
**ID:** 557442
**Sample Name:** arm
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 06:00:31
**Date:** 21/01/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents

# Linux Analysis Report

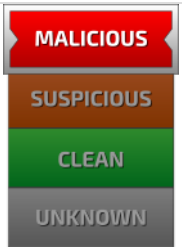
## arm

## Overview

### General Information

| | |
|---|---|
| Sample Name: | arm |
| Analysis ID: | 557442 |
| MD5: | c8eac6c41bd5f6… |
| SHA1: | ae41cee628bdac.. |
| SHA256: | b916d6f9d2756f3. |
| Tags: | Mirai |
| Infos: | |

### Detection



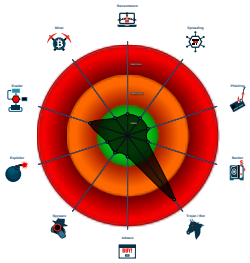

**Mirai Moobot**

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

### Signatures

- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Moobot
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…
- Uses the "uname" system call to qu…
- Executes the "chmod" command us…

### 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 only run correctly on MIPS or ARM architectures**

**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: | 557442 |
| Start date: | 21.01.2022 |
| Start time: | 06:00:31 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 0s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | arm |
| 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: | mal100.troj.lin@0/0@1/0 |

## Warnings

### Runtime Messages

| | |
|---|---|
| Command: | /tmp/arm |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | qazwsxedc |

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

## Process Tree

- **system is lnxubuntu20**
- arm (PID: 5201, Parent: 5115, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm
  - arm New Fork (PID: 5223, Parent: 5201)
  - sh (PID: 5223, Parent: 5201, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/arm bin/systemd; chmod 777 bin/systemd"
    - sh New Fork (PID: 5225, Parent: 5223)
    - rm (PID: 5225, Parent: 5223, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/systemd
    - sh New Fork (PID: 5226, Parent: 5223)
    - mkdir (PID: 5226, Parent: 5223, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 5227, Parent: 5223)
    - mv (PID: 5227, Parent: 5223, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/arm bin/systemd
    - sh New Fork (PID: 5228, Parent: 5223)
    - chmod (PID: 5228, Parent: 5223, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/systemd
  - arm New Fork (PID: 5229, Parent: 5201)
    - arm New Fork (PID: 5231, Parent: 5229)
- **cleanup**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| arm | Mirai_Botnet_Malware | Detects Mirai Botnet Malware | Florian Roth | • 0x12be8:$x1: POST /cdn-cgi/<br>• 0x12168:$x3: /dev/watchdog<br>• 0x122b4:$s1: LCOGQGPTGP |
| arm | MAL_ELF_LNX_Mirai_Oct10_2 | Detects ELF malware Mirai related | Florian Roth | • 0x12be8:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A |
| arm | JoeSecurity_Moobot | Yara detected Moobot | Joe Security | |
| arm | JoeSecurity_Mirai_5 | Yara detected Mirai | Joe Security | |
| arm | JoeSecurity_Mirai_9 | Yara detected Mirai | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 5201.1.000000002e6ad643.0000000062dfdce7.r-x.sdmp | Mirai_Botnet_Malware | Detects Mirai Botnet Malware | Florian Roth | • 0x12be8:$x1: POST /cdn-cgi/<br>• 0x12168:$x3: /dev/watchdog<br>• 0x122b4:$s1: LCOGQGPTGP |
| 5201.1.000000002e6ad643.0000000062dfdce7.r-x.sdmp | MAL_ELF_LNX_Mirai_Oct10_2 | Detects ELF malware Mirai related | Florian Roth | • 0x12be8:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A |
| 5201.1.000000002e6ad643.0000000062dfdce7.r-x.sdmp | JoeSecurity_Moobot | Yara detected Moobot | Joe Security | |
| 5201.1.000000002e6ad643.0000000062dfdce7.r-x.sdmp | JoeSecurity_Mirai_5 | Yara detected Mirai | Joe Security | |
| 5201.1.000000002e6ad643.0000000062dfdce7.r-x.sdmp | JoeSecurity_Mirai_9 | Yara detected Mirai | Joe Security | |

Click to see the 1 entries

## Jbx Signature Overview

### AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

### Networking

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

### System Summary

Malicious sample detected (through community Yara rule)

### Persistence and Installation Behavior

Sets full permissions to files and/or directories

### Stealing of Sensitive Information

Yara detected Mirai

Yara detected Moobot

### Remote Access Functionality

Yara detected Mirai

Yara detected Moobot

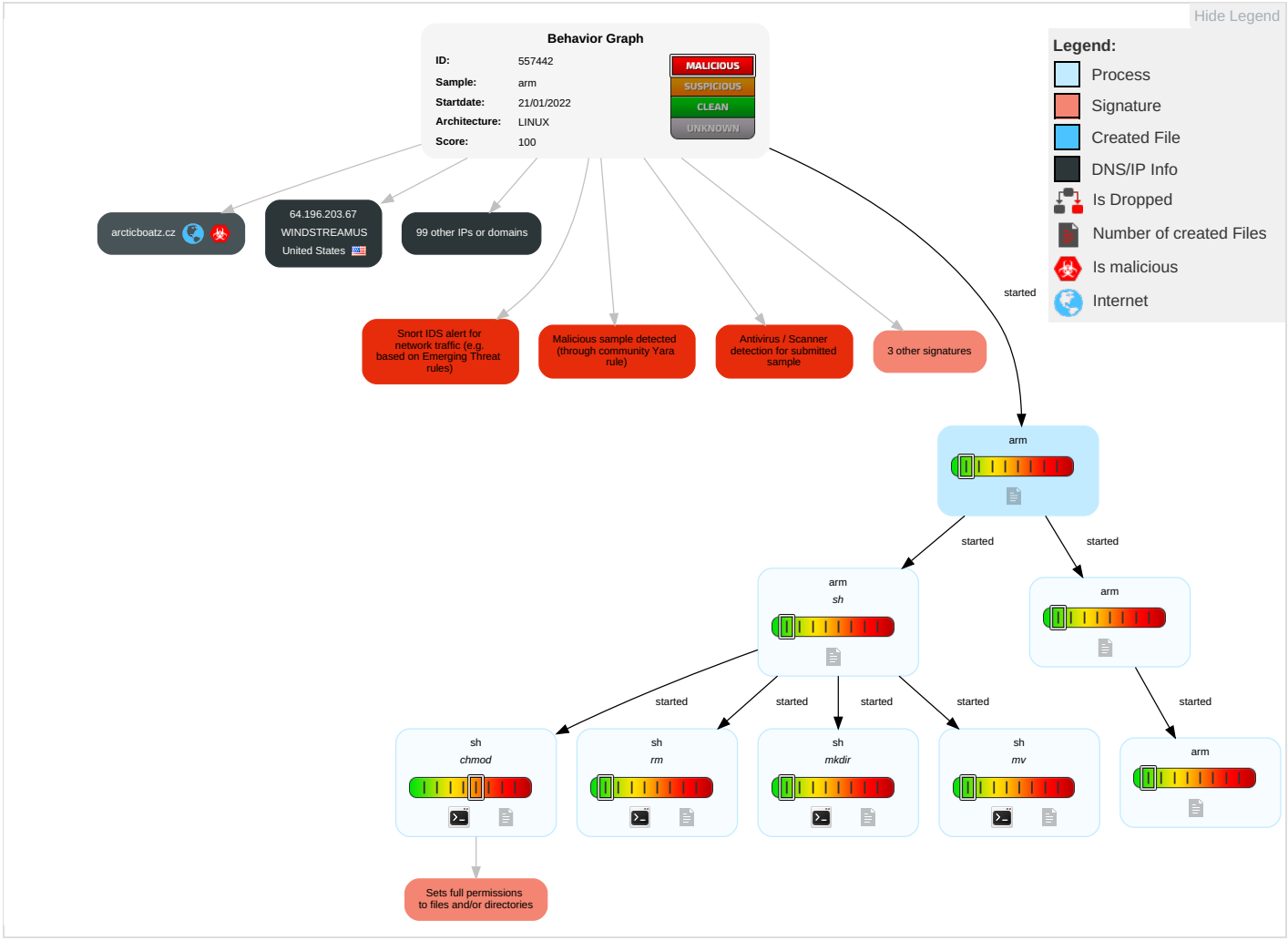
## Mitre Att&ck Matrix

| 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 | 1 Scripting | Path Interception | Path Interception | 2 File and Directory Permissions Modification | 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 | 1 Scripting | 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) | 1 File Deletion | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 1 Non-Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 2 Application Layer Protocol | SIM Card Swap | | Carrier Billing Fraud |

## Malware Configuration

No configs have been found

## Behavior Graph




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| arm | 39% | Virustotal | | Browse |
| arm | 50% | ReversingLabs | Linux.Trojan.Mirai | |
| arm | 100% | Avira | LINUX/Mirai.bonb | |

### Dropped Files

No Antivirus matches

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| arcticboatz.cz | 4% | Virustotal | | Browse |

### URLs

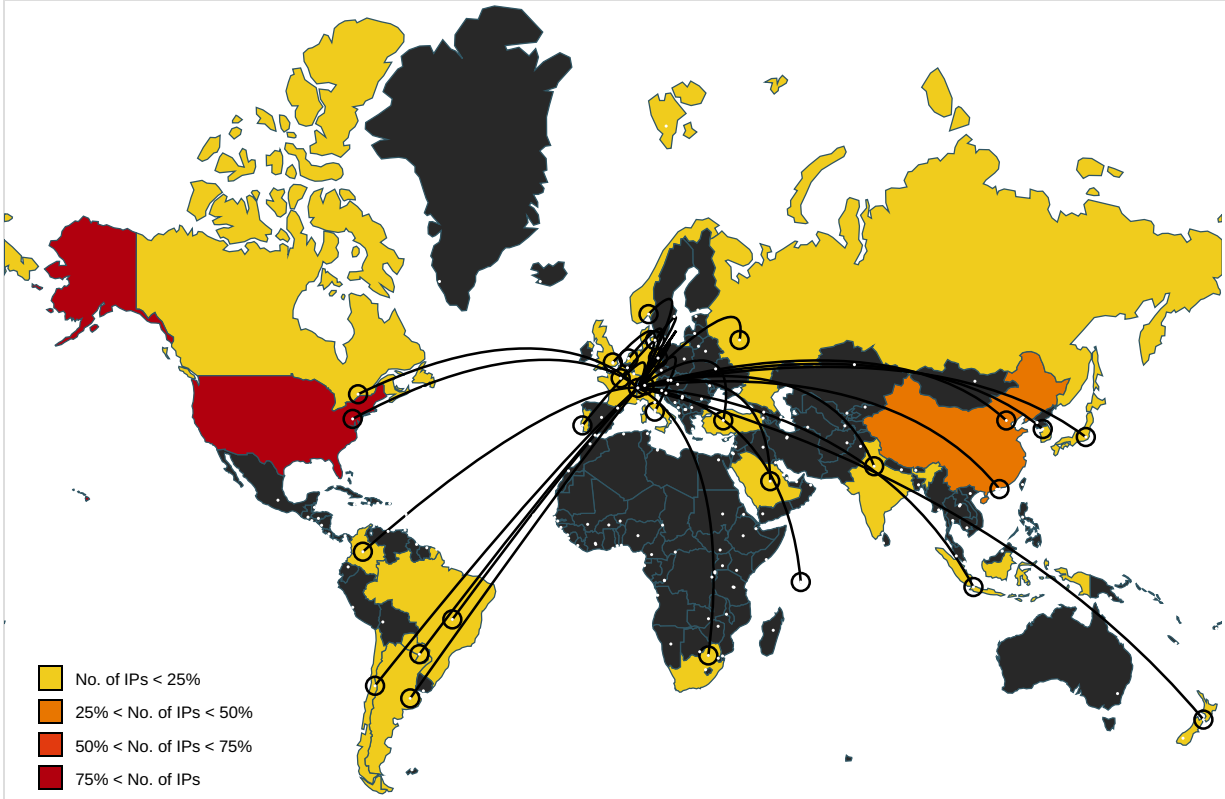
No Antivirus matches

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| arcticboatz.cz | 95.181.161.40 | true | true | • 4%, Virustotal, Browse | unknown |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 90.21.87.76 | unknown | France | | 3215 | FranceTelecom-OrangeFR | false |
| 39.70.211.12 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 191.151.188.107 | unknown | Colombia | | 26611 | COMCELSACO | false |
| 158.248.198.227 | unknown | Norway | | 29695 | ALTIBOX_ASNorwayNO | false |
| 152.55.146.223 | unknown | United States | | 81 | NCRENUS | false |
| 72.235.23.15 | unknown | United States | | 36149 | HAWAIIAN-TELCOMUS | false |
| 97.39.187.32 | unknown | United States | | 6167 | CELLCO-PARTUS | false |
| 153.247.68.182 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 80.208.170.47 | unknown | Switzerland | | 15600 | FINECOMQuicklineAGCH | false |
| 181.126.230.132 | unknown | Paraguay | | 23201 | TelecelSAPY | false |
| 74.169.133.116 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 82.117.30.106 | unknown | Liechtenstein | | 35223 | HOI-ASLI | false |
| 88.253.17.216 | unknown | Turkey | | 9121 | TTNETTR | false |
| 187.95.178.164 | unknown | Brazil | | 53090 | VianetTelecomunicacoesInternetBR | false |
| 138.142.32.215 | unknown | United States | | 721 | DNIC-ASBLK-00721-00726US | false |
| 58.210.29.106 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 46.138.231.194 | unknown | Russian Federation | | 25513 | ASN-MGTS-USPDRU | false |
| 91.53.126.192 | unknown | Germany | | 3320 | DTAGInternetserviceprovideroperationsDE | false |
| 23.49.42.170 | unknown | United States | | 16625 | AKAMAI-ASUS | false |
| 200.179.36.152 | unknown | Brazil | | 4230 | CLAROSABR | false |
| 80.166.163.211 | unknown | Denmark | | 3292 | TDCTDCASDK | false |
| 133.150.17.100 | unknown | Japan | | 10021 | KVHKVHCoLtdJP | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 176.224.147.61 | unknown | Saudi Arabia | | 35819 | MOBILY-ASEtihadEtisalatCompanyMobilySA | false |
| 1.69.204.55 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 216.37.77.119 | unknown | United States | | 21922 | WEBNETUS | false |
| 217.129.155.32 | unknown | Portugal | | 13156 | AS13156PalmelaPT | false |
| 163.218.53.125 | unknown | Japan | | 7502 | IP-KYOTOAdvancedSoftwareTechnologyManagementResearch | false |
| 141.21.45.141 | unknown | Germany | | 205046 | FZI-AS-1DE | false |
| 173.112.71.235 | unknown | United States | | 10507 | SPCSUS | false |
| 4.105.216.207 | unknown | United States | | 3356 | LEVEL3US | false |
| 165.52.21.238 | unknown | South Africa | | 37053 | RSAWEB-ASZA | false |
| 190.125.166.121 | unknown | Colombia | | 26611 | COMCELSACO | false |
| 162.107.199.176 | unknown | United States | | 17162 | DONALDSONUS | false |
| 191.223.166.113 | unknown | Brazil | | 8167 | BrasilTelecomSA-FilialDistritoFederalBR | false |
| 81.133.225.89 | unknown | United Kingdom | | 2856 | BT-UK-ASBTnetUKRegionalnetworkGB | false |
| 114.23.5.71 | unknown | New Zealand | | 56030 | VOYAGERNET-AS-APVoyagerInternetLtdNZ | false |
| 111.17.173.192 | unknown | China | | 24444 | CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany | false |
| 136.161.34.86 | unknown | United States | | 174 | COGENT-174US | false |
| 45.83.121.194 | unknown | Netherlands | | 200313 | INTERNET-ITNL | false |
| 153.193.162.150 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 1.104.172.183 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 200.151.155.13 | unknown | Brazil | | 7738 | TelemarNorteLesteSABR | false |
| 213.36.152.232 | unknown | France | | 12322 | PROXADFR | false |
| 61.15.226.39 | unknown | Hong Kong | | 9908 | HKCABLE2-HK-APHKCableTVLtdHK | false |
| 61.185.7.40 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 190.145.21.183 | unknown | Colombia | | 14080 | TelmexColombiaSACO | false |
| 201.176.134.4 | unknown | Argentina | | 22927 | TelefonicadeArgentinaAR | false |
| 125.82.123.197 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 74.33.205.71 | unknown | United States | | 7011 | FRONTIER-AND-CITIZENSUS | false |
| 132.97.141.117 | unknown | United States | | 306 | DNIC-ASBLK-00306-00371US | false |
| 154.197.40.201 | unknown | Seychelles | | 137443 | ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK | false |
| 151.141.190.160 | unknown | United States | | 29842 | ETSU-NETUS | false |
| 59.65.228.14 | unknown | China | | 4538 | ERX-CERNET-BKBChinaEducationandResearchNetworkCenter | false |
| 99.105.83.245 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 152.250.150.236 | unknown | Brazil | | 27699 | TELEFONICABRASILSABR | false |
| 27.201.102.121 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 189.71.43.234 | unknown | Brazil | | 7738 | TelemarNorteLesteSABR | false |
| 136.109.100.212 | unknown | United States | | 60311 | ONEFMCH | false |
| 82.45.153.218 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 144.67.166.155 | unknown | United States | | 3243 | MEO-RESIDENCIALPT | false |
| 207.34.108.176 | unknown | Canada | | 15247 | RADIANT-VANCOUVERCA | false |
| 191.49.3.3 | unknown | Brazil | | 26615 | TIMSABR | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 40.99.144.217 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 86.7.59.119 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 12.47.81.13 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 200.45.30.120 | unknown | Argentina | | 7303 | TelecomArgentinaSAAR | false |
| 48.171.205.123 | unknown | United States | | 2686 | ATGS-MMD-ASUS | false |
| 34.205.37.162 | unknown | United States | | 14618 | AMAZON-AESUS | false |
| 61.17.124.120 | unknown | India | | 17908 | TCISLTataCommunicationsIN | false |
| 4.19.212.157 | unknown | United States | | 3356 | LEVEL3US | false |
| 190.227.23.147 | unknown | Argentina | | 7303 | TelecomArgentinaSAAR | false |
| 60.0.108.189 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 153.12.215.116 | unknown | United States | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 54.17.208.21 | unknown | United States | | 14618 | AMAZON-AESUS | false |
| 84.208.212.180 | unknown | Norway | | 41164 | GET-NOGETNorwayNO | false |
| 117.54.211.86 | unknown | Indonesia | | 9340 | INDONET-AS-APINDOInternetPTID | false |
| 135.71.50.102 | unknown | United States | | 18676 | AVAYAUS | false |
| 152.241.175.204 | unknown | Brazil | | 26599 | TELEFONICABRASILSABR | false |
| 212.189.180.251 | unknown | Italy | | 137 | ASGARRConsortiumGARREU | false |
| 158.178.182.15 | unknown | United Kingdom | | 15830 | EQUINIX-CONNECT-EMEAGB | false |
| 173.28.235.234 | unknown | United States | | 30036 | MEDIACOM-ENTERPRISE-BUSINESSUS | false |
| 9.179.51.161 | unknown | United States | | 3356 | LEVEL3US | false |
| 151.250.30.253 | unknown | Turkey | | 34984 | TELLCOM-ASTR | false |
| 98.144.53.110 | unknown | United States | | 10796 | TWC-10796-MIDWESTUS | false |
| 134.235.160.137 | unknown | United States | | 1586 | DNIC-ASBLK-01550-01601US | false |
| 42.55.187.255 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 78.144.25.71 | unknown | United Kingdom | | 13285 | OPALTELECOM-ASTalkTalkCommunicationsLimitedGB | false |
| 126.117.92.254 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 37.20.211.92 | unknown | Russian Federation | | 12389 | ROSTELECOM-ASRU | false |
| 148.184.114.2 | unknown | United States | | 3423 | ATTIS-ASN3423US | false |
| 201.222.187.82 | unknown | Chile | | 7418 | TELEFONICACHILESACL | false |
| 223.37.56.169 | unknown | Korea Republic of | | 9644 | SKTELECOM-NET-ASSKTelecomKR | false |
| 209.58.18.6 | unknown | United States | | 6453 | AS6453US | false |
| 44.138.49.166 | unknown | United States | | 7377 | UCSDUS | false |
| 64.196.203.67 | unknown | United States | | 7029 | WINDSTREAMUS | false |
| 143.201.46.60 | unknown | unknown | | 3128 | BRUWS-AS3128US | false |
| 151.171.248.30 | unknown | United States | | 3257 | GTT-BACKBONEGTTDE | false |
| 76.168.35.52 | unknown | United States | | 20001 | TWC-20001-PACWESTUS | false |
| 19.255.230.120 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 65.56.241.202 | unknown | United States | | 3356 | LEVEL3US | 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): | 6.105130846651577 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | arm |
| File size: | 83264 |
| MD5: | c8eac6c41bd5f6ec5a65524142f340e0 |
| SHA1: | ae41cee628bdacfe7dd71dd1e4ab90e71a9d0a86 |
| SHA256: | b916d6f9d2756f35b510f1e89cf54a3601b3aafdba2a506cd9e5254e0dade88e |
| SHA512: | 4903b1f5a4a5e87704dbdd6caff2a496ca3de1fec833cfbdfdbf566f4f3ee2eef1eb8ab1e9347eee35bdcf623bd13a70d83e2aeb3611c2bc0dd8f722375235cd |
| SSDEEP: | 1536:0DS1KyEi7hinozX7mgbmvKbvlTuWrYn4XqbMyHFrzLv6aevo0YwbZnFA:YZi9zLmvvKuwYNoyHFTcKwbZnFA |
| File Content Preview: | .ELF...a.....(.....4....C.....4. ...(.....D=..D=.....@...@...@..p....&.....Q.td.....-...L."....G.....0@-.\P...0....S.0...P@...0... ....R.....0...0. .....0... ....R..... 0....S |

## 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: | 0x8190 |
| Flags: | 0x202 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 82864 |
| Section Header Size: | 40 |

## ELF header

| | |
|---|---|
| Number of Section Headers: | 10 |
| Header String Table Index: | 9 |

## Sections

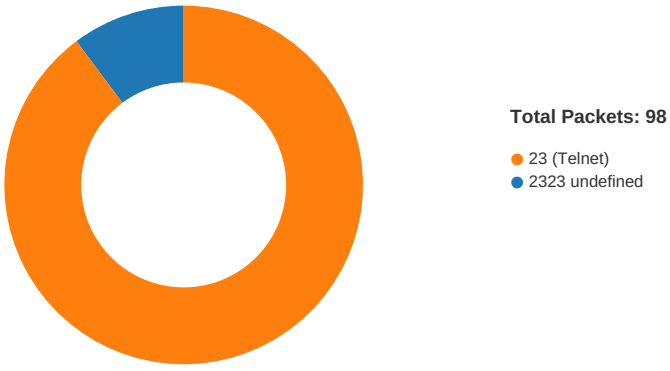
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x8094 | 0x94 | 0x18 | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .text | PROGBITS | 0x80b0 | 0xb0 | 0x11f3c | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .fini | PROGBITS | 0x19fec | 0x11fec | 0x14 | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .rodata | PROGBITS | 0x1a000 | 0x12000 | 0x1d44 | 0x0 | 0x2 | A | 0 | 0 | 4 |
| .ctors | PROGBITS | 0x24000 | 0x14000 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x24008 | 0x14008 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x24014 | 0x14014 | 0x35c | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .bss | NOBITS | 0x24370 | 0x14370 | 0x237c | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .shstrtab | STRTAB | 0x0 | 0x14370 | 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 | 0x8000 | 0x8000 | 0x13d44 | 0x13d44 | 3.4485 | 0x5 | R E | 0x8000 | | .init .text .fini .rodata |
| LOAD | 0x14000 | 0x24000 | 0x24000 | 0x370 | 0x26ec | 1.6757 | 0x6 | RW | 0x8000 | | .ctors .dtors .data .bss |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

# Network Behavior

## Network Port Distribution




## TCP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jan 21, 2022 06:01:11.452682972 CET | 192.168.2.23 | 8.8.8.8 | 0xd01c | Standard query (0) | arcticboatz.cz | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jan 21, 2022 06:01:11.471282959 CET | 8.8.8.8 | 192.168.2.23 | 0xd01c | No error (0) | arcticboatz.cz | | 95.181.161.40 | A (IP address) | IN (0x0001) |

## System Behavior

### Analysis Process: arm PID: **5201**, Parent PID: **5115**

#### General

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /tmp/arm |
| Arguments: | /tmp/arm |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

#### File Activities

##### File Read

### Analysis Process: arm PID: **5223**, Parent PID: **5201**

#### General

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### Analysis Process: sh PID: **5223**, Parent PID: **5201**

#### General

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd &&  mv /tmp/arm bin/systemd; chmod 777 bin/systemd" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

#### File Activities

##### File Read

### Analysis Process: sh PID: **5225**, Parent PID: **5223**

#### General

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### Analysis Process: rm PID: **5225**, Parent PID: **5223**

#### General

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /usr/bin/rm |
| Arguments: | rm -rf bin/systemd |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

**File Activities**

**File Deleted**

**File Read**

## Analysis Process: sh PID: **5226**, Parent PID: **5223**

**General**

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: mkdir PID: **5226**, Parent PID: **5223**

**General**

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /usr/bin/mkdir |
| Arguments: | mkdir bin |
| File size: | 88408 bytes |
| MD5 hash: | 088c9d1df5a28ed16c726eca15964cb7 |

**File Activities**

**File Read**

**Directory Created**

## Analysis Process: sh PID: **5227**, Parent PID: **5223**

**General**

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: mv PID: **5227**, Parent PID: **5223**

**General**

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /usr/bin/mv |
| Arguments: | mv /tmp/arm bin/systemd |
| File size: | 149888 bytes |
| MD5 hash: | 504f0590fa482d4da070a702260e3716 |

**File Activities**

**File Read**

**File Moved**

## Analysis Process: sh PID: **5228**, Parent PID: **5223**

**General**

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |

| | |
|---|---|
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: chmod PID: **5228**, Parent PID: **5223**

### General

| | |
|---|---|
| Start time: | 06:01:10 |
| Start date: | 21/01/2022 |
| Path: | /usr/bin/chmod |
| Arguments: | chmod 777 bin/systemd |
| File size: | 63864 bytes |
| MD5 hash: | 739483b900c045ae1374d6f53a86a279 |

### File Activities

**File Read**

**Permission Modified**

## Analysis Process: arm PID: **5229**, Parent PID: **5201**

### General

| | |
|---|---|
| Start time: | 06:01:11 |
| Start date: | 21/01/2022 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: arm PID: **5231**, Parent PID: **5229**

### General

| | |
|---|---|
| Start time: | 06:01:11 |
| Start date: | 21/01/2022 |
| Path: | /tmp/arm |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |