
**ID:** 544729
**Sample Name:** yH3AxCHT3I
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 01:47:05
**Date:** 24/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

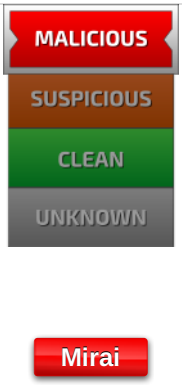
# Linux Analysis Report yH3AxCHT3I

## Overview

### General Information

| | |
|---|---|
| Sample Name: | yH3AxCHT3I |
| Analysis ID: | 544729 |
| MD5: | 9065d02c3a51d2.. |
| SHA1: | cdd354cd859054.. |
| SHA256: | 0054cf56d6a4ef6.. |
| Tags: | 32 arm elf mirai |
| Infos: | |

### Detection

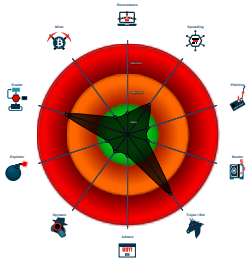



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Sample contains only a LOAD segm…
- Yara signature match
- 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 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: | 544729 |
| Start date: | 24.12.2021 |
| Start time: | 01:47:05 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 32s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | yH3AxCHT3I |
| 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: | mal84.troj.evad.lin@0/2@0/0 |
| Warnings: | Show All |

## Process Tree

- **system is lnxubuntu20**
- yH3AxCHT3I (PID: 5224, Parent: 5115, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/yH3AxCHT3I
  - yH3AxCHT3I New Fork (PID: 5227, Parent: 5224)
  - yH3AxCHT3I New Fork (PID: 5228, Parent: 5224)
  - yH3AxCHT3I New Fork (PID: 5229, Parent: 5224)
    - yH3AxCHT3I New Fork (PID: 5233, Parent: 5229)
    - yH3AxCHT3I New Fork (PID: 5234, Parent: 5229)
    - yH3AxCHT3I New Fork (PID: 5237, Parent: 5229)
- systemd New Fork (PID: 5261, Parent: 1)
- sshd (PID: 5261, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5262, Parent: 1)
- sshd (PID: 5262, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

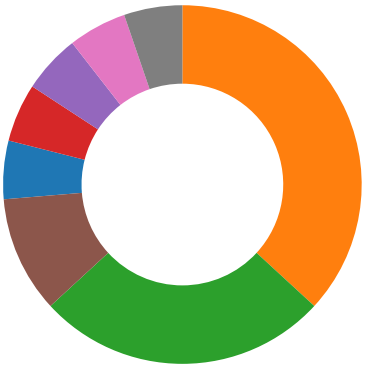
# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 5224.1.0000000007c53d73.000000006a7c51ae.rw-.sdmp | SUSP_XORed_Mozilla | Detects suspicious XORed keyword - Mozilla/5.0 | Florian Roth | • 0x1414:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1488:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x14fc:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1570:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x15e4:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1864:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x18bc:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1914:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x196c:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x19c4:$xo1: oMXKNNC\x0D\x17\x0C\x12 |
| 5233.1.00000000f26ed677.000000008ccd47ee.r-x.sdmp | SUSP_XORed_Mozilla | Detects suspicious XORed keyword - Mozilla/5.0 | Florian Roth | • 0x103cc:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1043c:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x104ac:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1051c:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1058c:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x107fc:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x10850:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x108a4:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x108f8:$xo1: oMXKNNC\x0D\x17\x0C\x12<br>• 0x1094c:$xo1: oMXKNNC\x0D\x17\x0C\x12 |
| 5233.1.00000000f26ed677.000000008ccd47ee.r-x.sdmp | Mirai_Botnet_Malware | Detects Mirai Botnet Malware | Florian Roth | • 0xfd84:$x1: POST /cdn-cgi/<br>• 0x1024c:$s1: LCOGQGPTGP |
| 5233.1.00000000f26ed677.000000008ccd47ee.r-x.sdmp | MAL_ELF_LNX_Mirai_Oct10_2 | Detects ELF malware Mirai related | Florian Roth | • 0xfd84:$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 |
| 5233.1.00000000f26ed677.000000008ccd47ee.r-x.sdmp | JoeSecurity_Mirai_5 | Yara detected Mirai | Joe Security | |

Click to see the 19 entries

# Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

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)**

## System Summary:

**Malicious sample detected (through community Yara rule)**

## Data Obfuscation:

**Sample is packed with UPX**

## Stealing of Sensitive Information:

**Yara detected Mirai**

## Remote Access Functionality:

**Yara detected Mirai**

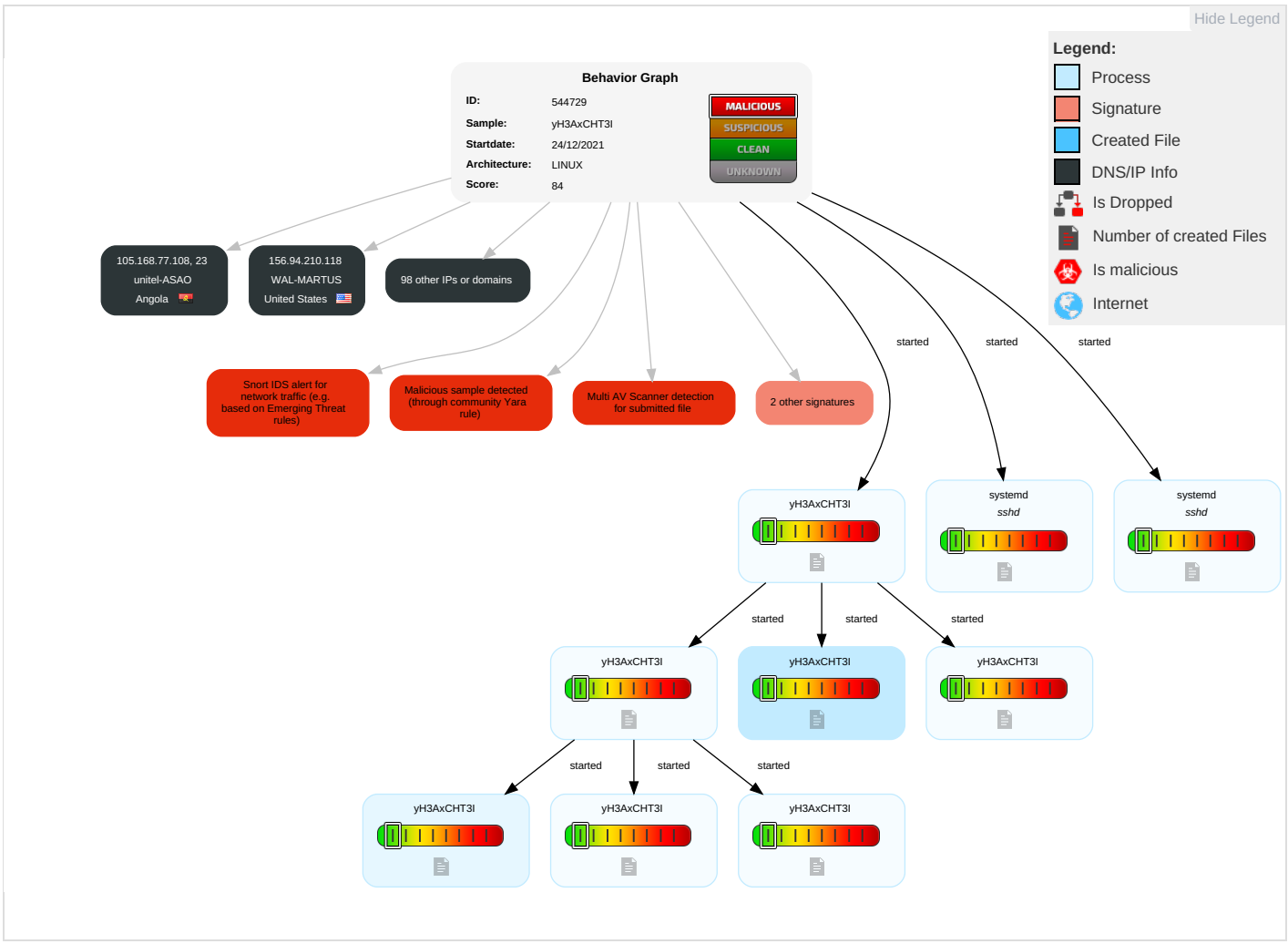
# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impa |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Path Interception | Obfuscated Files or Information 1 | OS Credential Dumping 1 | 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 | Mod Syst Parti |
| 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 | Devi Lock |
| 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 | Dele Devi Data |

# Malware Configuration

**No configs have been found**

# Behavior Graph




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| yH3AxCHT3I | 28% | Virustotal | | Browse |
| yH3AxCHT3I | 37% | 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

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 81.141.55.38 | unknown | United Kingdom | | 6871 | PLUSNETUKInternetServiceProviderGB | false |
| 163.53.56.189 | unknown | China | | 56005 | FASTIDCZhengzhouFastidcTechnologyCoLtdCN | false |
| 184.27.0.99 | unknown | United States | | 16625 | AKAMAI-ASUS | false |
| 41.140.93.155 | unknown | Morocco | | 36903 | MT-MPLSMA | false |
| 60.3.49.65 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 41.211.25.148 | unknown | Ghana | | 35091 | TELEDATA-ASTeledataGhanaIL | false |
| 37.14.40.204 | unknown | Spain | | 12479 | UNI2-ASES | false |
| 248.18.198.212 | unknown | Reserved | | unknown | unknown | false |
| 77.70.221.252 | unknown | Norway | | 5377 | MARLINK-EMEANO | false |
| 109.59.137.164 | unknown | Sweden | | 44034 | HI3GSE | false |
| 125.142.230.126 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 13.145.202.198 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 170.192.212.123 | unknown | United States | | 11685 | HNBCOL-ASUS | false |
| 166.29.182.20 | unknown | United States | | 206 | CSC-IGN-AMERUS | false |
| 66.224.112.73 | unknown | United States | | 7385 | ALLSTREAMUS | false |
| 9.40.103.0 | unknown | United States | | 3356 | LEVEL3US | false |
| 106.72.195.169 | unknown | Japan | | 2516 | KDDIKDDICORPORATIONJP | false |
| 44.40.175.57 | unknown | United States | | 20473 | AS-CHOOPAUS | false |
| 123.87.18.133 | unknown | China | | 9394 | CTTNETChinaTieTongTelecommunicationsCorporationCN | false |
| 40.197.171.2 | unknown | United States | | 4249 | LILLY-ASUS | false |
| 114.5.205.188 | unknown | Indonesia | | 4761 | INDOSAT-INP-APINDOSATInternetNetworkProviderID | false |
| 211.163.111.102 | unknown | China | | 4847 | CNIX-APChinaNetworksInter-ExchangeCN | false |
| 45.75.160.232 | unknown | United Kingdom | | 49425 | DIGITAL-REALTY-UKGB | false |
| 200.199.40.172 | unknown | Brazil | | 7738 | TelemarNorteLesteSABR | false |
| 58.237.168.215 | unknown | Korea Republic of | | 9318 | SKB-ASSKBroadbandCoLtdKR | false |
| 123.108.189.204 | unknown | Korea Republic of | | 10175 | HCNKUMHO-AS-KRKumhoCableKR | false |
| 155.250.111.153 | unknown | Germany | | 13167 | MERCK-KGAADarmstadtGermanyDE | false |
| 34.109.90.207 | unknown | United States | | 15169 | GOOGLEUS | false |
| 178.81.128.60 | unknown | Saudi Arabia | | 35819 | MOBILY-ASEtihadEtisalatCompanyMobilySA | false |
| 209.122.96.77 | unknown | United States | | 6079 | RCN-ASUS | false |
| 5.24.137.60 | unknown | Turkey | | 16135 | TURKCELL-ASTurkcellASTR | false |
| 63.148.160.65 | unknown | United States | | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 249.223.115.142 | unknown | Reserved | | unknown | unknown | false |
| 68.201.64.64 | unknown | United States | | 11427 | TWC-11427-TEXASUS | false |
| 58.199.186.139 | unknown | China | | 4538 | ERX-CERNET-BKBChinaEducationandResearchNetworkCenter | false |
| 200.152.150.49 | unknown | Brazil | | 28590 | DirectnetPrestacaodeServicosLtdaBR | false |
| 207.144.199.204 | unknown | United States | | 22646 | HARCOM1US | false |
| 118.170.22.249 | unknown | Taiwan; Republic of China (ROC) | | 3462 | HINETDataCommunicationBusinessGroupTW | false |
| 115.52.204.84 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOMChina169BackboneCN | false |
| 79.141.10.235 | unknown | France | | 25540 | ALPHALINK-ASFR | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 114.60.198.77 | unknown | China | | 9812 | CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN | false |
| 177.145.138.208 | unknown | Brazil | | 26599 | TELEFONICABRASILSABR | false |
| 32.185.230.113 | unknown | United States | | 20057 | ATT-MOBILITY-LLC-AS20057US | false |
| 113.55.196.3 | unknown | China | | 4538 | ERX-CERNET-BKBChinaEducationandResearchNetworkCenter | false |
| 18.140.158.93 | unknown | United States | | 16509 | AMAZON-02US | false |
| 68.42.99.162 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 189.174.41.83 | unknown | Mexico | | 8151 | UninetSAdeCVMX | false |
| 9.11.181.108 | unknown | United States | | 3356 | LEVEL3US | false |
| 220.221.242.63 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 79.57.118.183 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 72.52.137.100 | unknown | United States | | 32244 | LIQUIDWEBUS | false |
| 100.248.229.26 | unknown | United States | | 21928 | T-MOBILE-AS21928US | false |
| 31.102.195.59 | unknown | United Kingdom | | 12576 | EELtdGB | false |
| 173.223.114.161 | unknown | United States | | 16625 | AKAMAI-ASUS | false |
| 35.122.244.156 | unknown | United States | | 237 | MERIT-AS-14US | false |
| 193.13.86.3 | unknown | Sweden | | 1257 | TELE2EU | false |
| 177.165.238.214 | unknown | Brazil | | 26615 | TIMSABR | false |
| 101.162.4.142 | unknown | Australia | | 1221 | ASN-TELSTRATelstraCorporationLtdAU | false |
| 121.188.110.123 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 75.75.74.187 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 5.130.84.210 | unknown | Russian Federation | | 31200 | NTKIPv6customersRU | false |
| 255.210.145.196 | unknown | Reserved | | unknown | unknown | false |
| 184.101.8.131 | unknown | United States | | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 37.79.117.209 | unknown | Russian Federation | | 12389 | ROSTELECOM-ASRU | false |
| 68.109.108.216 | unknown | United States | | 22773 | ASN-CXA-ALL-CCI-22773-RDCUS | false |
| 75.127.194.9 | unknown | United States | | 6128 | CABLE-NET-1US | false |
| 99.34.80.250 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 200.122.108.186 | unknown | Argentina | | 10481 | TelecomArgentinaSAAR | false |
| 165.243.24.41 | unknown | Korea Republic of | | 4668 | LGNET-AS-KRLGCNSKR | false |
| 105.168.77.108 | unknown | Angola | | 37119 | unitel-ASAO | false |
| 171.248.31.10 | unknown | Viet Nam | | 7552 | VIETEL-AS-APViettelGroupVN | false |
| 94.239.156.8 | unknown | France | | 5410 | BOUYGTEL-ISPFR | false |
| 92.186.173.40 | unknown | France | | 12479 | UNI2-ASES | false |
| 242.94.217.63 | unknown | Reserved | | unknown | unknown | false |
| 83.7.185.173 | unknown | Poland | | 5617 | TPNETPL | false |
| 20.161.36.36 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 88.53.30.66 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 105.154.88.139 | unknown | Morocco | | 36903 | MT-MPLSMA | false |
| 189.76.171.77 | unknown | Brazil | | 28358 | INTERTELCOTELECOMUNICACOESMULTIMIDIALTDABR | false |
| 100.128.95.133 | unknown | United States | | 21928 | T-MOBILE-AS21928US | false |
| 218.239.129.52 | unknown | Korea Republic of | | 9318 | SKB-ASSKBroadbandCoLtdKR | false |
| 83.211.190.35 | unknown | Italy | | 15589 | ASN-CLOUDITALIAIT | false |
| 38.237.254.194 | unknown | United States | | 174 | COGENT-174US | false |
| 66.251.214.57 | unknown | United States | | 18624 | CITYOFWILSONNCUS | false |
| 39.198.18.103 | unknown | Indonesia | | 23693 | TELKOMSEL-ASN-IDPTTelekomunikasiSelularID | false |
| 197.109.134.51 | unknown | South Africa | | 37168 | CELL-CZA | false |
| 117.63.65.234 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 82.1.18.205 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 173.79.81.100 | unknown | United States | | 701 | UUNETUS | false |
| 201.180.141.26 | unknown | Argentina | | 22927 | TelefonicadeArgentinaAR | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 156.94.210.118 | unknown | United States | | 10695 | WAL-MARTUS | false |
| 94.82.238.146 | unknown | Italy | | 3269 | ASN-IBSNAZIT | false |
| 17.139.38.27 | unknown | United States | | 714 | APPLE-ENGINEERINGUS | false |
| 141.237.226.38 | unknown | Greece | | 3329 | HOL-GRAthensGreeceGR | false |
| 154.47.211.221 | unknown | United States | | 174 | COGENT-174US | false |
| 159.245.168.149 | unknown | European Union | | 29899 | GEISINGERUS | false |
| 101.211.73.148 | unknown | India | | 58519 | CHINATELECOM-CTCLOUDCloudComputingCorporationCN | false |
| 40.94.195.122 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 113.157.0.65 | unknown | Japan | | 2516 | KDDIKDDICORPORATIONJP | false |
| 188.151.72.64 | unknown | Norway | | 39651 | COMHEM-SWEDENSE | false |

### Runtime Messages

| | |
|---|---|
| Command: | /tmp/yH3AxCHT3I |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | lzrd cock fest'/proc/'/exe |
| Standard Error: | |

## Joe Sandbox View / Context

### IPs

**No context**

### Domains

**No context**

### ASN

**No context**

### JA3 Fingerprints

**No context**

### Dropped Files

**No context**

## Created / dropped Files

| /proc/5262/oom_score_adj | |
|---|---|
| Process: | /usr/sbin/sshd |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 6 |
| Entropy (8bit): | 1.7924812503605778 |
| Encrypted: | false |
| SSDEEP: | 3:ptn:Dn |
| MD5: | CBF282CC55ED0792C33D10003D1F760A |

| /proc/5262/oom_score_adj | |
|---|---|
| SHA1: | 007DD8BD75468E6B7ABA4285E9B267202C7EAEED |
| SHA-256: | FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22 |
| SHA-512: | 4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | -1000. |

| /run/sshd.pid | |
|---|---|
| Process: | /usr/sbin/sshd |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 1.9219280948873623 |
| Encrypted: | false |
| SSDEEP: | 3:CL:CL |
| MD5: | E106DF5C7ADCDDF2A3C9B1E5C78112A2 |
| SHA1: | 53E55A4072F9624175A43F956606B439CBE28772 |
| SHA-256: | 66A2BED186C11E9F5C0CBF32D971D14325F871E209C68211608711757 22A43D0 |
| SHA-512: | B9EA0BC991203AD49366990596FDF035447600B1155BAD741F7C797C20C0D4E30D06F0E06AE59C4B01FD115F9E5E6B345A155BE01112D384FCF72D7B153F2EA |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 5262. |

# Static File Info

## General

| | |
|---|---|
| File type: | ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped |
| Entropy (8bit): | 7.9512483718866385 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | yH3AxCHT3I |
| File size: | 29944 |
| MD5: | 9065d02c3a51d27d6a930d838fa9d700 |
| SHA1: | cdd354cd859054955116cc0476884ed3b77b4c93 |
| SHA256: | 0054cf56d6a4ef6e38ccaaf189be5f9a2e94781c8234ed52bec896fbc525d511 |
| SHA512: | bd03ea2796cef23906b5675454344b78cfc297cc10cc4648ae65391e72ff5d2766e3c480056aea1be81328d416f27295a14bc0e9eb2ca9a72055381a73778f8a |
| SSDEEP: | 384:++pBNm5t8706u9jtiyM0hYQEmIyzc/bgDB290RUWFZd/f25K2j0U+7+ThymdGUoo:BA4uBc0THcq21qZdhfU+7Is3UozE |
| File Content Preview: | .ELF...a.....(.....X...4.....4. ...(.....t...t.....L...L...L.....Q.td.....s.y.UPX!.....D...D.....R.....?.E.h;.}...^.....f*..J.%.",.....n7..Io.Z....'.....5.1...#....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: | 0xe258 |
| Flags: | 0x202 |
| ELF Header Size: | 52 |

### ELF header

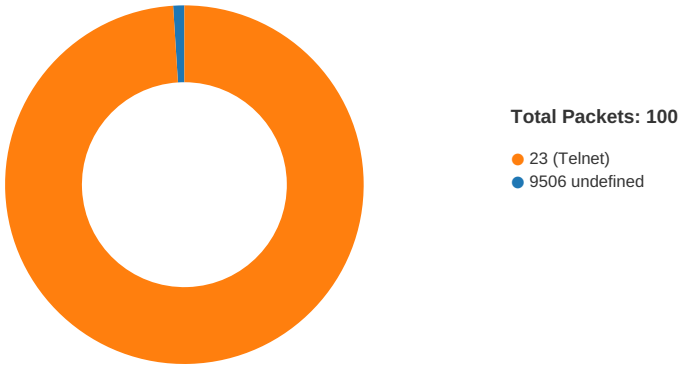
| | |
|---|---|
| Program Header Offset: | 52 |
| Program Header Size: | 32 |
| Number of Program Headers: | 3 |
| Section Header Offset: | 0 |
| Section Header Size: | 40 |
| Number of Section Headers: | 0 |
| Header String Table Index: | 0 |

### 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 | 0x7407 | 0x7407 | 3.9980 | 0x5 | R E | 0x8000 | | |
| LOAD | 0x164c | 0x2164c | 0x2164c | 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: yH3AxCHT3I PID: 5224 Parent PID: 5115

### General

| | |
|---|---|
| Start time: | 01:47:47 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | /tmp/yH3AxCHT3I |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

#### File Read

## Analysis Process: yH3AxCHT3I PID: 5227 Parent PID: 5224

### General

| | |
|---|---|
| Start time: | 01:47:48 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: yH3AxCHT3I PID: 5228 Parent PID: 5224

### General

| | |
|---|---|
| Start time: | 01:47:48 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: yH3AxCHT3I PID: 5229 Parent PID: 5224

### General

| | |
|---|---|
| Start time: | 01:47:48 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: yH3AxCHT3I PID: 5233 Parent PID: 5229

### General

| | |
|---|---|
| Start time: | 01:47:48 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: yH3AxCHT3I PID: 5234 Parent PID: 5229

### General

| | |
|---|---|
| Start time: | 01:47:48 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: yH3AxCHT3I PID: 5237 Parent PID: 5229

### General

| | |
|---|---|
| Start time: | 01:47:48 |
| Start date: | 24/12/2021 |
| Path: | /tmp/yH3AxCHT3I |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: systemd PID: 5261 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 01:47:57 |
| Start date: | 24/12/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: sshd PID: 5261 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 01:47:57 |
| Start date: | 24/12/2021 |
| Path: | /usr/sbin/sshd |
| Arguments: | /usr/sbin/sshd -t |
| File size: | 876328 bytes |
| MD5 hash: | dbca7a6bbf7bf57fedac243d4b2cb340 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: systemd PID: 5262 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 01:47:57 |
| Start date: | 24/12/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: sshd PID: 5262 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 01:47:57 |
| Start date: | 24/12/2021 |
| Path: | /usr/sbin/sshd |
| Arguments: | /usr/sbin/sshd -D |
| File size: | 876328 bytes |
| MD5 hash: | dbca7a6bbf7bf57fedac243d4b2cb340 |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated