


**ID:** 626477
**Sample Name:** tU468ylYjx
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 04:25:24
**Date:** 14/05/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents


Table of Contents 2
Linux Analysis Report tU468ylYjx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Warnings 4
Runtime Messages 4
Process Tree 5
Yara Signatures 5
PCAP (Network Traffic) 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Data Obfuscation 5
Hooking and other Techniques for Hiding and Protection 5
Stealing of Sensitive Information 5
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Malware Configuration 6
Behavior Graph 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Domains 7
URLs 7
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 8
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
Static ELF Info 11
ELF header 11
Program Segments 11
Network Behavior 12
Network Port Distribution 12
TCP Packets 12
System Behavior 12
Analysis Process: tU468ylYjx PID: 6224, Parent PID: 6123 12
General 12
File Activities 12
File Read 12
Analysis Process: tU468ylYjx PID: 6226, Parent PID: 6224 12
General 12
File Activities 12
File Read 12
Directory Enumerated 13
Analysis Process: tU468ylYjx PID: 6323, Parent PID: 6226 13
General 13
Analysis Process: tU468ylYjx PID: 6324, Parent PID: 6226 13
General 13
Analysis Process: tU468ylYjx PID: 6327, Parent PID: 6324 13
General 13
Analysis Process: tU468ylYjx PID: 6340, Parent PID: 6327 13
General 13
Analysis Process: tU468ylYjx PID: 6341, Parent PID: 6327 13
General 13
Analysis Process: tU468ylYjx PID: 6328, Parent PID: 6324 13
General 13
Analysis Process: tU468ylYjx PID: 6330, Parent PID: 6324 14
General 14
Analysis Process: tU468ylYjx PID: 6227, Parent PID: 6224 14
General 14


Copyright Joe Security LLC 2022

Analysis Process: tU468ylYjx PID: 6228, Parent PID: 6224 14
General 14
Analysis Process: tU468ylYjx PID: 6232, Parent PID: 6228 14
General 14
File Activities 14
File Read 14
Directory Enumerated 14
Analysis Process: tU468ylYjx PID: 6333, Parent PID: 6232 14
General 14
Analysis Process: tU468ylYjx PID: 6334, Parent PID: 6232 14
General 14
Analysis Process: tU468ylYjx PID: 6233, Parent PID: 6228 15
General 15
Analysis Process: tU468ylYjx PID: 6235, Parent PID: 6228 15
General 15

Copyright Joe Security LLC 2022

# Linux Analysis Report

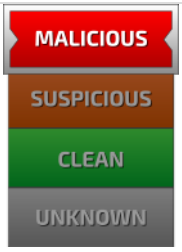
## tU468ylYjx

## Overview

### General Information

| | |
|---|---|
| Sample Name: | tU468ylYjx |
| Analysis ID: | 626477 |
| MD5: | 1f435b2e68e159.. |
| SHA1: | 8c76b05125e6bf.. |
| SHA256: | 2a918615507819. |
| Tags: | 32 elf mirai powerpc |
| Infos: | |

### Detection



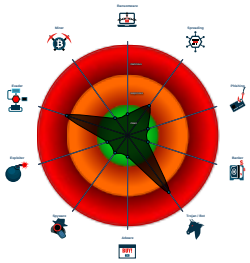

Mirai

| | |
|---|---|
| Score: | 64 |
| 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 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
- Sample tries to kill a process (SIGK…

### 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.**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 626477 |
| Start date and time: 14/05/202204:25:24 | 2022-05-14 04:25:24 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 50s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | tU468ylYjx |
| 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.evad.lin@0/0@0/0 |

## Warnings

## Runtime Messages

| | |
|---|---|
| Command: | /tmp/tU468ylYjx |
| PID: | 6224 |
| Exit Code: | 0 |
| Exit Code Info: | |
| Killed: | False |
| Standard Output: | Connected To CNC |
| Standard Error: | |

Copyright Joe Security LLC 2022

## Process Tree

- **system is lnxubuntu20**
- tU468ylYjx (PID: 6224, Parent: 6123, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/tU468ylYjx
  - tU468ylYjx New Fork (PID: 6226, Parent: 6224)
    - tU468ylYjx New Fork (PID: 6323, Parent: 6226)
    - tU468ylYjx New Fork (PID: 6324, Parent: 6226)
      - tU468ylYjx New Fork (PID: 6327, Parent: 6324)
        - tU468ylYjx New Fork (PID: 6340, Parent: 6327)
        - tU468ylYjx New Fork (PID: 6341, Parent: 6327)
      - tU468ylYjx New Fork (PID: 6328, Parent: 6324)
      - tU468ylYjx New Fork (PID: 6330, Parent: 6324)
  - tU468ylYjx New Fork (PID: 6227, Parent: 6224)
  - tU468ylYjx New Fork (PID: 6228, Parent: 6224)
    - tU468ylYjx New Fork (PID: 6232, Parent: 6228)
      - tU468ylYjx New Fork (PID: 6333, Parent: 6232)
      - tU468ylYjx New Fork (PID: 6334, Parent: 6232)
    - tU468ylYjx New Fork (PID: 6233, Parent: 6228)
    - tU468ylYjx New Fork (PID: 6235, Parent: 6228)
- **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

### 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

Copyright Joe Security LLC 2022

Yara detected Mirai

## Mitre Att&ck Matrix

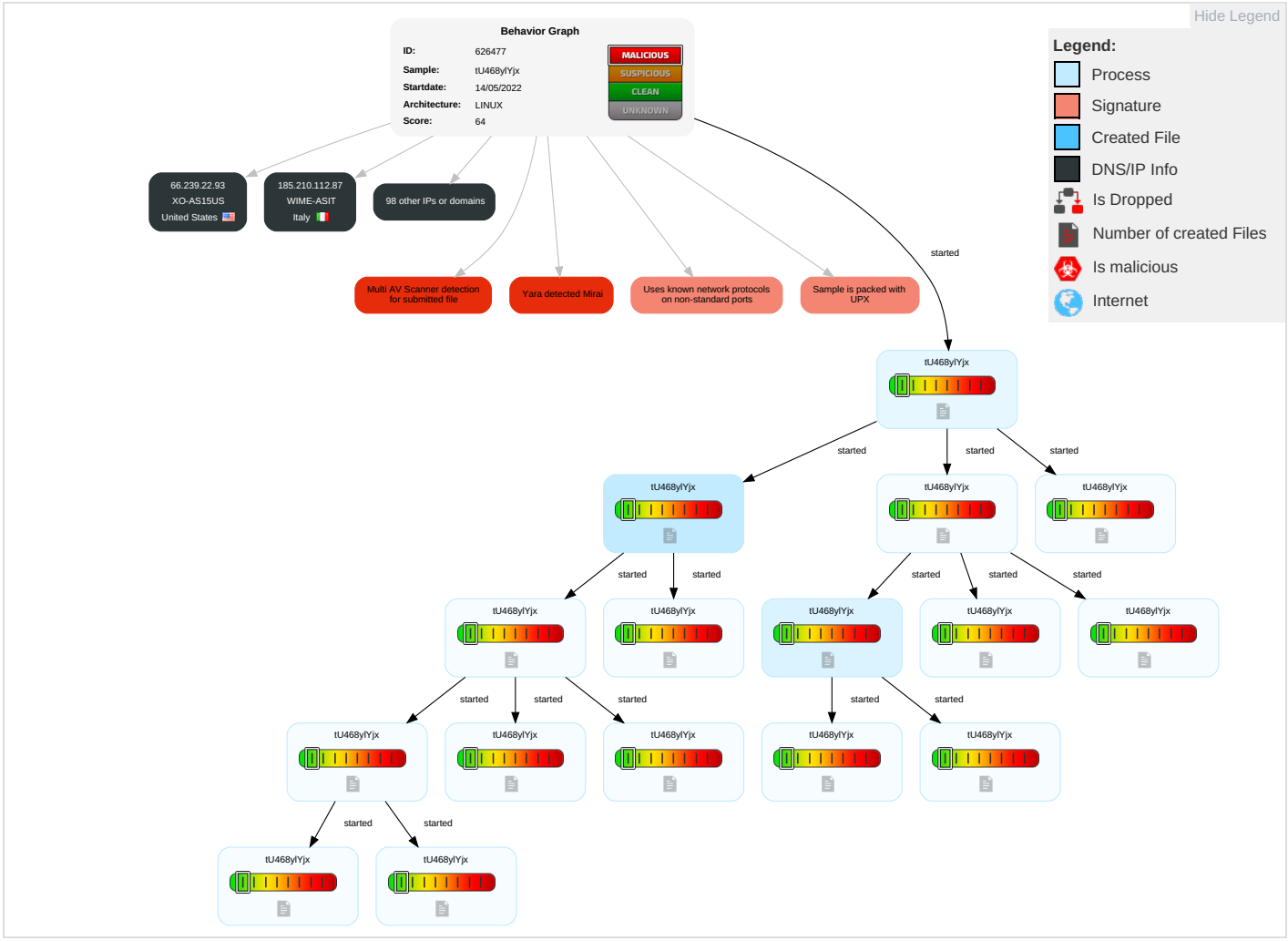
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid 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 | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 1 Non-Standard Port | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 1 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |

## Malware Configuration

No configs have been found

## Behavior Graph

Copyright Joe Security LLC 2022




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| tU468ylYjx | 39% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

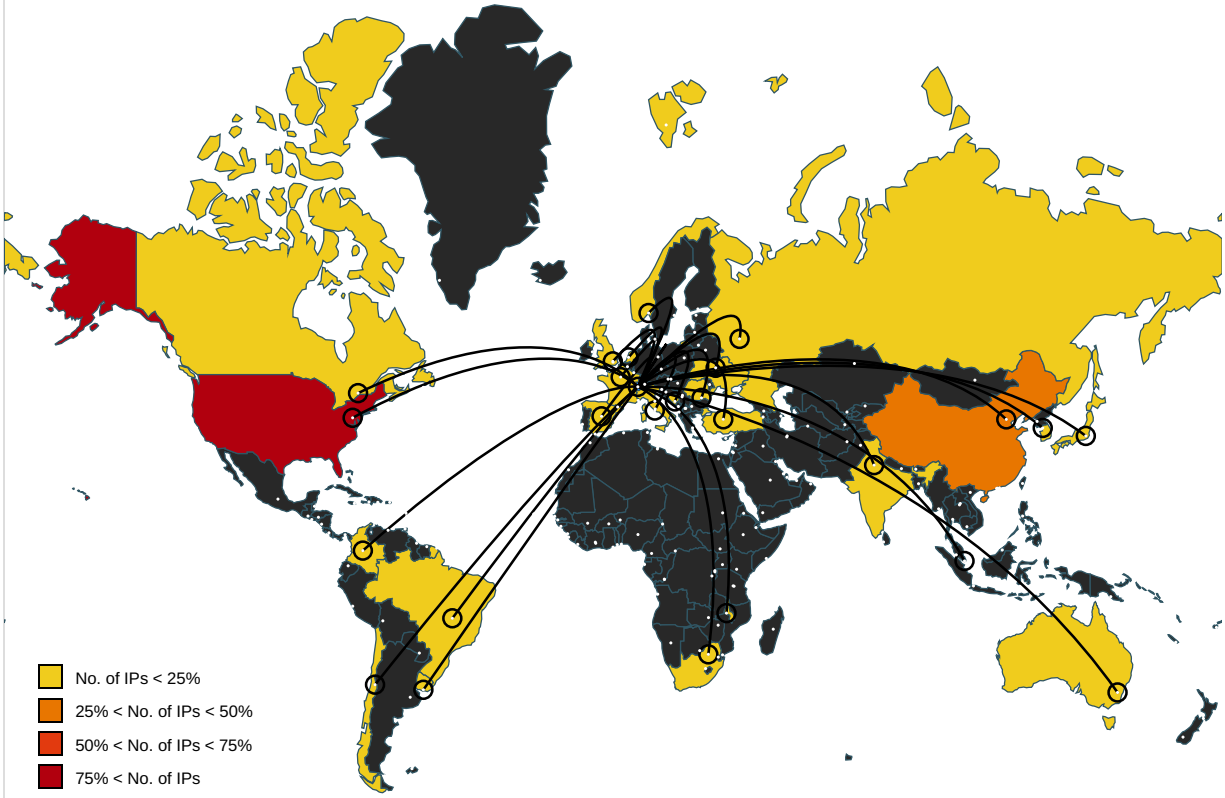
## Domains and IPs

### 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 |
|---|---|---|---|---|---|---|
| 124.75.165.150 | unknown | China | | 4812 | CHINANET-SH-APChinaTelecomGroupCN | false |
| 216.92.92.101 | unknown | United States | | 7859 | PAIR-NETWORKSUS | false |
| 150.217.3.109 | unknown | Italy | | 137 | ASGARRConsortiumGARREU | false |
| 244.158.124.82 | unknown | Reserved | | unknown | unknown | false |
| 170.248.7.61 | unknown | United States | | 21433 | ACCENTUREFSSCLondonDCGB | false |
| 71.99.94.185 | unknown | United States | | 5650 | FRONTIER-FRTRUS | false |
| 208.165.164.65 | unknown | United States | | 3561 | CENTURYLINK-LEGACY-SAVVISUS | false |
| 220.210.235.162 | unknown | Japan | | 18144 | AS-ENECOMEnergiaCommunicationsIncJP | false |
| 125.76.82.63 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 83.207.100.101 | unknown | France | | 3215 | FranceTelecom-OrangeFR | false |
| 174.140.145.193 | unknown | United States | | 29748 | QTS-ASHUS | false |
| 248.171.46.242 | unknown | Reserved | | unknown | unknown | false |
| 35.255.218.17 | unknown | United States | | 3549 | LVLT-3549US | false |
| 78.110.158.83 | unknown | Russian Federation | | 43530 | IRTELCOM-ASRU | false |
| 13.133.28.227 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 178.198.88.170 | unknown | Switzerland | | 3303 | SWISSCOMSwisscomSwitzerlandLtdCH | false |
| 148.128.197.77 | unknown | United States | | 2386 | INS-ASUS | false |
| 75.136.133.5 | unknown | United States | | 20115 | CHARTER-20115US | false |
| 146.213.125.26 | unknown | Norway | | 5619 | EVRY-NO | false |
| 66.239.22.93 | unknown | United States | | 2828 | XO-AS15US | false |
| 197.90.74.64 | unknown | South Africa | | 10474 | OPTINETZA | false |
| 123.91.75.157 | unknown | China | | 9394 | CTTNETChinaTieTongTelecommunicationsCorporationCN | false |

Copyright Joe Security LLC 2022

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 87.125.105.248 | unknown | Spain | | 12430 | VODAFONE_ESES | false |
| 166.121.243.157 | unknown | Singapore | | 9911 | CONNECTPLUS-APSingaporeTelecomSG | false |
| 101.87.127.209 | unknown | China | | 4812 | CHINANET-SH-APChinaTelecomGroupCN | false |
| 12.155.33.184 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 184.103.198.217 | unknown | United States | | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 88.145.164.184 | unknown | United Kingdom | | 12708 | ONETEL-ASTalkTalkCommunicationsLimitedGB | false |
| 141.112.190.217 | unknown | United States | | 6 | BULL-HNUS | false |
| 60.124.156.62 | unknown | Japan | | 17676 | GIGAINFRASoftbankBBCorpJP | false |
| 198.93.34.243 | unknown | United States | | 6352 | ETRADE-ASUS | false |
| 241.4.244.146 | unknown | Reserved | | unknown | unknown | false |
| 73.112.121.58 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 86.120.245.134 | unknown | Romania | | 8708 | RCS-RDS73-75DrStaicoviciRO | false |
| 93.151.65.201 | unknown | Italy | | 44957 | OPITELIT | false |
| 114.170.121.58 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 178.209.254.131 | unknown | Russian Federation | | 12714 | TI-ASMoscowRussiaRU | false |
| 66.206.239.222 | unknown | Canada | | 23184 | PERSONACA | false |
| 190.146.201.91 | unknown | Colombia | | 10620 | TelmexColombiaSACO | false |
| 93.127.41.180 | unknown | Ukraine | | 6703 | ALKAR-ASUA | false |
| 206.162.114.249 | unknown | United States | | 1239 | SPRINTLINKUS | false |
| 151.83.84.10 | unknown | Italy | | 1267 | ASN-WINDTREIUNETEU | false |
| 48.192.124.95 | unknown | United States | | 2686 | ATGS-MMD-ASUS | false |
| 9.99.10.27 | unknown | United States | | 3356 | LEVEL3US | false |
| 255.64.112.201 | unknown | Reserved | | unknown | unknown | false |
| 36.175.243.139 | unknown | China | | 9808 | CMNET-GDGuangdongMobileCommunicationCoLtdCN | false |
| 185.210.112.87 | unknown | Italy | | 207029 | WIME-ASIT | false |
| 178.245.236.25 | unknown | Turkey | | 16135 | TURKCELL-ASTurkcellASTR | false |
| 16.84.55.94 | unknown | United States | | unknown | unknown | false |
| 140.228.246.149 | unknown | United States | | 600 | OARNET-ASUS | false |
| 242.5.233.28 | unknown | Reserved | | unknown | unknown | false |
| 186.105.116.215 | unknown | Chile | | 7418 | TELEFONICACHILESACL | false |
| 73.172.210.228 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 188.163.100.152 | unknown | Ukraine | | 15895 | KSNET-ASUA | false |
| 241.120.255.24 | unknown | Reserved | | unknown | unknown | false |
| 133.38.251.68 | unknown | Japan | | 2907 | SINET-ASResearchOrganizationofInformationandSystemsN | false |
| 197.211.114.67 | unknown | Malawi | | 37187 | SKYBANDMW | false |
| 208.137.162.169 | unknown | United States | | 3561 | CENTURYLINK-LEGACY-SAVVISUS | false |
| 92.207.185.241 | unknown | United Kingdom | | 31655 | ASN-GAMMATELECOMGB | false |
| 135.133.91.192 | unknown | United States | | 14962 | NCR-252US | false |
| 109.191.69.227 | unknown | Russian Federation | | 8369 | INTERSVYAZ-AS38-BKomsomolskyprospektRU | false |
| 194.158.255.197 | unknown | Switzerland | | 6730 | SUNRISECH | false |
| 99.70.226.9 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 112.216.243.179 | unknown | Korea Republic of | | 3786 | LGDACOMLGDACOMCorporationKR | false |
| 78.208.95.165 | unknown | France | | 12322 | PROXADFR | false |
| 95.98.201.16 | unknown | Netherlands | | 31615 | TMO-NL-ASNL | false |
| 204.99.97.160 | unknown | United States | | 18862 | NCS-HEALTHCAREUS | false |
| 251.181.98.112 | unknown | Reserved | | unknown | unknown | false |
| 18.104.56.4 | unknown | United States | | 3 | MIT-GATEWAYSUS | false |
| 209.174.40.205 | unknown | United States | | 6325 | ILLINOIS-CENTURYUS | false |

Copyright Joe Security LLC 2022

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 249.121.54.201 | unknown | Reserved | | unknown | unknown | false |
| 204.127.184.185 | unknown | United States | | 4466 | EASYLINK2US | false |
| 243.74.170.105 | unknown | Reserved | | unknown | unknown | false |
| 42.84.186.120 | unknown | China | | 9929 | CUIICHINAUNICOMIndustrialInternetBackboneCN | false |
| 159.56.40.145 | unknown | United States | | 11351 | TWC-11351-NORTHEASTUS | false |
| 122.226.30.57 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 101.190.18.150 | unknown | Australia | | 1221 | ASN-TELSTRATelstraCorporationLtdAU | false |
| 191.131.223.31 | unknown | Brazil | | 26615 | TIMSABR | false |
| 202.233.148.100 | unknown | Japan | | 4675 | U-NETSURFUNIADEXLTDJP | false |
| 190.134.2.247 | unknown | Uruguay | | 6057 | AdministracionNacionaldeTelecomunicacionesUY | false |
| 251.37.69.2 | unknown | Reserved | | unknown | unknown | false |
| 249.120.39.186 | unknown | Reserved | | unknown | unknown | false |
| 8.156.208.151 | unknown | Singapore | | 37963 | CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd | false |
| 107.60.65.39 | unknown | United States | | 16567 | NETRIX-16567US | false |
| 177.92.168.108 | unknown | Brazil | | 263107 | QwertyComunicacoeseTecnologiaEducacionalLtdaBR | false |
| 210.42.148.53 | unknown | China | | 24358 | CNGI-WH-IX-AS-APCERNET2IXatHuazhongUniversityofScienc | false |
| 172.185.37.93 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 32.68.194.104 | unknown | United States | | 2686 | ATGS-MMD-ASUS | false |
| 247.57.2.218 | unknown | Reserved | | unknown | unknown | false |
| 92.203.241.85 | unknown | Japan | | 2527 | SO-NETSo-netEntertainmentCorporationJP | false |
| 169.172.184.107 | unknown | United States | | 37611 | AfrihostZA | false |
| 124.7.224.3 | unknown | India | | 9583 | SIFY-AS-INSifyLimitedIN | false |
| 213.81.126.107 | unknown | United Kingdom | | 5089 | NTLGB | false |
| 161.93.54.189 | unknown | Japan | | 14298 | EPA-NETUS | false |
| 114.183.221.41 | unknown | Japan | | 4713 | OCNNTTCommunicationsCorporationJP | false |
| 218.0.41.111 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 12.216.23.176 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 86.129.125.230 | unknown | United Kingdom | | 2856 | BT-UK-ASBTnetUKRegionalnetworkGB | false |
| 40.48.200.190 | unknown | United States | | 4249 | LILLY-ASUS | false |
| 93.180.151.102 | unknown | Bosnia and Herzegowina | | 198252 | ELTAKABEL-ASDobojskihbrigadaBBBA | 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 MSB executable, PowerPC or cisco 4500, version 1 (GNU/Linux), statically linked, stripped |
| Entropy (8bit): | 7.91879712795437 |
| TrID: | • ELF Executable and Linkable format (Linux) (4029/14) 50.16%<br>• ELF Executable and Linkable format (generic) (4004/1) 49.84% |
| File name: | tU468ylYjx |
| File size: | 23936 |
| MD5: | 1f435b2e68e159ee636a17bf3552d7de |
| SHA1: | 8c76b05125e6bf6c32f72934181d52fd07ba9ad9 |
| SHA256: | 2a918615507819ee0c0c1c1ced7afd8ab35e44488b78340273c39e5fd60c77a3 |
| SHA512: | 611bfdea682cf72cdf07b7efd7827367adec1263bc1b81fe9205b7fb42048e26fb8fbbf5a4a472ef0988ec49d0799abcd7882c22f3794164402ccc87c5e1f18c |
| SSDEEP: | 384:2OA0AeimAzNCdvw1PwlWWtKfz9VuBFoeIoA8FXw2t7tTmojIo8wNM4uVcqgw05VC:2AApCdvwJr69VJoA8FZtxCo8MC4uVcqF |
| TLSH: | 22B2D01AC0AE3E74FE9B7D355941E2817B619BDF7A62CDC017C15B120622D2C1F9CAD8 |
| File Content Preview: | .ELF.....J....4.....4. ...<br>(.....\...\.....dt.Q.....UPX!.....S.....?.E.h4...@b.....D*aN.....]&a.r...K{.LS....9.5o..V |

### Static ELF Info

#### ELF header

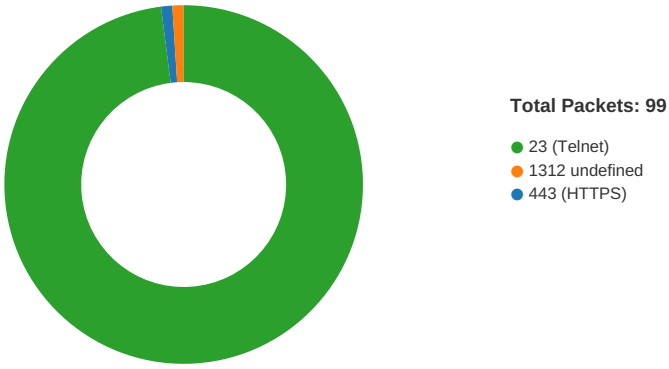
| | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, big endian |
| Version: | 1 (current) |
| Machine: | PowerPC |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | UNIX - Linux |
| ABI Version: | 0 |
| Entry Point Address: | 0x104aa0 |
| Flags: | 0x0 |
| ELF Header Size: | 52 |
| 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 | 0x100000 | 0x100000 | 0x5c88 | 0x5c88 | 4.2067 | 0x5 | R E | 0x10000 | | |
| LOAD | 0xc9e8 | 0x1001c9e8 | 0x1001c9e8 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x10000 | | |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x4 | | |

## Network Behavior

### Network Port Distribution




### TCP Packets

## System Behavior

### Analysis Process: tU468ylYjx PID: 6224, Parent PID: 6123

#### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | /tmp/tU468ylYjx |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

#### File Activities

##### File Read

### Analysis Process: tU468ylYjx PID: 6226, Parent PID: 6224

#### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

#### File Activities

##### File Read

Copyright Joe Security LLC 2022

## Directory Enumerated

### Analysis Process: tU468ylYjx PID: 6323, Parent PID: 6226

#### General

| | |
|---|---|
| Start time: | 04:28:59 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: 6324, Parent PID: 6226

#### General

| | |
|---|---|
| Start time: | 04:28:59 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: 6327, Parent PID: 6324

#### General

| | |
|---|---|
| Start time: | 04:28:59 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: 6340, Parent PID: 6327

#### General

| | |
|---|---|
| Start time: | 04:29:04 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: 6341, Parent PID: 6327

#### General

| | |
|---|---|
| Start time: | 04:29:04 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: 6328, Parent PID: 6324

#### General

| | |
|---|---|
| Start time: | 04:28:59 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |

Copyright Joe Security LLC 2022

| | |
|---|---|
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: **6330**, Parent PID: **6324**

#### General

| | |
|---|---|
| Start time: | 04:28:59 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: **6227**, Parent PID: **6224**

#### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: **6228**, Parent PID: **6224**

#### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: **6232**, Parent PID: **6228**

#### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

#### File Activities

**File Read**

**Directory Enumerated**

### Analysis Process: tU468ylYjx PID: **6333**, Parent PID: **6232**

#### General

| | |
|---|---|
| Start time: | 04:28:59 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

### Analysis Process: tU468ylYjx PID: **6334**, Parent PID: **6232**

#### General

| | |
|---|---|
| Start time: | 04:28:59 |

Copyright Joe Security LLC 2022

| | |
|---|---|
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

## Analysis Process: tU468ylYjx PID: **6233**, Parent PID: **6228**

### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

## Analysis Process: tU468ylYjx PID: **6235**, Parent PID: **6228**

### General

| | |
|---|---|
| Start time: | 04:26:10 |
| Start date: | 14/05/2022 |
| Path: | /tmp/tU468ylYjx |
| Arguments: | n/a |
| File size: | 5388968 bytes |
| MD5 hash: | ae65271c943d3451b7f026d1fadccea6 |

Copyright Joe Security LLC 2022