
**ID:** 514643
**Sample Name:** QX4Kudvf1x
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 14:01:57
**Date:** 03/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

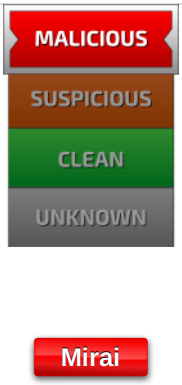
# Linux Analysis Report QX4Kudvf1x

## Overview

### General Information

| | |
|---|---|
| Sample Name: | QX4Kudvf1x |
| Analysis ID: | 514643 |
| MD5: | 5fe33cf30e900cb.. |
| SHA1: | 92f9cdbf6ca4efd… |
| SHA256: | 5be14a462004f55. |
| Tags: | 32 elf mirai motorola |
| Infos: | |

### Detection

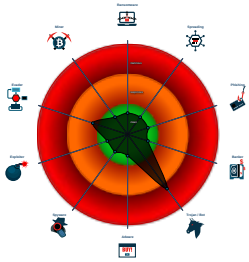



| | |
|---|---|
| Score: | 64 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### 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…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket

### Classification



### Analysis Advice

**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: | 514643 |
| Start date: | 03.11.2021 |
| Start time: | 14:01:57 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 17s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | QX4Kudvf1x |
| 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: | Show All |

## Process Tree

- **system is lnxubuntu20**
- QX4Kudvf1x (PID: 5239, Parent: 5115, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/QX4Kudvf1x
  - QX4Kudvf1x New Fork (PID: 5241, Parent: 5239)
  - QX4Kudvf1x New Fork (PID: 5242, Parent: 5239)
    - QX4Kudvf1x New Fork (PID: 5244, Parent: 5242)
    - QX4Kudvf1x New Fork (PID: 5246, Parent: 5242)
- **cleanup**

# Yara Overview

## PCAP (Network Traffic)

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

# Jbx Signature Overview


Click to jump to signature section

## 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

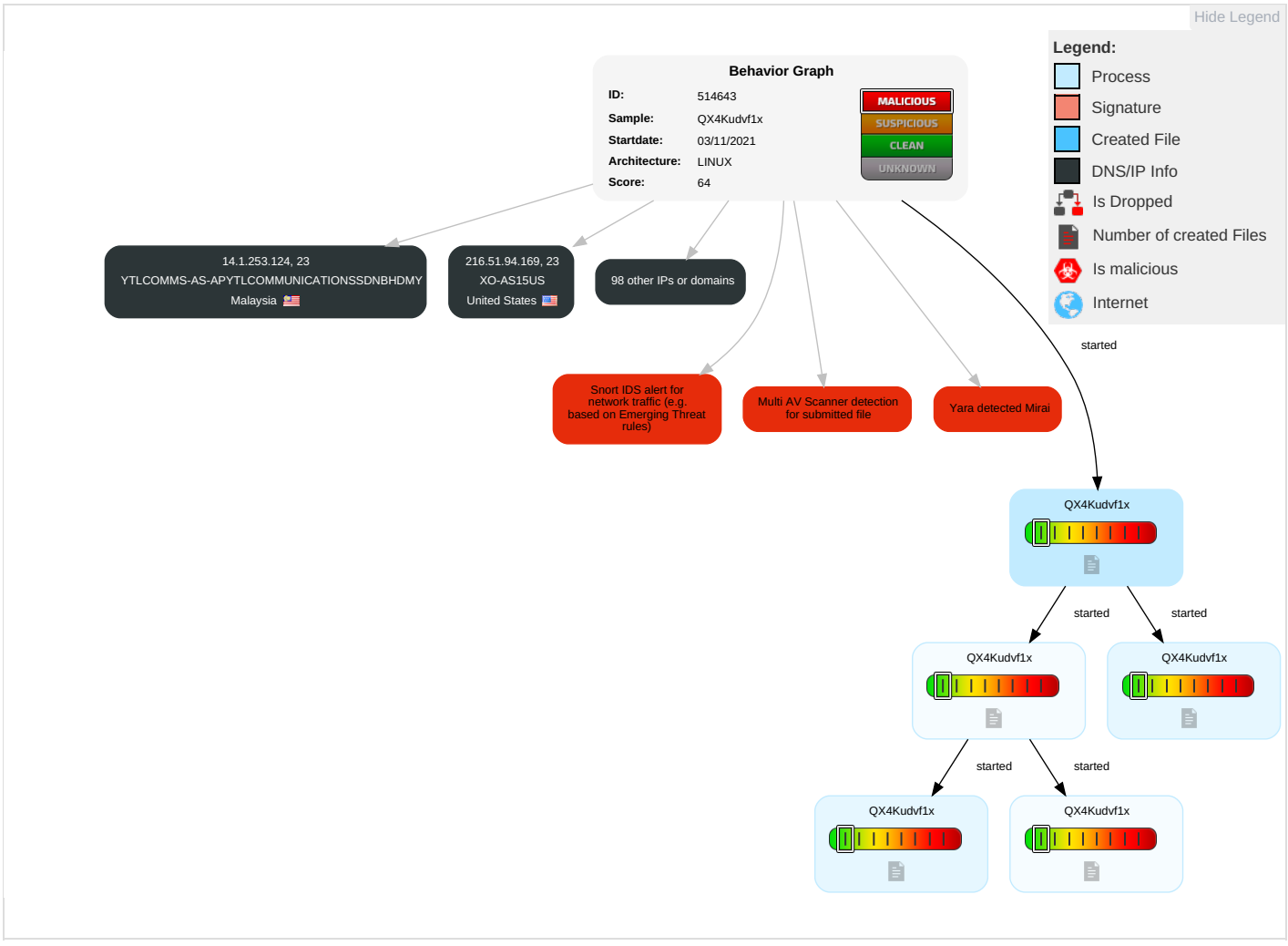
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid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

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
|---|---|---|---|---|
| QX4Kudvf1x | 49% | Virustotal | | Browse |
| QX4Kudvf1x | 49% | 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 |
|---|---|---|---|---|---|---|
| 207.252.253.15 | unknown | United States | | 10844 | VASTNETUS | false |
| 87.174.170.218 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 170.215.1.123 | unknown | United States | | 7011 | FRONTIER-AND-CITIZENSUS | false |
| 64.215.59.186 | unknown | United States | | 3549 | LVLT-3549US | false |
| 209.188.192.81 | unknown | United States | | 2152 | CSUNET-NWUS | false |
| 12.248.178.247 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 69.8.94.83 | unknown | United States | | 8025 | BRIGHTOK-ASUS | false |
| 42.93.143.143 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 71.9.12.218 | unknown | United States | | 20115 | CHARTER-20115US | false |
| 19.113.39.80 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 140.12.77.152 | unknown | United States | | 23700 | FASTNET-AS-IDLinknet-FastnetASNID | false |
| 187.114.120.15 | unknown | Brazil | | 18881 | TELEFONICABRASILSABR | false |
| 99.207.129.35 | unknown | United States | | 10507 | SPCSUS | false |
| 104.144.45.85 | unknown | Canada | | 55286 | SERVER-MANIACA | false |
| 186.27.91.17 | unknown | Bolivia | | 28024 | NuevatelPCSdeBoliviaSABO | false |
| 150.163.105.17 | unknown | Brazil | | 1916 | AssociacaoRedeNacionaldeEnsinoePesquisaBR | false |
| 194.136.239.177 | unknown | Finland | | 719 | ELISA-ASHelsinkiFinlandEU | false |
| 93.173.196.81 | unknown | Israel | | 1680 | NV-ASNCELLCOMltdIL | false |
| 149.209.248.84 | unknown | Norway | | 2830 | MCI-DUAL-HOMED-CUSTOMERSGB | false |
| 161.108.200.86 | unknown | United States | | 3955 | WANG-US-1US | false |
| 46.172.91.173 | unknown | Ukraine | | 48422 | IT-STARCOM-AShttpwwwitstarcomnetUA | false |
| 61.179.183.141 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 82.239.146.208 | unknown | France | | 12322 | PROXADFR | false |
| 17.153.147.49 | unknown | United States | | 714 | APPLE-ENGINEERINGUS | false |
| 1.61.30.168 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 36.212.52.156 | unknown | China | | 9394 | CTTNETChinaTieTongTelecommunicationsCorporationCN | false |
| 90.17.49.162 | unknown | France | | 3215 | FranceTelecom-OrangeFR | false |
| 219.47.227.225 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 178.192.115.23 | unknown | Switzerland | | 3303 | SWISSCOMSwisscomSwitzerlandLtdCH | false |
| 153.14.218.209 | unknown | United States | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 82.27.173.98 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 84.46.182.188 | unknown | Lithuania | | 15419 | LRTC-ASLT | false |
| 92.117.4.8 | unknown | Germany | | 8881 | VERSATELDE | false |
| 106.117.45.97 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 143.146.199.87 | unknown | United States | | 399 | AFCONC-BLOCK1-ASUS | false |
| 37.177.110.215 | unknown | Italy | | 30722 | VODAFONE-IT-ASNIT | false |
| 178.24.145.59 | unknown | Germany | | 31334 | KABELDEUTSCHLAND-ASDE | false |
| 212.79.253.142 | unknown | Germany | | 203507 | AVIRADEKaplaneiweg1DE | false |
| 210.48.212.143 | unknown | Australia | | 38084 | ETHAN-AU-APEthanGroupAU | false |
| 94.241.196.54 | unknown | Russian Federation | | 12389 | ROSTELECOM-ASRU | false |
| 165.166.229.161 | unknown | United States | | 2711 | SPIRITTEL-ASUS | false |
| 139.39.35.7 | unknown | United States | | 5972 | DNIC-ASBLK-05800-06055US | false |
| 138.185.157.196 | unknown | Brazil | | 264342 | UPNETPROVEDORDEACESSOETELECOMBR | false |
| 24.142.43.136 | unknown | Canada | | 32233 | PERSONACA | false |
| 86.210.197.248 | unknown | France | | 3215 | FranceTelecom-OrangeFR | false |
| 125.136.218.237 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 192.36.40.33 | unknown | Sweden | | 25176 | AC-NETSE | false |
| 173.25.184.131 | unknown | United States | | 30036 | MEDIACOM-ENTERPRISE-BUSINESSUS | false |
| 57.249.89.90 | unknown | Belgium | | 2686 | ATGS-MMD-ASUS | false |
| 110.19.130.27 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOM China169BackboneCN | false |
| 150.142.226.27 | unknown | United States | | 14223 | NYSDOHUS | false |
| 14.1.253.124 | unknown | Malaysia | | 45960 | YTLCOMMS-AS-APYTLCOMMUNICATIONS SDNBHDMY | false |
| 31.40.126.0 | unknown | Russian Federation | | 56761 | MULTINEX-MIASS-ASRU | false |
| 213.5.165.223 | unknown | Russian Federation | | 15673 | TELESETI-PLUS-ASRU | false |
| 135.248.152.229 | unknown | United States | | 10455 | LUCENT-CIOUS | false |
| 46.215.117.92 | unknown | Poland | | 8374 | PLUSNETPlusnetworkoperatorinPolandPL | false |
| 118.123.103.213 | unknown | China | | 38283 | CHINANET-SCIDC-AS-APCHINANETSiChuanTelecomInternetData | false |
| 209.15.189.55 | unknown | Canada | | 11290 | CC-3272CA | false |
| 191.160.73.87 | unknown | Brazil | | 26615 | TIMSABR | false |
| 206.116.23.4 | unknown | Canada | | 852 | ASN852CA | false |
| 36.173.8.143 | unknown | China | | 9808 | CMNET-GDGuangdongMobileCommunicationCoLtdCN | false |
| 122.202.143.12 | unknown | Korea Republic of | | 9946 | CABLENET-AS-KRKCTVJEJUBROADCASTINGKR | false |
| 172.132.121.255 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 125.227.201.219 | unknown | Taiwan; Republic of China (ROC) | | 3462 | HINETDataCommunicationBusinessGroupTW | false |
| 132.213.80.133 | unknown | Canada | | 376 | RISQ-ASCA | false |
| 142.10.232.203 | unknown | Canada | | 13576 | SDNW-13576US | false |
| 111.48.103.28 | unknown | China | | 9808 | CMNET-GDGuangdongMobileCommunicationCoLtdCN | false |
| 208.254.25.78 | unknown | United States | | 11486 | COLO-PREM-VZBUS | false |
| 161.64.39.252 | unknown | Macau | | 7582 | UMAC-AS-APUniversityofMacauMO | false |
| 82.32.247.245 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 61.197.166.78 | unknown | Japan | | 2514 | INFOSPHERENTTPCCommunicationsIncJP | false |
| 12.16.138.186 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 83.47.191.245 | unknown | Spain | | 3352 | TELEFONICA_DE_ESPANA ES | false |
| 168.76.73.116 | unknown | South Africa | | 265240 | ULTRANETSERVICOSEMINTERNETLTDABR | false |
| 179.138.235.187 | unknown | Brazil | | 26599 | TELEFONICABRASILSABR | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 94.79.60.224 | unknown | Russian Federation | | 8732 | COMCOR-ASMoscowRU | false |
| 131.44.242.127 | unknown | United States | | 385 | AFCONC-BLOCK1-ASUS | false |
| 104.19.61.172 | unknown | United States | | 13335 | CLOUDFLARENETUS | false |
| 148.22.80.216 | unknown | United States | | 6400 | CompaniaDominicanadeTelefonosSADO | false |
| 114.99.197.138 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 162.32.169.48 | unknown | United States | | 35893 | ACPCA | false |
| 86.173.157.118 | unknown | United Kingdom | | 2856 | BT-UK-ASBTnetUKRegionalnetworkGB | false |
| 216.51.94.169 | unknown | United States | | 2828 | XO-AS15US | false |
| 206.249.88.101 | unknown | United States | | 174 | COGENT-174US | false |
| 204.29.221.41 | unknown | United States | | 13325 | STOMIUS | false |
| 2.98.162.245 | unknown | United Kingdom | | 13285 | OPALTELECOM-ASTalkTalkCommunicationsLimitedGB | false |
| 19.71.89.200 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 70.74.179.170 | unknown | Canada | | 6327 | SHAWCA | false |
| 64.148.234.59 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 150.170.41.46 | unknown | United States | | 26438 | MONROE-COMMUNITY-COLLEGEUS | false |
| 97.61.226.168 | unknown | United States | | 22394 | CELLCOUS | false |
| 149.214.42.119 | unknown | Germany | | 5605 | NETUSEDE | false |
| 176.251.72.11 | unknown | United Kingdom | | 5607 | BSKYB-BROADBAND-ASGB | false |
| 69.199.77.191 | unknown | United States | | 17184 | ATL-CBEYONDUS | false |
| 87.17.71.206 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 161.16.200.200 | unknown | United States | | 19512 | LYONDELLUS | false |
| 207.82.211.10 | unknown | United States | | 10584 | TRADEWEBUS | false |
| 73.207.81.13 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 221.246.215.107 | unknown | Japan | | 17506 | UCOMARTERIANetworksCorporationJP | false |
| 38.52.110.100 | unknown | United States | | 174 | COGENT-174US | false |

## Runtime Messages

| | |
|---|---|
| Command: | /tmp/QX4Kudvf1x |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | JEW was here lol |
| Standard Error: | |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 187.114.120.15 | AD0cHN7dR2 | Get hash | malicious | Browse | |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| VASTNETUS | arm7-20211013-0650 | Get hash | malicious | Browse | • 207.252.204.98 |
| | LsgCcJSqnz | Get hash | malicious | Browse | • 207.252.216.85 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | sora.x86 | Get hash | malicious | Browse | • 207.252.228.91 |
| | E2ecGhjXtG | Get hash | malicious | Browse | • 207.252.216.89 |
| | eOtLRCQr22 | Get hash | malicious | Browse | • 207.252.228.60 |
| | i5aeHz4aJM | Get hash | malicious | Browse | • 207.252.25 3.102 |
| DTAGInternetserviceprovideroperationsDE | b3astmode.arm | Get hash | malicious | Browse | • 217.4.69.177 |
| | cavEG2l8fj | Get hash | malicious | Browse | • 2.170.90.44 |
| | nY0UOuOPzl | Get hash | malicious | Browse | • 84.187.195.54 |
| | arm7-20211103-0152 | Get hash | malicious | Browse | • 84.137.48.47 |
| | x86-20211103-0152 | Get hash | malicious | Browse | • 91.29.31.39 |
| | sora.arm | Get hash | malicious | Browse | • 79.237.66.215 |
| | sora.x86 | Get hash | malicious | Browse | • 217.237.3.225 |
| | sora.arm | Get hash | malicious | Browse | • 93.204.166.84 |
| | sora.arm7 | Get hash | malicious | Browse | • 79.254.97.190 |
| | sora.arm | Get hash | malicious | Browse | • 84.144.143.146 |
| | sora.arm7 | Get hash | malicious | Browse | • 80.132.249.121 |
| | WmEErPtdS9 | Get hash | malicious | Browse | • 87.154.68.57 |
| | sora.x86 | Get hash | malicious | Browse | • 87.180.143.9 |
| | sora.arm7 | Get hash | malicious | Browse | • 79.235.254.132 |
| | 6A9RyJXCd7 | Get hash | malicious | Browse | • 79.214.175.95 |
| | arm-20211102-0937 | Get hash | malicious | Browse | • 79.238.112.149 |
| | sora.arm7 | Get hash | malicious | Browse | • 93.221.174.122 |
| | sora.x86 | Get hash | malicious | Browse | • 91.26.71.219 |
| | sora.mips | Get hash | malicious | Browse | • 37.91.93.228 |
| | mips-20211102-0937 | Get hash | malicious | Browse | • 93.217.229.75 |
| FRONTIER-AND-CITIZENSUS | arm7-20211103-0152 | Get hash | malicious | Browse | • 74.34.248.64 |
| | sora.x86 | Get hash | malicious | Browse | • 74.33.14.3 |
| | dUW6YG1Tdv | Get hash | malicious | Browse | • 184.9.231.61 |
| | 7DoAjWX5uZ | Get hash | malicious | Browse | • 50.36.214.99 |
| | 1Y2rsDBP9s | Get hash | malicious | Browse | • 74.34.248.47 |
| | Yoshi.arm7 | Get hash | malicious | Browse | • 184.12.211.39 |
| | Yoshi.x86 | Get hash | malicious | Browse | • 184.13.242.168 |
| | HgTC70XRum | Get hash | malicious | Browse | • 184.14.58.56 |
| | INsMwWSMeh | Get hash | malicious | Browse | • 184.9.231.90 |
| | Tsunami.arm | Get hash | malicious | Browse | • 184.13.229.66 |
| | 07xBxVsvEn | Get hash | malicious | Browse | • 74.40.196.242 |
| | yZ7D7o1Z7p | Get hash | malicious | Browse | • 74.39.43.37 |
| | bKHI9UT0D1 | Get hash | malicious | Browse | • 184.13.205.31 |
| | IcwrPqGkXP | Get hash | malicious | Browse | • 184.11.40.157 |
| | BMP4Nk5TTq | Get hash | malicious | Browse | • 184.14.180.127 |
| | MMpysQ37RU | Get hash | malicious | Browse | • 65.73.206.158 |
| | 7SerHvEAjE | Get hash | malicious | Browse | • 74.42.216.110 |
| | hoho.arm7 | Get hash | malicious | Browse | • 170.215.191.1 |
| | 9aAl5Mt3Jz | Get hash | malicious | Browse | • 184.13.230.28 |
| | 4syAQhYxm8 | Get hash | malicious | Browse | • 184.13.230.53 |

## 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, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped |
| Entropy (8bit): | 6.2171470760115675 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | QX4Kudvf1x |
| File size: | 57092 |
| MD5: | 5fe33cf30e900cb2903960d16f1f3ace |
| SHA1: | 92f9cdbf6ca4efdb09a48714907913a74b70bf9e |
| SHA256: | 5be14a462004f551c39bae8155098090695e6dc2ad48219a7792bf4d28a364f9 |
| SHA512: | db84dc122a044bab4b3a605c188868135f6282930fe64a3b34d65668a7d9bbf92d0edbe206da7fbe1dcb9f061f826edabef0e9f4c5a7de71935c21957c81f1d |
| SSDEEP: | 768:uMHejQFpI44XZAJ0xwv6qOl35a7SP0ypuo8Wh2QCfBqntyzruCi:uc4QFpUZAJIwv6qwHsyIo8Wh6fBqozrg |
| File Content Preview: | .ELF.....D...4...t....4. ...(.....(..... .dt.Q.....NV..a....da....N^NuNV..J9...4f>"y...$ QJ.g.X.#....$N."y...$ QJ.f.A.....J.g.Hy....N.X.....4N^NuNV..N^NuN |

## Static ELF Info

### ELF header

| | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, big endian |
| Version: | 1 (current) |
| Machine: | MC68000 |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | UNIX - System V |
| ABI Version: | 0 |
| Entry Point Address: | 0x80000144 |
| Flags: | 0x0 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 56692 |
| Section Header Size: | 40 |
| Number of Section Headers: | 10 |
| Header String Table Index: | 9 |

### Sections

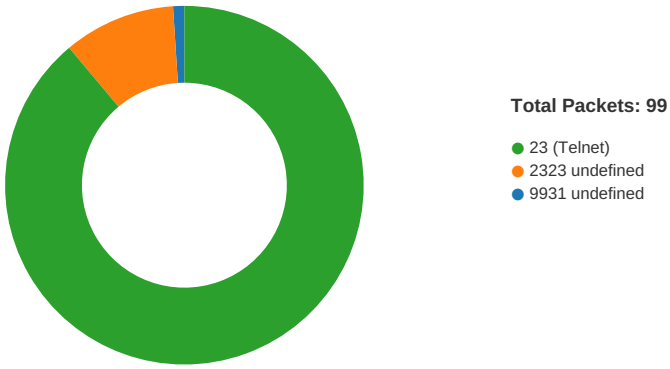
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x80000094 | 0x94 | 0x14 | 0x0 | 0x6 | AX | 0 | 0 | 2 |
| .text | PROGBITS | 0x800000a8 | 0xa8 | 0xd33e | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .fini | PROGBITS | 0x8000d3e6 | 0xd3e6 | 0xe | 0x0 | 0x6 | AX | 0 | 0 | 2 |
| .rodata | PROGBITS | 0x8000d3f4 | 0xd3f4 | 0x712 | 0x0 | 0x2 | A | 0 | 0 | 2 |
| .ctors | PROGBITS | 0x8000fb0c | 0xdb0c | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x8000fb14 | 0xdb14 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x8000fb20 | 0xdb20 | 0x214 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .bss | NOBITS | 0x8000fd34 | 0xdd34 | 0x2a8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .shstrtab | STRTAB | 0x0 | 0xdd34 | 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 | 0x80000000 | 0x80000000 | 0xdb06 | 0xdb06 | 4.2934 | 0x5 | R E | 0x2000 | | .init .text .fini .rodata |
| LOAD | 0xdb0c | 0x8000fb0c | 0x8000fb0c | 0x228 | 0x4d0 | 1.5122 | 0x6 | RW | 0x2000 | | .ctors .dtors .data .bss |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x4 | | |

# Network Behavior

## Network Port Distribution




## TCP Packets

# System Behavior

## Analysis Process: QX4Kudvf1x PID: 5239 Parent PID: 5115

### General

| | |
|---|---|
| Start time: | 14:02:43 |
| Start date: | 03/11/2021 |
| Path: | /tmp/QX4Kudvf1x |
| Arguments: | /tmp/QX4Kudvf1x |
| File size: | 4463432 bytes |
| MD5 hash: | cd177594338c77b895ae27c33f8f86cc |

### File Activities

#### File Read

## Analysis Process: QX4Kudvf1x PID: 5241 Parent PID: 5239

### General

| | |
|---|---|
| Start time: | 14:02:43 |
| Start date: | 03/11/2021 |
| Path: | /tmp/QX4Kudvf1x |
| Arguments: | n/a |
| File size: | 4463432 bytes |
| MD5 hash: | cd177594338c77b895ae27c33f8f86cc |

## Analysis Process: QX4Kudvf1x PID: 5242 Parent PID: 5239

### General

| | |
|---|---|
| Start time: | 14:02:43 |
| Start date: | 03/11/2021 |
| Path: | /tmp/QX4Kudvf1x |
| Arguments: | n/a |
| File size: | 4463432 bytes |
| MD5 hash: | cd177594338c77b895ae27c33f8f86cc |

## Analysis Process: QX4Kudvf1x PID: 5244 Parent PID: 5242

### General

| | |
|---|---|
| Start time: | 14:02:43 |
| Start date: | 03/11/2021 |
| Path: | /tmp/QX4Kudvf1x |
| Arguments: | n/a |
| File size: | 4463432 bytes |
| MD5 hash: | cd177594338c77b895ae27c33f8f86cc |

## Analysis Process: QX4Kudvf1x PID: 5246 Parent PID: 5242

### General

| | |
|---|---|
| Start time: | 14:02:43 |
| Start date: | 03/11/2021 |
| Path: | /tmp/QX4Kudvf1x |
| Arguments: | n/a |
| File size: | 4463432 bytes |
| MD5 hash: | cd177594338c77b895ae27c33f8f86cc |