
**ID:** 626466
**Sample Name:** 0vFX7VXc9U
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 04:00:30
**Date:** 14/05/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents

# Linux Analysis Report

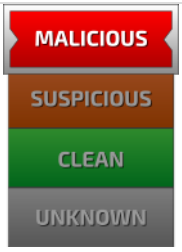
## 0vFX7VXc9U

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 0vFX7VXc9U |
| Analysis ID: | 626466 |
| MD5: | 5d6cccddcb88cb.. |
| SHA1: | 18e29b4aaad7d4. |
| SHA256: | 1dfc8108548442.. |
| Tags: | 32 arm elf mirai |
| Infos: | |

### Detection



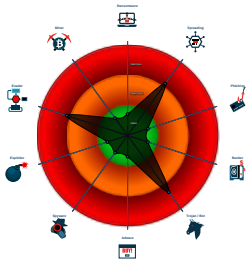

Mirai

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

### Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- 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

### 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: | 34.0.0 Boulder Opal |
| Analysis ID: | 626466 |
| Start date and time: 14/05/202204:00:30 | 2022-05-14 04:00:30 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 19s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 0vFX7VXc9U |
| 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.spre.troj.evad.lin@0/0@0/0 |

## Warnings

### Runtime Messages

| | |
|---|---|
| Command: | /tmp/0vFX7VXc9U |
| PID: | 6229 |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | Connected To CNC |

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

## Process Tree

- **system is lnxubuntu20**
- 0vFX7VXc9U (PID: 6229, Parent: 6122, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/0vFX7VXc9U
  - 0vFX7VXc9U New Fork (PID: 6231, Parent: 6229)
  - 0vFX7VXc9U New Fork (PID: 6233, Parent: 6229)
  - 0vFX7VXc9U New Fork (PID: 6235, Parent: 6229)
    - 0vFX7VXc9U New Fork (PID: 6237, Parent: 6235)
    - 0vFX7VXc9U New Fork (PID: 6239, Parent: 6235)
    - 0vFX7VXc9U 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

### Networking

Uses known network protocols on non-standard ports

### System Summary

Sample tries to kill multiple processes (SIGKILL)

### Data Obfuscation

Sample is packed with UPX

### Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

### Stealing of Sensitive Information

Yara detected Mirai

Yara detected Mirai

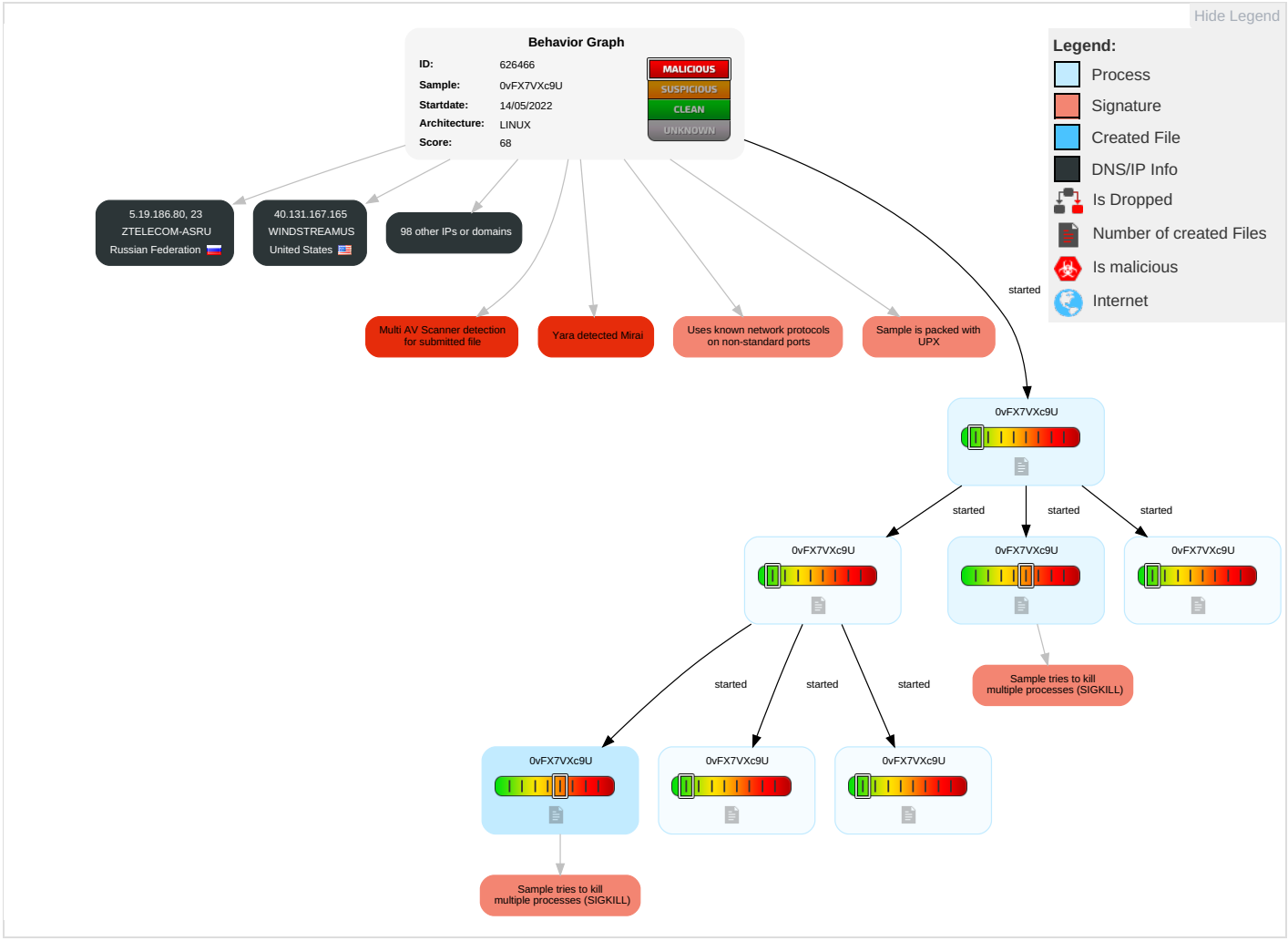
## Mitre Att&ck Matrix

| 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 Obfuscated Files or Information | 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 | 1 Service Stop |
| 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 |
|---|---|---|---|---|
| 0vFX7VXc9U | 40% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

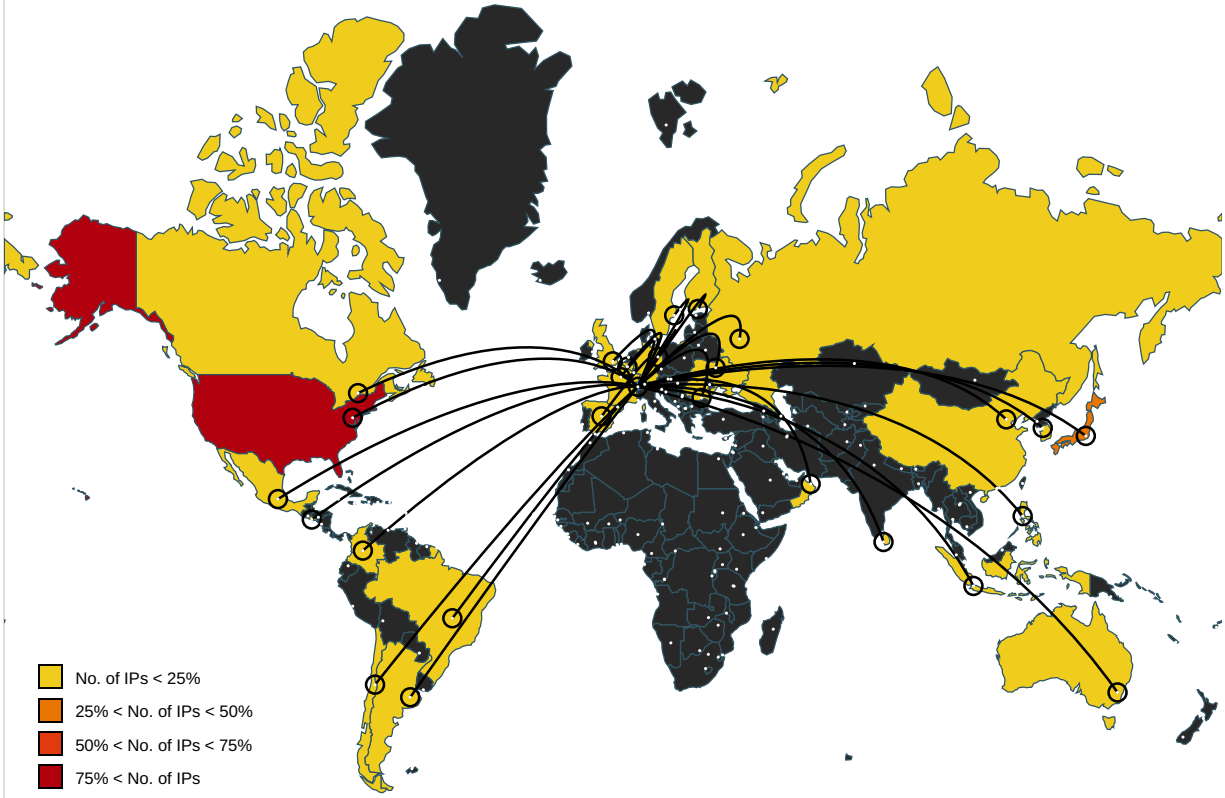
## Domains and IPs

### 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 |
|---|---|---|---|---|---|---|
| 159.199.38.171 | unknown | United States | | 11363 | FUJITSU-USAUS | false |
| 126.210.129.155 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 193.197.13.107 | unknown | Germany | | 553 | BELWUEBelWue-KoordinationEU | false |
| 38.162.241.46 | unknown | United States | | 174 | COGENT-174US | false |
| 158.34.190.148 | unknown | United States | | 721 | DNIC-ASBLK-00721-00726US | false |
| 17.68.111.77 | unknown | United States | | 714 | APPLE-ENGINEERINGUS | false |
| 202.211.43.114 | unknown | Japan | | 23637 | BI-CDN-IXEquinixJpapanEnterpriseKKJP | false |
| 58.49.78.189 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 187.44.116.221 | unknown | Brazil | | 28303 | UNASSIGNED | false |
| 167.194.166.140 | unknown | United States | | 2897 | GEORGIA-1US | false |
| 155.103.234.205 | unknown | United States | | 17055 | UTAHUS | false |
| 117.20.6.89 | unknown | Australia | | 45671 | AS45671-NET-AUWholesaleServicesProviderAU | false |
| 123.123.10.10 | unknown | China | | 4808 | CHINA169-BJChinaUnicomBeijingProvinceNetworkCN | false |
| 211.215.142.151 | unknown | Korea Republic of | | 9318 | SKB-ASSKBroadbandCoLtdKR | false |
| 184.183.128.14 | unknown | United States | | 22773 | ASN-CXA-ALL-CCI-22773-RDCUS | false |
| 27.91.141.132 | unknown | Japan | | 2516 | KDDIKDDICORPORATIONJP | false |
| 191.69.208.120 | unknown | Colombia | | 26611 | COMCELSACO | false |
| 179.181.230.189 | unknown | Brazil | | 18881 | TELEFONICABRASILSABR | false |
| 106.178.36.12 | unknown | Japan | | 2516 | KDDIKDDICORPORATIONJP | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 79.212.37.114 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 242.191.215.50 | unknown | Reserved | | unknown | unknown | false |
| 173.159.96.56 | unknown | United States | | 10507 | SPCSUS | false |
| 192.70.114.91 | unknown | France | | 2200 | FR-RENATERReseauNationaldetelecommunicationspourlaTec | false |
| 188.65.30.16 | unknown | Oman | | 15679 | CISOM | false |
| 252.233.33.84 | unknown | Reserved | | unknown | unknown | false |
| 155.174.155.129 | unknown | United States | | 797 | AMERITECH-ASUS | false |
| 190.87.78.146 | unknown | El Salvador | | 14754 | TelguaGT | false |
| 18.132.24.3 | unknown | United States | | 16509 | AMAZON-02US | false |
| 112.135.85.14 | unknown | Sri Lanka | | 9329 | SLTINT-AS-APSriLankaTelecomInternetLK | false |
| 122.238.160.53 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 63.222.211.96 | unknown | United States | | 3491 | BTN-ASNUS | false |
| 47.111.235.144 | unknown | China | | 37963 | CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd | false |
| 60.78.199.133 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 113.151.235.184 | unknown | Japan | | 2516 | KDDIKDDICORPORATIONJP | false |
| 210.151.10.111 | unknown | Japan | | 4725 | ODNSoftBankMobileCorpJP | false |
| 67.150.211.85 | unknown | United States | | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 221.161.108.168 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 172.127.100.178 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 241.170.151.161 | unknown | Reserved | | unknown | unknown | false |
| 209.221.88.255 | unknown | Canada | | 17054 | AS17054US | false |
| 255.103.13.193 | unknown | Reserved | | unknown | unknown | false |
| 216.46.11.151 | unknown | Canada | | 11478 | OPENFACECA | false |
| 189.197.247.189 | unknown | Mexico | | 13999 | MegaCableSAdeCVMX | false |
| 145.245.19.10 | unknown | Switzerland | | 2047 | ASN-ROCHE-BASLEGlobalcorporateIPnetworkCH | false |
| 57.62.76.32 | unknown | Belgium | | 2686 | ATGS-MMD-ASUS | false |
| 202.231.94.147 | unknown | Japan | | 2519 | VECTANTARTERIANetworksCorporationJP | false |
| 135.166.174.163 | unknown | United States | | 14962 | NCR-252US | false |
| 165.26.68.176 | unknown | United States | | 14381 | CATERPILLAR-INCUS | false |
| 147.147.16.159 | unknown | United Kingdom | | 6871 | PLUSNETUKInternetServiceProviderGB | false |
| 4.138.164.110 | unknown | United States | | 3356 | LEVEL3US | false |
| 34.38.58.196 | unknown | United States | | 2686 | ATGS-MMD-ASUS | false |
| 84.239.71.93 | unknown | France | | 20926 | PULSATION-ASFR | false |
| 152.47.196.81 | unknown | United States | | 81 | NCRENUS | false |
| 188.103.181.52 | unknown | Germany | | 3209 | VODANETInternationalIP-BackboneofVodafoneDE | false |
| 85.186.170.195 | unknown | Romania | | 6830 | LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding | false |
| 34.66.240.213 | unknown | United States | | 139070 | GOOGLE-AS-APGoogleAsiaPacificPteLtdSG | false |
| 20.151.130.134 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 177.167.27.22 | unknown | Brazil | | 26615 | TIMSABR | false |
| 247.149.253.146 | unknown | Reserved | | unknown | unknown | false |
| 243.95.58.195 | unknown | Reserved | | unknown | unknown | false |
| 5.19.186.80 | unknown | Russian Federation | | 41733 | ZTELECOM-ASRU | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 62.8.167.45 | unknown | Germany | | 20676 | PLUSNETDE | false |
| 68.40.94.171 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 176.67.2.141 | unknown | Ukraine | | 25133 | MCLAUT-ASUA | false |
| 110.3.119.105 | unknown | Japan | | 10013 | FBDCFreeBitCoLtdJP | false |
| 24.232.201.65 | unknown | Argentina | | 10318 | TelecomArgentinaSAAR | false |
| 24.237.4.6 | unknown | United States | | 8047 | GCIUS | false |
| 58.253.21.183 | unknown | China | | 17622 | CNCGROUP-GZChinaUnicomGuangzhounetworkCN | false |
| 212.214.203.146 | unknown | Sweden | | 3246 | TDCSONGTele2BusinessTDCSwedenSE | false |
| 47.19.240.28 | unknown | United States | | 6128 | CABLE-NET-1US | false |
| 79.94.237.131 | unknown | France | | 15557 | LDCOMNETFR | false |
| 12.170.33.63 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 35.115.167.133 | unknown | United States | | 237 | MERIT-AS-14US | false |
| 40.131.167.165 | unknown | United States | | 7029 | WINDSTREAMUS | false |
| 168.223.68.65 | unknown | United States | | 7202 | FAMUUS | false |
| 251.241.122.248 | unknown | Reserved | | unknown | unknown | false |
| 188.102.19.180 | unknown | Germany | | 3209 | VODANETInternationalIP-BackboneofVodafoneDE | false |
| 121.137.248.232 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 5.40.190.26 | unknown | Spain | | 43160 | ES-MDC-DATACENTERMalagaDataCenterES | false |
| 92.175.5.148 | unknown | France | | 3215 | FranceTelecom-OrangeFR | false |
| 201.188.216.73 | unknown | Chile | | 7418 | TELEFONICACHILESACL | false |
| 120.168.146.194 | unknown | Indonesia | | 4761 | INDOSAT-INP-APINDOSATInternetNetworkProviderID | false |
| 242.205.249.210 | unknown | Reserved | | unknown | unknown | false |
| 129.3.73.40 | unknown | United States | | 14433 | SUNY-OSWEGO-ASNUS | false |
| 135.251.35.234 | unknown | United States | | 10455 | LUCENT-CIOUS | false |
| 192.89.10.120 | unknown | Finland | | 1759 | TSF-IP-CORETeliaFinlandOyjEU | false |
| 250.57.212.23 | unknown | Reserved | | unknown | unknown | false |
| 36.118.159.83 | unknown | China | | 4847 | CNIX-APChinaNetworksInter-ExchangeCN | false |
| 24.69.73.98 | unknown | Canada | | 6327 | SHAWCA | false |
| 117.53.253.20 | unknown | Korea Republic of | | 9770 | SPEEDONSTV-AS-KRLGHelloVisionCorpKR | false |
| 253.198.199.189 | unknown | Reserved | | unknown | unknown | false |
| 113.35.47.165 | unknown | Japan | | 17506 | UCOMARTERIANetworksCorporationJP | false |
| 31.53.204.8 | unknown | United Kingdom | | 2856 | BT-UK-ASBTnetUKRegionalnetworkGB | false |
| 194.223.115.79 | unknown | United Kingdom | | 138384 | RMNI-AS-APRakutenMobileNetworkInc JP | false |
| 254.55.175.61 | unknown | Reserved | | unknown | unknown | false |
| 186.112.241.175 | unknown | Colombia | | 3816 | COLOMBIATELECOMUNICACIONESSAESPCO | false |
| 202.137.122.48 | unknown | Philippines | | 38553 | DCTECHDVO-AS-APInternetServiceProviderandDataCenterP | false |
| 119.109.212.116 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 45.25.50.42 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 99.11.105.169 | unknown | United States | | 7018 | ATT-INTERNET4US | 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, version 1 (ARM), statically linked, stripped |
| Entropy (8bit): | 7.929417373612622 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | 0vFX7VXc9U |
| File size: | 25004 |
| MD5: | 5d6cccddcb88cb4daefbc964e23de098 |
| SHA1: | 18e29b4aaad7d49a2b2adba64387494c6590c8dc |
| SHA256: | 1dfc810854844288a6f5c6b1e8dc25059bcff19c5585773956e568eaa4794970 |
| SHA512: | 1847514de3f1c5940ffead1621460b99b793b3f80550397985e8ac6672cafa5950e5bcaf9a66d605b5847052183cf934a1cc5e7ef1bb1d1ad0aa71d11abf793e |
| SSDEEP: | 768:5X9nxn8o9wnBoWzEQf2EjKb3pOIs3UozH:5tn+o9wjfBAZO9zH |
| TLSH: | 21B2D0727015F8B7C7E600B76AEDCA83FA800EF8D0E8B3291465099DE9D4846BBF1547 |
| File Content Preview: | .ELF...a.....(.....4.....4. ...(.....`...`.....^.....Q.td.....CvUPX!.....0...0.....R.....?.E.h;.}...^.....f.Z.6..<br>(fw....&.x:.E.....oe.`.S..T.....n.. |

### Static ELF Info

#### ELF header

| | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, little endian |
| Version: | 1 (current) |
| Machine: | ARM |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | ARM - ABI |
| ABI Version: | 0 |
| Entry Point Address: | 0xcf10 |
| Flags: | 0x202 |
| ELF Header Size: | 52 |

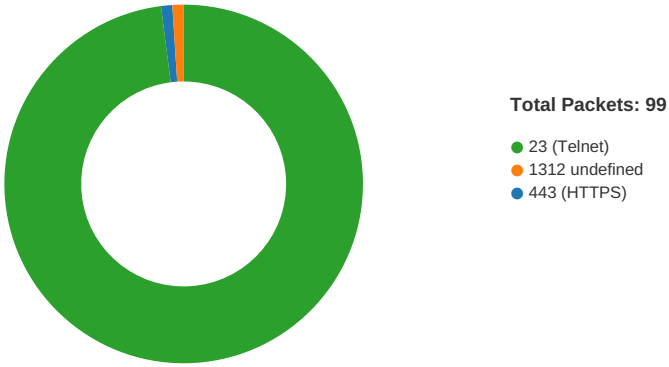
| ELF header | |
|---|---|
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 0 |
| Section Header Size: | 40 |
| Number of Section Headers: | 0 |
| Header String Table Index: | 0 |

**Program Segments**

| Type | Offset | Virtual Address | Physical Address | File Size | Memory Size | Entropy | Flags | Flags Description | Align | Prog Interpreter | Section Mappings |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LOAD | 0x0 | 0x8000 | 0x8000 | 0x60bf | 0x60bf | 4.0486 | 0x5 | R E | 0x8000 | | |
| LOAD | 0x5ee0 | 0x1dee0 | 0x1dee0 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x8000 | | |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

# Network Behavior

## Network Port Distribution




## TCP Packets

# System Behavior

## Analysis Process: 0vFX7VXc9U PID: 6229, Parent PID: 6122

### General

| | |
|---|---|
| Start time: | 04:06:46 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | /tmp/0vFX7VXc9U |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

#### File Read

## Analysis Process: 0vFX7VXc9U PID: 6231, Parent PID: 6229

### General

| | |
|---|---|
| Start time: | 04:06:47 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

**File Read**

**Directory Enumerated**

## Analysis Process: 0vFX7VXc9U PID: **6233**, Parent PID: **6229**

### General

| | |
|---|---|
| Start time: | 04:06:47 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: 0vFX7VXc9U PID: **6235**, Parent PID: **6229**

### General

| | |
|---|---|
| Start time: | 04:06:47 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: 0vFX7VXc9U PID: **6237**, Parent PID: **6235**

### General

| | |
|---|---|
| Start time: | 04:06:47 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

**File Read**

**Directory Enumerated**

## Analysis Process: 0vFX7VXc9U PID: **6239**, Parent PID: **6235**

### General

| | |
|---|---|
| Start time: | 04:06:47 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: 0vFX7VXc9U PID: **6240**, Parent PID: **6235**

### General

| | |
|---|---|
| Start time: | 04:06:47 |
| Start date: | 14/05/2022 |
| Path: | /tmp/0vFX7VXc9U |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |