | 1 File Deletion | OS Credential Dumping | System Service 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 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 |
|---|---|---|---|---|
| 63CYVWIouB | 44% | Virustotal | | Browse |
| 63CYVWIouB | 31% | Metadefender | | Browse |
| 63CYVWIouB | 61% | ReversingLabs | Linux.Trojan.Mirai | |
| 63CYVWIouB | 100% | Joe Sandbox ML | | |

## Dropped Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

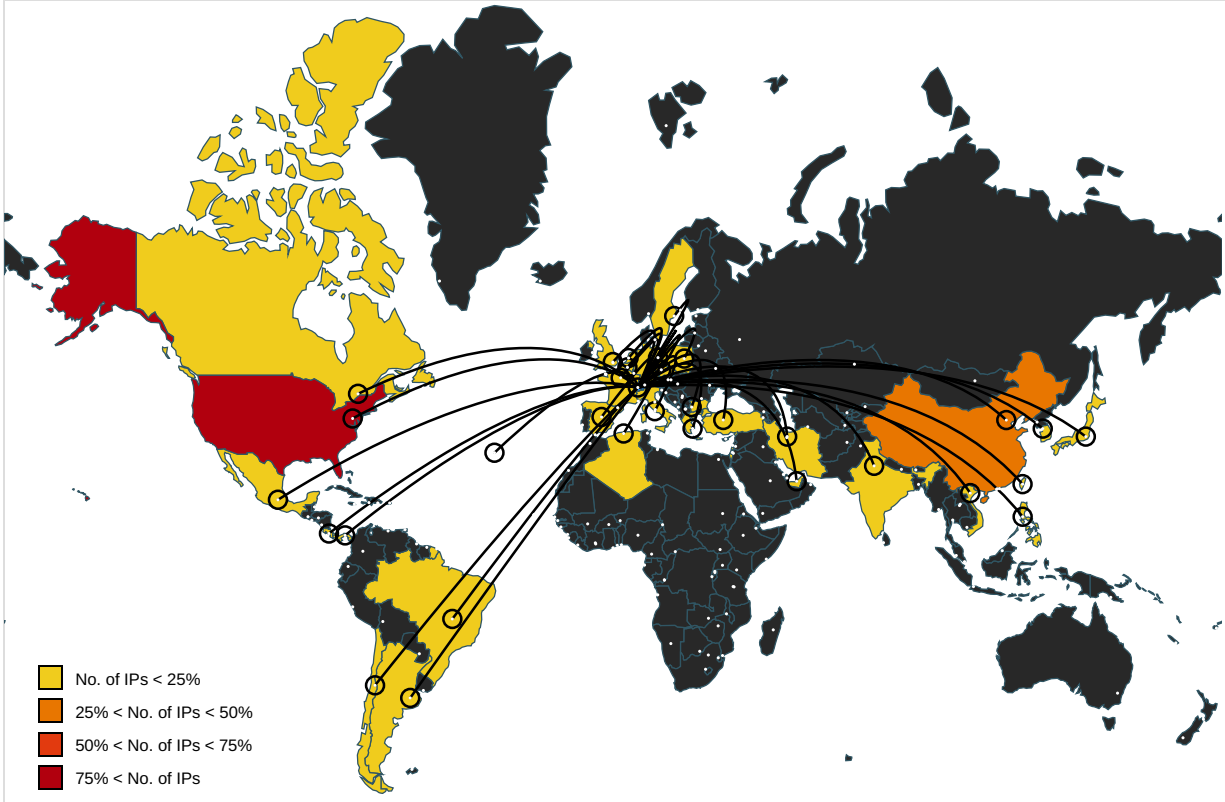
No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 136.225.157.141 | unknown | Sweden | | 158 | ERI-ASUS | false |
| 23.40.23.231 | unknown | United States | | 16625 | AKAMAI-ASUS | false |
| 65.196.3.91 | unknown | United States | | 701 | UUNETUS | false |
| 105.100.195.17 | unknown | Algeria | | 36947 | ALGTEL-ASDZ | false |

Copyright Joe Security LLC 2022

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 186.100.167.17 | unknown | Argentina | | 11315 | TelefonicaMovilesArgentinaSAMovistarArgentinaAR | false |
| 124.245.123.199 | unknown | Japan | | 7671 | MCNETNTTSmartConnectCorporationJP | false |
| 182.99.121.177 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 41.106.43.118 | unknown | Algeria | | 36947 | ALGTEL-ASDZ | false |
| 140.178.253.97 | unknown | United States | | 668 | DNIC-AS-00668US | false |
| 84.61.19.221 | unknown | Germany | | 3209 | VODANETInternationalIP-BackboneofVodafoneDE | false |
| 188.136.134.234 | unknown | Iran (ISLAMIC Republic Of) | | 48309 | AGS-ASIR | false |
| 77.124.162.219 | unknown | Israel | | 9116 | GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste | false |
| 38.253.112.215 | unknown | United States | | 174 | COGENT-174US | false |
| 87.17.178.52 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 152.148.171.215 | unknown | United States | | 10455 | LUCENT-CIOUS | false |
| 1.248.72.166 | unknown | Korea Republic of | | 9318 | SKB-ASSKBroadbandCoLtdKR | false |
| 149.65.120.44 | unknown | United States | | 188 | SAIC-ASUS | false |
| 186.237.47.112 | unknown | Brazil | | 28255 | WESTINTERNETBANDALARGABR | false |
| 201.63.244.79 | unknown | Brazil | | 10429 | TELEFONICABRASILSABR | false |
| 220.198.152.187 | unknown | China | | 17816 | CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi | false |
| 117.141.51.100 | unknown | China | | 9808 | CMNET-GDGuangdongMobileCommunicationCoLtdCN | false |
| 31.148.200.113 | unknown | Czech Republic | | 56965 | GOTHAMADS-ASNL | false |
| 62.34.129.222 | unknown | France | | 5410 | BOUYGTEL-ISPFR | false |
| 90.135.191.83 | unknown | Sweden | | 1257 | TELE2EU | false |
| 12.158.226.122 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 201.225.63.198 | unknown | Panama | | 11556 | CableWirelessPanamaPA | false |
| 178.103.193.162 | unknown | United Kingdom | | 12576 | EELtdGB | false |
| 87.199.107.186 | unknown | Poland | | 41201 | DOLSATulWojskaPolskiego23CPL | false |
| 99.64.162.0 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 208.70.241.77 | unknown | United States | | 13612 | SYSMEXUS | false |
| 218.155.160.227 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 188.153.199.83 | unknown | Italy | | 30722 | VODAFONE-IT-ASNIT | false |
| 134.74.249.33 | unknown | United States | | 31822 | CITY-UNIVERSITY-OF-NEW-YORKUS | false |
| 191.219.7.169 | unknown | Brazil | | 8167 | BrasilTelecomSA-FilialDistritoFederalBR | false |
| 76.146.57.241 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 92.26.2.105 | unknown | United Kingdom | | 13285 | OPALTELECOM-ASTalkTalkCommunicationsLimitedGB | false |
| 57.5.138.213 | unknown | Belgium | | 2686 | ATGS-MMD-ASUS | false |
| 85.205.176.67 | unknown | Germany | | 12663 | VODAFONE-GROUPIT | false |
| 27.173.40.87 | unknown | Korea Republic of | | 9644 | SKTELECOM-NET-ASSKTelecomKR | false |
| 193.92.123.61 | unknown | Greece | | 1241 | FORTHNET-GRForthnetEU | false |
| 194.178.167.33 | unknown | Netherlands | | 702 | UUNETUS | false |
| 159.246.182.29 | unknown | United States | | 29899 | GEISINGERUS | false |
| 199.1.57.37 | unknown | United States | | 1239 | SPRINTLINKUS | false |
| 183.44.54.26 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 39.145.157.139 | unknown | China | | 9808 | CMNET-GDGuangdongMobileCommunicationCoLtdCN | false |
| 40.134.73.86 | unknown | United States | | 7029 | WINDSTREAMUS | false |

Copyright Joe Security LLC 2022

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 69.42.38.251 | unknown | United States | | 18474 | AENEAS-CWUS | false |
| 78.120.46.62 | unknown | France | | 8228 | CEGETEL-ASFR | false |
| 134.155.120.140 | unknown | Germany | | 553 | BELWUEBelWue-KoordinationEU | false |
| 158.216.116.51 | unknown | Switzerland | | 2907 | SINET-ASResearchOrganizationofInformationandSystemsN | false |
| 223.138.247.180 | unknown | Taiwan; Republic of China (ROC) | | 17421 | EMOME-NETMobileBusinessGroupTW | false |
| 120.192.206.133 | unknown | China | | 9808 | CMNET-GDGuangdongMobileCommunicationCoLtdCN | false |
| 131.143.196.74 | unknown | United States | | 1742 | HARVARD-UNIVUS | false |
| 179.105.7.56 | unknown | Brazil | | 28573 | CLAROSABR | false |
| 13.36.254.82 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 68.80.0.80 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 71.174.46.144 | unknown | United States | | 701 | UUNETUS | false |
| 191.215.104.101 | unknown | Brazil | | 7738 | TelemarNorteLesteSABR | false |
| 213.37.253.63 | unknown | Spain | | 12357 | COMUNITELSPAINES | false |
| 218.209.89.122 | unknown | Korea Republic of | | 23563 | VITSSEN-SUWON-AS-KRTbroadSuwonBroadcastingCorporationK | false |
| 125.60.167.11 | unknown | Philippines | | 10139 | SMARTBRO-PH-APSmartBroadbandIncPH | false |
| 190.171.98.115 | unknown | Costa Rica | | 52263 | TelecableEconomicoSACR | false |
| 187.254.178.141 | unknown | Mexico | | 16960 | CablevisionRedSAdeCVMX | false |
| 27.73.132.243 | unknown | Viet Nam | | 7552 | VIETEL-AS-APViettelGroupVN | false |
| 123.252.200.52 | unknown | India | | 17762 | HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN | false |
| 37.154.194.0 | unknown | Turkey | | 20978 | TT_MOBILIstanbulTR | false |
| 138.87.192.170 | unknown | United States | | 7386 | ILLINOIS-STATE-UNIVUS | false |
| 126.71.66.53 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 176.124.185.235 | unknown | Czech Republic | | 59664 | ASOPTONCZ | false |
| 39.81.218.251 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 141.247.220.223 | unknown | United States | | 40112 | OPPD-ASUS | false |
| 13.232.173.25 | unknown | United States | | 16509 | AMAZON-02US | false |
| 203.9.36.233 | unknown | China | | 136518 | WA-GOVERNMENT-AS-APWAGovernmentprojectAU | false |
| 181.201.137.240 | unknown | Chile | | 7418 | TELEFONICACHILESACL | false |
| 220.140.87.227 | unknown | Taiwan; Republic of China (ROC) | | 3462 | HINETDataCommunicationBusinessGroupTW | false |
| 200.101.106.240 | unknown | Brazil | | 8167 | BrasilTelecomSA-FilialDistritoFederalBR | false |
| 179.209.165.147 | unknown | Brazil | | 28573 | CLAROSABR | false |
| 44.130.57.133 | unknown | United States | | 7377 | UCSDUS | false |
| 168.71.201.22 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 217.143.93.248 | unknown | Sweden | | 16253 | BORDERLIGHT-ASVretgrand18SE | false |
| 45.85.242.100 | unknown | United Kingdom | | 9009 | M247GB | false |
| 134.172.186.186 | unknown | United States | | 18128 | RIKENRIKENPhysicalandChemicalResearchInstituteJP | false |
| 88.9.29.165 | unknown | Spain | | 3352 | TELEFONICA_DE_ESPANAES | false |
| 94.101.198.11 | unknown | Bulgaria | | 50810 | MOBINNET-ASAS47823belongstoArvanCloudCDNthatismobinn | false |
| 121.238.137.183 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 42.12.217.6 | unknown | Korea Republic of | | 4249 | LILLY-ASUS | false |

Copyright Joe Security LLC 2022

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 183.43.220.254 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 23.51.50.78 | unknown | United States | | 4788 | TMNET-AS-APTMNetInternetServiceProviderMY | false |
| 70.2.128.107 | unknown | United States | | 10507 | SPCSUS | false |
| 27.61.234.156 | unknown | India | | 45609 | BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService | false |
| 112.189.85.6 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 47.91.186.107 | unknown | United States | | 45102 | CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC | false |
| 125.76.57.67 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 142.228.94.163 | unknown | Canada | | 13576 | SDNW-13576US | false |
| 27.180.138.117 | unknown | Korea Republic of | | 9644 | SKTELECOM-NET-ASSKTelecomKR | false |
| 2.51.225.179 | unknown | United Arab Emirates | | 5384 | EMIRATES-INTERNETEmiratesInternetAE | false |
| 25.198.61.139 | unknown | United Kingdom | | 7922 | COMCAST-7922US | false |
| 117.222.44.210 | unknown | India | | 9829 | BSNL-NIBNationalInternetBackboneIN | false |
| 4.241.66.250 | unknown | United States | | 3356 | LEVEL3US | false |
| 174.208.50.11 | unknown | United States | | 22394 | CELLCOUS | 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

Copyright Joe Security LLC 2022

# Static File Info

## General

| | |
|---|---|
| File type: | ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped |
| Entropy (8bit): | 6.57007357366659 |
| TrID: | • ELF Executable and Linkable format (Linux) (4029/14) 50.16%<br>• ELF Executable and Linkable format (generic) (4004/1) 49.84% |
| File name: | 63CYVWIouB |
| File size: | 46384 |
| MD5: | c43b1f7f5d82b0e0af11805d19221314 |
| SHA1: | 1da4e06856562c57e45e2b2785060026a238ef6b |
| SHA256: | f403c4a3db6554515ee5ee692b93baa31a4083ac1832a0ed64f62043c9467b60 |
| SHA512: | 68c6916a6da7f756606b48d6eadeee92dd9c36bdfeb06f192c2bd79556dc732283cdcc9b011265b712e66a8b58ccebac1262fde279ecf64315f7317bff96b86a |
| SSDEEP: | 768:WIBprzbRqekEBKcavT3AU6z3525ZY/V68AA0x/fDhX8kUSXnIYB:WyRqeBRFU6tQ3TAKHDh9USX |
| TLSH: | B5237E81C5C3CDB5EC2319B224BB5BB28776E59D2060FB49D36D9A35ED03702A22B35D |
| File Content Preview: | .ELF.....d...4.....4. ...(.....\|...\|.....0...0..`... *.....Q.td.....U..S.....w....h....c...<br>[]...$.....U.....=`3...t..5....$0.....$0.....u.....t....h\|-..... |

## Static ELF Info

### ELF header

| | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, little endian |
| Version: | 1 (current) |
| Machine: | Intel 80386 |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | UNIX - System V |
| ABI Version: | 0 |
| Entry Point Address: | 0x8048164 |
| Flags: | 0x0 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 45984 |
| Section Header Size: | 40 |
| Number of Section Headers: | 10 |
| Header String Table Index: | 9 |

### Sections

| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x8048094 | 0x94 | 0x1c | 0x0 | 0x6 | AX | 0 | 0 | 1 |
| .text | PROGBITS | 0x80480b0 | 0xb0 | 0x8f86 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .fini | PROGBITS | 0x8051036 | 0x9036 | 0x17 | 0x0 | 0x6 | AX | 0 | 0 | 1 |
| .rodata | PROGBITS | 0x8051060 | 0x9060 | 0x1d1c | 0x0 | 0x2 | A | 0 | 0 | 32 |
| .ctors | PROGBITS | 0x8053000 | 0xb000 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x8053008 | 0xb008 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x8053020 | 0xb020 | 0x340 | 0x0 | 0x3 | WA | 0 | 0 | 32 |
| .bss | NOBITS | 0x8053360 | 0xb360 | 0x26c0 | 0x0 | 0x3 | WA | 0 | 0 | 32 |
| .shstrtab | STRTAB | 0x0 | 0xb360 | 0x3e | 0x0 | 0x0 | | 0 | 0 | 1 |

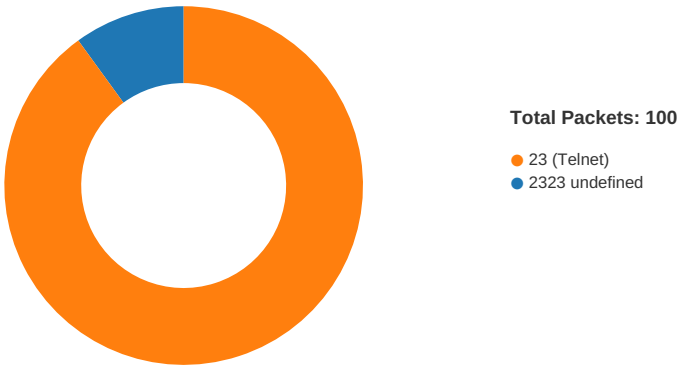
### Program Segments

| Type | Offset | Virtual Address | Physical Address | File Size | Memory Size | Entropy | Flags | Flags Description | Align | Prog Interpreter | Section Mappings |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LOAD | 0x0 | 0x8048000 | 0x8048000 | 0xad7c | 0xad7c | 3.8869 | 0x5 | R E | 0x1000 | | .init .text .fini .rodata |
| LOAD | 0xb000 | 0x8053000 | 0x8053000 | 0x360 | 0x2a20 | 2.7347 | 0x6 | RW | 0x1000 | | .ctors .dtors .data .bss |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x4 | | |

Copyright Joe Security LLC 2022

## Network Behavior

### Network Port Distribution




### TCP Packets

## System Behavior

### Analysis Process: 63CYVWIouB PID: 6234, Parent PID: 6125

#### General

| | |
|---|---|
| Start time: | 14:45:53 |
| Start date: | 14/05/2022 |
| Path: | /tmp/63CYVWIouB |
| Arguments: | /tmp/63CYVWIouB |
| File size: | 46384 bytes |
| MD5 hash: | c43b1f7f5d82b0e0af11805d19221314 |

#### File Activities

##### File Deleted

### Analysis Process: 63CYVWIouB PID: 6235, Parent PID: 6234

#### General

| | |
|---|---|
| Start time: | 14:45:53 |
| Start date: | 14/05/2022 |
| Path: | /tmp/63CYVWIouB |
| Arguments: | n/a |
| File size: | 46384 bytes |
| MD5 hash: | c43b1f7f5d82b0e0af11805d19221314 |

### Analysis Process: 63CYVWIouB PID: 6236, Parent PID: 6235

#### General

| | |
|---|---|
| Start time: | 14:45:53 |
| Start date: | 14/05/2022 |
| Path: | /tmp/63CYVWIouB |
| Arguments: | n/a |
| File size: | 46384 bytes |
| MD5 hash: | c43b1f7f5d82b0e0af11805d19221314 |

Copyright Joe Security LLC 2022

## Analysis Process: 63CYVWIouB PID: **6237**, Parent PID: **6235**

### General

| | |
|---|---|
| Start time: | 14:45:53 |
| Start date: | 14/05/2022 |
| Path: | /tmp/63CYVWIouB |
| Arguments: | n/a |
| File size: | 46384 bytes |
| MD5 hash: | c43b1f7f5d82b0e0af11805d19221314 |

## Analysis Process: 63CYVWIouB PID: **6238**, Parent PID: **6235**

### General

| | |
|---|---|
| Start time: | 14:45:53 |
| Start date: | 14/05/2022 |
| Path: | /tmp/63CYVWIouB |
| Arguments: | n/a |
| File size: | 46384 bytes |
| MD5 hash: | c43b1f7f5d82b0e0af11805d19221314 |

### File Activities

**File Read**

**Directory Enumerated**

## Analysis Process: 63CYVWIouB PID: **6240**, Parent PID: **6235**

### General

| | |
|---|---|
| Start time: | 14:45:53 |
| Start date: | 14/05/2022 |
| Path: | /tmp/63CYVWIouB |
| Arguments: | n/a |
| File size: | 46384 bytes |
| MD5 hash: | c43b1f7f5d82b0e0af11805d19221314 |

### File Activities

**Directory Enumerated**

Copyright Joe Security LLC 2022