


**ID:** 635046
**Sample Name:** mNMOQlPshG
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 11:39:28
**Date:** 27/05/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents

# Linux Analysis Report

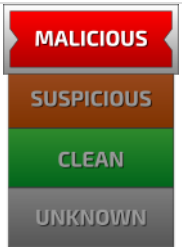
## mNMOQlPshG

## Overview

### General Information

| | |
|---|---|
| Sample Name: | mNMOQlPshG |
| Analysis ID: | 635046 |
| MD5: | 376ad57cf2b182.. |
| SHA1: | 21217f2f50c79b3.. |
| SHA256: | 6c47ca46c55529.. |
| Tags: | 32 arm elf |
| Infos: | |

### Detection



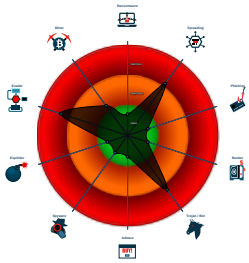

Mirai

| | |
|---|---|
| Score: | 72 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample deletes itself
- Sample is packed with UPX
- Deletes security-related log files
- Opens /proc/net/* files useful for fin…
- Executes the "kill" or "pkill" comma…
- Sample contains only a LOAD segm…
- Reads CPU information from /sys in…
- Yara signature match
- Deletes log files

### Classification



### Analysis Advice

**Static ELF header machine description suggests that the sample might not execute correctly on this machine.**

**All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.**

**Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 635046 |
| Start date and time: 27/05/202211:39:28 | 2022-05-27 11:39:28 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 49s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | mNMOQlPshG |
| 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: | mal72.spre.troj.evad.lin@0/0@0/0 |

## Warnings

## Process Tree

- **system is lnxubuntu20**
- mNMOQlPshG (PID: 6232, Parent: 6133, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/mNMOQlPshG
  - mNMOQlPshG New Fork (PID: 6235, Parent: 6232)
  - mNMOQlPshG New Fork (PID: 6237, Parent: 6232)
    - mNMOQlPshG New Fork (PID: 6239, Parent: 6237)

- mNMOQlPshG New Fork (PID: 6243, Parent: 6239)
- sh (PID: 6243, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*"
  - sh New Fork (PID: 6245, Parent: 6243)
  - rm (PID: 6245, Parent: 6243, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/hsperfdata_root /tmp/mNMOQlPshG /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jIxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf
- mNMOQlPshG New Fork (PID: 6253, Parent: 6239)
- sh (PID: 6253, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /var/log/wtmp"
  - sh New Fork (PID: 6255, Parent: 6253)
  - rm (PID: 6255, Parent: 6253, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /var/log/wtmp
- mNMOQlPshG New Fork (PID: 6256, Parent: 6239)
- sh (PID: 6256, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /tmp/*"
  - sh New Fork (PID: 6262, Parent: 6256)
  - rm (PID: 6262, Parent: 6256, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /tmp/*
- mNMOQlPshG New Fork (PID: 6263, Parent: 6239)
- sh (PID: 6263, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /bin/netstat"
  - sh New Fork (PID: 6265, Parent: 6263)
  - rm (PID: 6265, Parent: 6263, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /bin/netstat
- mNMOQlPshG New Fork (PID: 6266, Parent: 6239)
- sh (PID: 6266, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 busybox"
  - sh New Fork (PID: 6268, Parent: 6266)
  - pkill (PID: 6268, Parent: 6266, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 busybox
- mNMOQlPshG New Fork (PID: 6269, Parent: 6239)
- sh (PID: 6269, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 perl"
  - sh New Fork (PID: 6271, Parent: 6269)
  - pkill (PID: 6271, Parent: 6269, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 perl
- mNMOQlPshG New Fork (PID: 6274, Parent: 6239)
- sh (PID: 6274, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "pkill -9 python"
  - sh New Fork (PID: 6276, Parent: 6274)
  - pkill (PID: 6276, Parent: 6274, MD5: fa96a75a08109d8842e4865b2907d51f) Arguments: pkill -9 python
- mNMOQlPshG New Fork (PID: 6277, Parent: 6239)
- sh (PID: 6277, Parent: 6239, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -A INPUT -j DROP"
  - sh New Fork (PID: 6279, Parent: 6277)
  - iptables (PID: 6279, Parent: 6277, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -A INPUT -j DROP

- **cleanup**

# Yara Signatures

## Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| mNMOQlPshG | SUSP_ELF_LNX_UPX_Compressed_File | Detects a suspicious ELF binary with UPX compression | Florian Roth | • 0x9488:$s1: PROT_EXEC\|PROT_WRITE failed.<br>• 0x94f7:$s2: $Id: UPX<br>• 0x94a8:$s3: $Info: This file is packed with the UPX executable packer |

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 6232.1.00000000c2dc0f68.0000000061964638.r-x.sdmp | JoeSecurity_Mirai_8 | Yara detected Mirai | Joe Security | |
| 6237.1.00000000c2dc0f68.0000000061964638.r-x.sdmp | JoeSecurity_Mirai_8 | Yara detected Mirai | Joe Security | |
| 6235.1.00000000c2dc0f68.0000000061964638.r-x.sdmp | JoeSecurity_Mirai_8 | Yara detected Mirai | Joe Security | |

# Snort Signatures

**No Snort rule has matched**

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

### Spreading

Opens /proc/net/* files useful for finding connected devices and routers

### Data Obfuscation

Sample is packed with UPX

### Hooking and other Techniques for Hiding and Protection

Sample deletes itself

### Malware Analysis System Evasion

Deletes security-related log files

### Stealing of Sensitive Information

Yara detected Mirai

### Remote Access Functionality

Yara detected Mirai

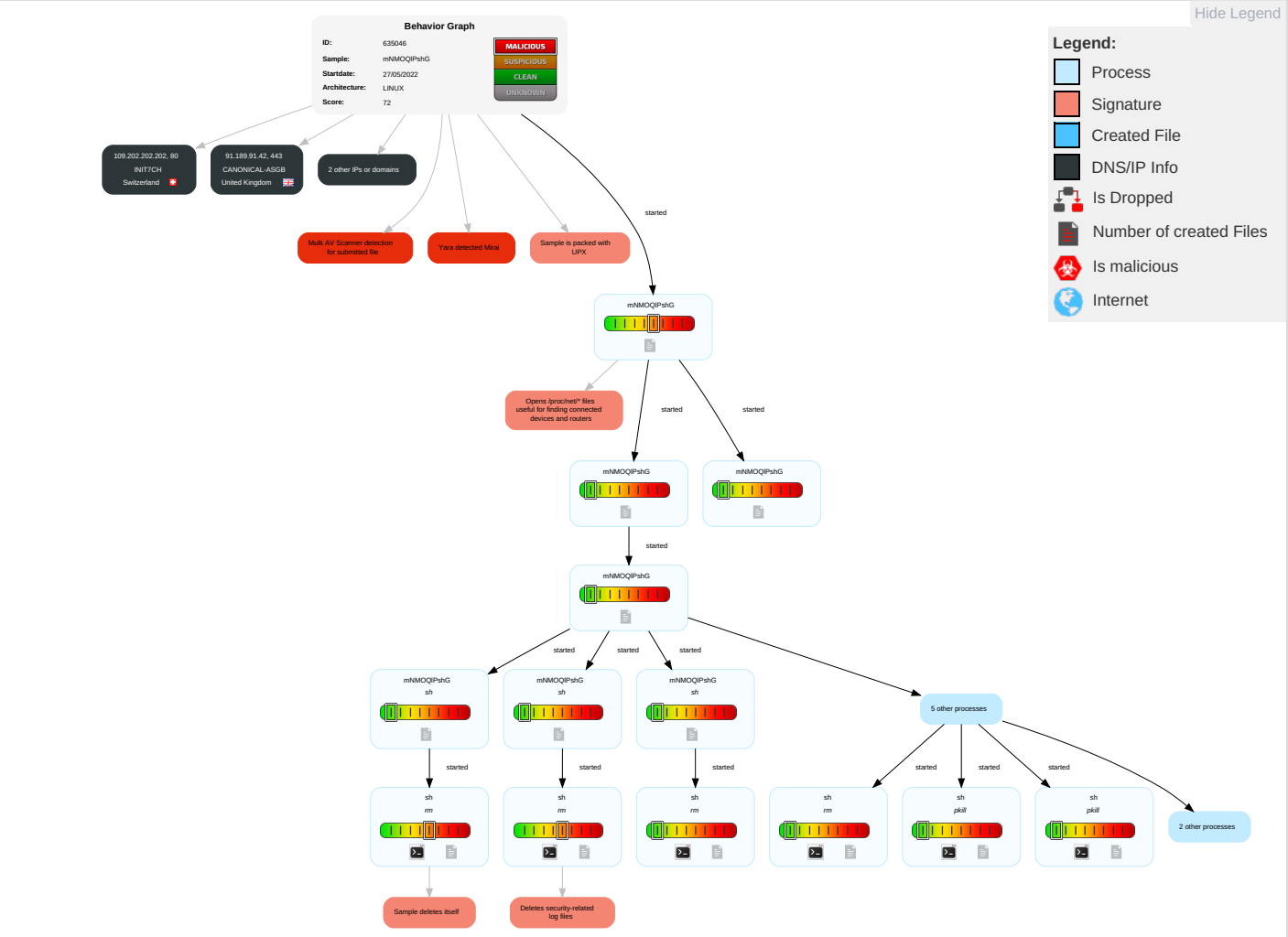
## Mitre Att&ck Matrix

| 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 | 1 Scripting | Path Interception | Path Interception | 1 Disable or Modify Tools | 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 | 1 Scripting | LSASS Memory | 1 System Information Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 Application Layer Protocol | 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 1 Indicator Removal on Host | Security Account Manager | 1 Remote System Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 1 Obfuscated Files or Information | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 1 1 File Deletion | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |

## Malware Configuration

No configs have been found

## Behavior Graph




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| mNMOQIPshG | 20% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

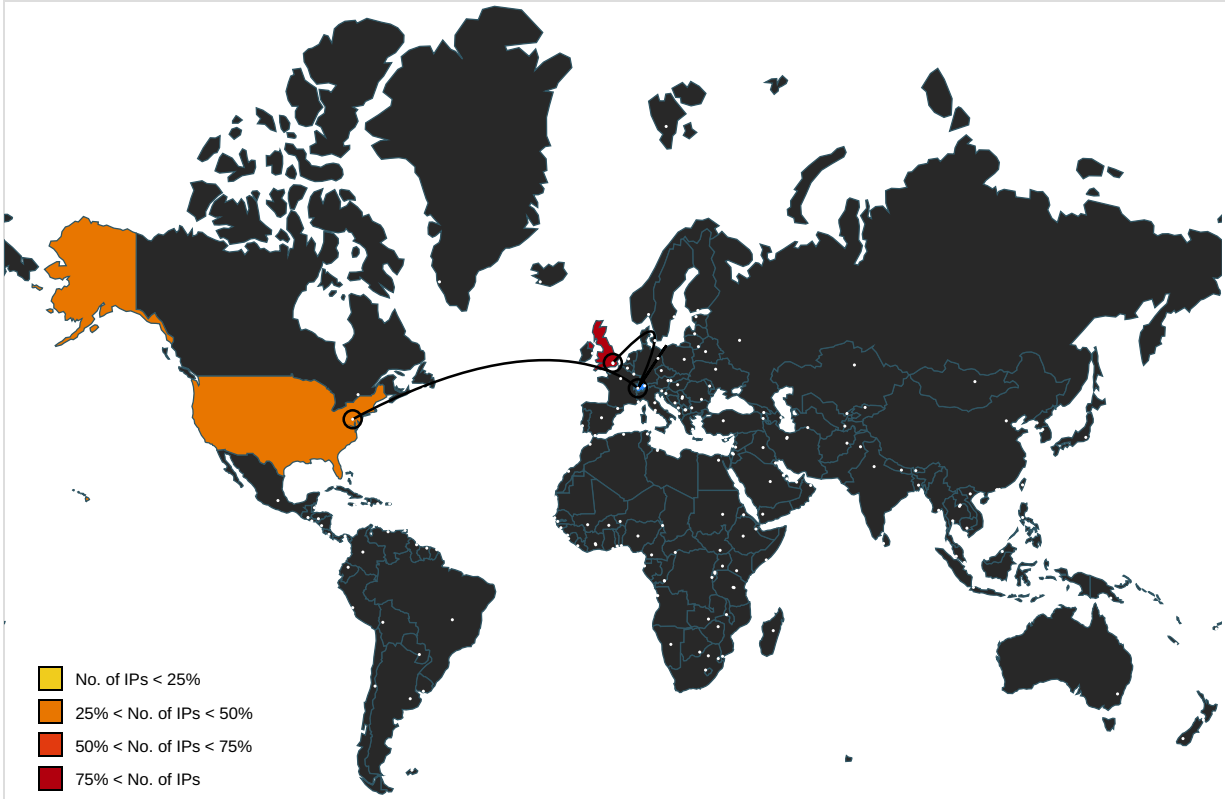
## Domains and IPs

### 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 |
|---|---|---|---|---|---|---|
| 172.245.210.119 | unknown | United States | | 36352 | AS-COLOCROSSINGUS | false |
| 109.202.202.202 | unknown | Switzerland | | 13030 | INIT7CH | false |
| 91.189.91.43 | unknown | United Kingdom | | 41231 | CANONICAL-ASGB | false |
| 91.189.91.42 | unknown | United Kingdom | | 41231 | CANONICAL-ASGB | false |

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped |
| Entropy (8bit): | 7.977681148888247 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | mNMOQlPshG |
| File size: | 49584 |
| MD5: | 376ad57cf2b182915c6406fc09268968 |
| SHA1: | 21217f2f50c79b3dea0a6f0219644d21d3dfc557 |
| SHA256: | 6c47ca46c555299c33e44f0db3a3efc886b2d2aaa9a8a865a236d3a80a36b8aa |
| SHA512: | c05495c16b109aed814c73054582194b201a93c0c9f9893d3b4572e4993eee4f46b11f325ef1dd27d878eb9c83fc33bbd8e93db92fe8ce4b778162f164a30055 |
| SSDEEP: | 1536:c9Afe4Si20ChlEsk0K4FdP9Y6zYm5ZGG1p:7feb7k0rf1NEm6q |
| TLSH: | 822302816BC394ACCF44D4BFC97D904DF73F95988EE9DD502438D7B0279202996E42E5 |
| File Content Preview: | .ELF...a.....(.....4.....4. ...(.....g...g.....(...(... (.....Q.td.....t.6.UPX!.....m[..m[.....S.....?.E.h;.}...^.....f13.Av4.jq.....un.V..j.$..g.."...K..E.1..:.i.R |

### 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: | 0x109b8 |
| Flags: | 0x202 |
| 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 | 0x8000 | 0x8000 | 0x9b67 | 0x9b67 | 4.0025 | 0x5 | R E | 0x8000 | | |
| LOAD | 0x28c4 | 0x328c4 | 0x328c4 | 0x0 | 0x0 | 0.0000 | 0x6 | RW | 0x8000 | | |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

## Network Behavior

### Network Port Distribution

**Total Packets: 11**

- 17372 undefined
- 80 (HTTP)
- 443 (HTTPS)

### TCP Packets

## System Behavior

### Analysis Process: mNMOQlPshG PID: **6232**, Parent PID: **6133**

#### General

| | |
|---|---|
| Start time: | 11:40:17 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | /tmp/mNMOQlPshG |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

#### File Activities

**File Deleted**

**File Read**

### Analysis Process: mNMOQlPshG PID: **6235**, Parent PID: **6232**

#### General

| | |
|---|---|
| Start time: | 11:40:17 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

### Analysis Process: mNMOQlPshG PID: **6237**, Parent PID: **6232**

#### General

| | |
|---|---|
| Start time: | 11:40:17 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |

| | |
|---|---|
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: mNMOQlPshG PID: **6239**, Parent PID: **6237**

### General

| | |
|---|---|
| Start time: | 11:40:17 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: mNMOQlPshG PID: **6243**, Parent PID: **6239**

### General

| | |
|---|---|
| Start time: | 11:40:19 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6243**, Parent PID: **6239**

### General

| | |
|---|---|
| Start time: | 11:40:19 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "rm -rf /tmp/* /var/* /var/run/* /var/tmp/*" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: sh PID: **6245**, Parent PID: **6243**

### General

| | |
|---|---|
| Start time: | 11:40:19 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: rm PID: **6245**, Parent PID: **6243**

### General

| | |
|---|---|
| Start time: | 11:40:19 |
| Start date: | 27/05/2022 |
| Path: | /usr/bin/rm |

| | |
|---|---|
| Arguments: | rm -rf /tmp/config-err-dHT8bZ /tmp/dmesgtail.log /tmp/hsperfdata_root /tmp/mNMOQlPshG /tmp/snap.lxd /tmp/ssh-hOQ5FjG2iVgO /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-c4RYFi /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-gKIF8e /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-gB0a9f /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-APWnLg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-IofUpj /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-AfPZzg /tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-x0xO0i /tmp/vmware-root_721-4290559889 /var/backups /var/cache /var/crash /var/lib /var/local /var/lock /var/log /var/mail /var/metrics /var/opt /var/run /var/snap /var/spool /var/tmp /var/run/NetworkManager /var/run/acpid.pid /var/run/acpid.socket /var/run/apport.lock /var/run/avahi-daemon /var/run/blkid /var/run/cloud-init /var/run/console-setup /var/run/crond.pid /var/run/crond.reboot /var/run/cryptsetup /var/run/cups /var/run/dbus /var/run/dmeventd-client /var/run/dmeventd-server /var/run/gdm3 /var/run/gdm3.pid /var/run/initctl /var/run/initramfs /var/run/irqbalance /var/run/lock /var/run/log /var/run/lvm /var/run/mlocate.daily.lock /var/run/mono-xsp4 /var/run/mono-xsp4.pid /var/run/motd.d /var/run/mount /var/run/multipathd.pid /var/run/netns /var/run/network /var/run/screen /var/run/sendsigs.omit.d /var/run/shm /var/run/snapd /var/run/snapd-snap.socket /var/run/snapd.socket /var/run/speech-dispatcher /var/run/spice-vdagentd /var/run/sshd /var/run/sshd.pid /var/run/sudo /var/run/systemd /var/run/tmpfiles.d /var/run/udev /var/run/udisks2 /var/run/unattended-upgrades.lock /var/run/user /var/run/utmp /var/run/uuidd /var/run/vmware /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-ModemManager.service-J6Q1Te /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-colord.service-srP90f /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-fwupd.service-biJ0Gi /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-switcheroo-control.service-1jIxdj /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-logind.service-llmWag /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-systemd-resolved.service-X16eHh /var/tmp/systemd-private-ec795e01d534441298b2bf519e4c51fc-upower.service-GpSnaf |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

**File Activities**

**File Deleted**

**File Read**

**Directory Enumerated**

## Analysis Process: mNMOQlPshG PID: **6253**, Parent PID: **6239**

### General

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6253**, Parent PID: **6239**

### General

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "rm -rf /var/log/wtmp" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

**File Activities**

**File Read**

## Analysis Process: sh PID: **6255**, Parent PID: **6253**

### General

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: rm PID: **6255**, Parent PID: **6253**

### General

| | |
|---|---|
| Start time: | 11:40:28 |

| | |
|---|---|
| Start date: | 27/05/2022 |
| Path: | /usr/bin/rm |
| Arguments: | rm -rf /var/log/wtmp |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

**File Activities**

**File Deleted**

**File Read**

## Analysis Process: mNMOQlPshG PID: **6256**, Parent PID: **6239**

**General**

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6256**, Parent PID: **6239**

**General**

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "rm -rf /tmp/*" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

**File Activities**

**File Read**

**Directory Enumerated**

## Analysis Process: sh PID: **6262**, Parent PID: **6256**

**General**

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: rm PID: **6262**, Parent PID: **6256**

**General**

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /usr/bin/rm |
| Arguments: | rm -rf /tmp/* |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

**File Activities**

**File Deleted**

**File Read**

## Analysis Process: mNMOQlPshG PID: **6263**, Parent PID: **6239**

| General | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6263**, Parent PID: **6239**

| General | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "rm -rf /bin/netstat" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

**File Activities**

**File Read**

## Analysis Process: sh PID: **6265**, Parent PID: **6263**

| General | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: rm PID: **6265**, Parent PID: **6263**

| General | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /usr/bin/rm |
| Arguments: | rm -rf /bin/netstat |
| File size: | 72056 bytes |
| MD5 hash: | aa2b5496fdbfd88e38791ab81f90b95b |

**File Activities**

**File Deleted**

**File Read**

## Analysis Process: mNMOQlPshG PID: **6266**, Parent PID: **6239**

| General | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6266**, Parent PID: **6239**

| General | |
|---|---|
| Start time: | 11:40:28 |

| | |
|---|---|
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "pkill -9 busybox" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

**File Activities**

**File Read**

## Analysis Process: sh PID: **6268**, Parent PID: **6266**

**General**

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: pkill PID: **6268**, Parent PID: **6266**

**General**

| | |
|---|---|
| Start time: | 11:40:28 |
| Start date: | 27/05/2022 |
| Path: | /usr/bin/pkill |
| Arguments: | pkill -9 busybox |
| File size: | 30968 bytes |
| MD5 hash: | fa96a75a08109d8842e4865b2907d51f |

**File Activities**

**File Read**

**Directory Enumerated**

## Analysis Process: mNMOQlPshG PID: **6269**, Parent PID: **6239**

**General**

| | |
|---|---|
| Start time: | 11:40:30 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6269**, Parent PID: **6239**

**General**

| | |
|---|---|
| Start time: | 11:40:30 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "pkill -9 perl" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

**File Activities**

**File Read**

## Analysis Process: sh PID: **6271**, Parent PID: **6269**

**General**

| | |
|---|---|
| Start time: | 11:40:30 |

| | |
|---|---|
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: pkill PID: **6271**, Parent PID: **6269**

### General

| | |
|---|---|
| Start time: | 11:40:30 |
| Start date: | 27/05/2022 |
| Path: | /usr/bin/pkill |
| Arguments: | pkill -9 perl |
| File size: | 30968 bytes |
| MD5 hash: | fa96a75a08109d8842e4865b2907d51f |

### File Activities

**File Read**

**Directory Enumerated**

## Analysis Process: mNMOQlPshG PID: **6274**, Parent PID: **6239**

### General

| | |
|---|---|
| Start time: | 11:40:34 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6274**, Parent PID: **6239**

### General

| | |
|---|---|
| Start time: | 11:40:34 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "pkill -9 python" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

**File Read**

## Analysis Process: sh PID: **6276**, Parent PID: **6274**

### General

| | |
|---|---|
| Start time: | 11:40:34 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: pkill PID: **6276**, Parent PID: **6274**

### General

| | |
|---|---|
| Start time: | 11:40:34 |
| Start date: | 27/05/2022 |
| Path: | /usr/bin/pkill |
| Arguments: | pkill -9 python |

| | |
|---|---|
| File size: | 30968 bytes |
| MD5 hash: | fa96a75a08109d8842e4865b2907d51f |

**File Activities**

**File Read**

**Directory Enumerated**

## Analysis Process: mNMOQlPshG PID: **6277**, Parent PID: **6239**

**General**

| | |
|---|---|
| Start time: | 11:40:36 |
| Start date: | 27/05/2022 |
| Path: | /tmp/mNMOQlPshG |
| Arguments: | n/a |
| File size: | 4956856 bytes |
| MD5 hash: | 5ebfcae4fe2471fcc5695c2394773ff1 |

## Analysis Process: sh PID: **6277**, Parent PID: **6239**

**General**

| | |
|---|---|
| Start time: | 11:40:36 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | sh -c "iptables -A INPUT -j DROP" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

**File Activities**

**File Read**

## Analysis Process: sh PID: **6279**, Parent PID: **6277**

**General**

| | |
|---|---|
| Start time: | 11:40:36 |
| Start date: | 27/05/2022 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: iptables PID: **6279**, Parent PID: **6277**

**General**

| | |
|---|---|
| Start time: | 11:40:36 |
| Start date: | 27/05/2022 |
| Path: | /usr/sbin/iptables |
| Arguments: | iptables -A INPUT -j DROP |
| File size: | 99296 bytes |
| MD5 hash: | 1ab05fef765b6342cdfadaa5275b33af |

**File Activities**

**File Read**