ID: 830716
Sample Name: mbl5k2b7z8.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:23:54
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

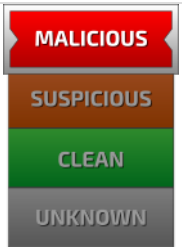
mbl5k2b7z8.elf

Overview

General Information

Sample Name:	mbl5k2b7z8.elf
Original Sample Name:	d7f3432247daa..
Analysis ID:	830716
MD5:	d7f3432247daa..
SHA1:	58ddd0d4593d...
SHA256:	686fb10624e0f...
Tags:	32 elf mips mirai
Infos:	

Detection



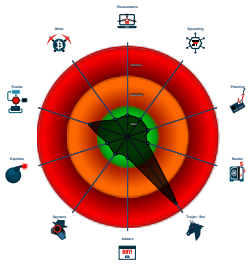
Mirai, Moobot

Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Moobot
- Snort IDS alert for network traffic
- Connects to many ports of the same…
- Uses known network protocols on n…
- Performs DNS queries to domains w…
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…

Classification



Analysis Advice

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

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

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

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830716
Start date and time:	2023-03-20 16:23:54 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample file name:	mbl5k2b7z8.elf
Original Sample Name:	d7f3432247daa3564a2f9f282fd892ca.elf
Detection:	MAL
Classification:	mal96.troj.linELF@0/0@1/0

Warnings

Runtime Messages

Command:	/tmp/mbl5k2b7z8.elf
PID:	6231
Exit Code:	0
Exit Code Info:	

Killed:	False
Standard Output:	done.
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- mbl5k2b7z8.elf (PID: 6231, Parent: 6130, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/mbl5k2b7z8.elf
  - mbl5k2b7z8.elf New Fork (PID: 6233, Parent: 6231)
  - sh (PID: 6233, Parent: 6231, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/busybox && mkdir bin; >bin/busybox && mv /tmp/mbl5k2b7z8.elf bin/busybox; chmod 777 bin/busybox"
    - sh New Fork (PID: 6235, Parent: 6233)
    - rm (PID: 6235, Parent: 6233, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/busybox
    - sh New Fork (PID: 6236, Parent: 6233)
    - mkdir (PID: 6236, Parent: 6233, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6237, Parent: 6233)
    - mv (PID: 6237, Parent: 6233, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/mbl5k2b7z8.elf bin/busybox
    - sh New Fork (PID: 6238, Parent: 6233)
    - chmod (PID: 6238, Parent: 6233, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/busybox
  - mbl5k2b7z8.elf New Fork (PID: 6239, Parent: 6231)
    - mbl5k2b7z8.elf New Fork (PID: 6241, Parent: 6239)
    - mbl5k2b7z8.elf New Fork (PID: 6243, Parent: 6239)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	**http://** osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Name	Description	Attribution	Blogpost URLs	Link
MooBot		No Attribution	**http://** https://blog.netlab.360.com/ddos-botnet-moobot-en/https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/https://otx.alienvault.com/pulse/6075b645942d5adf9bb8949bhttps://unit42.paloaltonetworks.com/moobot-d-link-devices/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.moobot

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
mbl5k2b7z8.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
mbl5k2b7z8.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
mbl5k2b7z8.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x11834:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11848:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1185c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11870:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11884:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11898:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118ac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118d4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118fc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11910:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11924:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11938:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1194c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11960:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11974:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11988:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1199c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F

Memory Dumps

Source	Rule	Description	Author	Strings
6231.1.00007f8304400000.00007f8304414000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6231.1.00007f8304400000.00007f8304414000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6231.1.00007f8304400000.00007f8304414000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x11834:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11848:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1185c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11870:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11884:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11898:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118ac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118d4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x118fc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11910:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11924:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11938:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1194c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11960:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11974:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11988:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1199c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x119c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Process Memory Space: mbl5k2b7z8.elf PID: 6231	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
Process Memory Space: mbl5k2b7z8.elf PID: 6231	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x8ba:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8ce:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8e2:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x8f6:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x90a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x91e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x932:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x946:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x95a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x96e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x982:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x996:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x9aa:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x9be:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x9d2:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x9e6:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x9fa:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xa0e:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xa22:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xa36:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xa4a:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F

Snort Signatures

ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1) - Source IP: 192.168.2.23 - Destination IP: 195.133.40.202

Timestamp:	192.168.2.23195.133.40.20236176569992030490 03/20/23-16:24:46.219802
SID:	2030490
Source Port:	36176
Destination Port:	56999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 163.18.94.240

Timestamp:	192.168.2.23163.18.94.240606703721528352222 03/20/23-16:25:01.651288
SID:	2835222
Source Port:	60670
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response - Source IP: 195.133.40.202 - Destination IP: 192.168.2.23

Timestamp:	195.133.40.202192.168.2.2356999361762030489 03/20/23-16:25:13.708877
SID:	2030489
Source Port:	56999
Destination Port:	36176
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 34.128.181.63

Timestamp:	192.168.2.2334.128.181.63542643721528352222 03/20/23-16:25:15.146221
SID:	2835222
Source Port:	54264
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.37.71.18

Timestamp:	192.168.2.2341.37.71.1833478372152835222 03/20/23-16:25:08.055278
SID:	2835222
Source Port:	33478
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

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

Uses known network protocols on non-standard ports

Performs DNS queries to domains with low reputation

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Sets full permissions to files and/or directories

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Yara detected Moobot

Remote Access Functionality

Yara detected Mirai

Yara detected Moobot

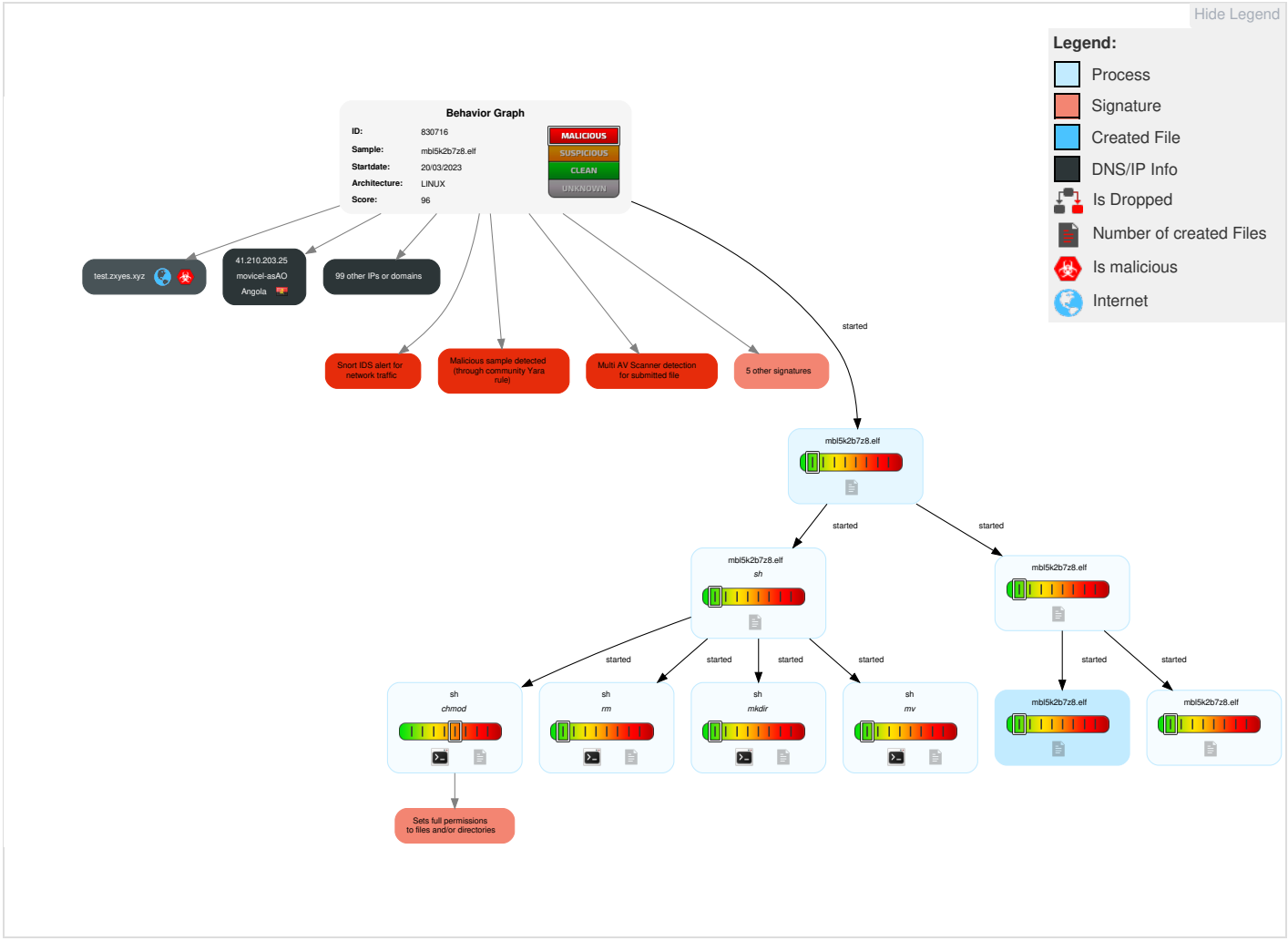
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	Path Interception	2 File and Directory Permissions Modification	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 File Deletion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	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	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
mbl5k2b7z8.elf	64%	ReversingLabs	Linux.Trojan.Mirai	
mbl5k2b7z8.elf	59%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

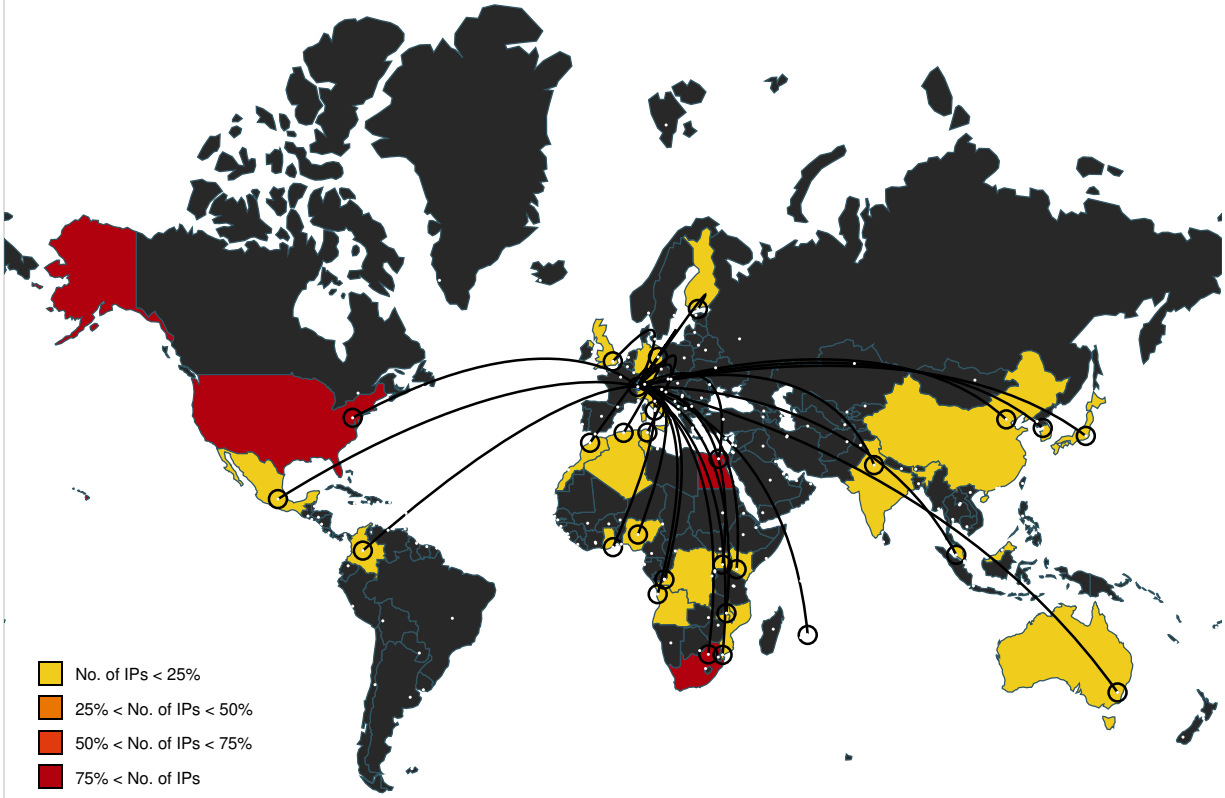
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
test.zxyes.xyz	195.133.40.202	true	true		unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.155.206.222	unknown	Australia		17983	COLESMYER-AS-APColesMyerAU	false
197.91.42.245	unknown	South Africa		10474	OPTINETZA	false
27.236.72.206	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
41.134.200.128	unknown	South Africa		10474	OPTINETZA	false
197.179.205.76	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.165.32.49	unknown	Egypt		24863	LINKdotNET-ASEG	false
12.198.103.37	unknown	United States		7018	ATT-INTERNET4US	false
150.247.95.86	unknown	United States		2527	SO-NETSo-netEntertainmentCorporationJP	false
41.51.182.15	unknown	South Africa		37168	CELL-CZA	false
157.33.200.173	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
41.72.45.47	unknown	Angola		37155	NETONEAO	false
157.59.194.195	unknown	United States		3598	MICROSOFT-CORP-ASUS	false
197.27.94.108	unknown	Tunisia		37492	ORANGE-TN	false
197.40.144.189	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.120.132.150	unknown	Egypt		36992	ETISALAT-MISREG	false
197.58.18.255	unknown	Egypt		8452	TE-ASTE-ASEG	false
212.97.40.105	unknown	Italy		5602	AS-IRIDEOS-KPIT	false
161.135.249.204	unknown	United States		7726	FITC-ASUS	false
60.52.117.189	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
134.105.51.121	unknown	Germany		42873	MPG-FR-SFreiburgStrafrechtDE	false
41.210.203.25	unknown	Angola		37081	movicel-asAO	false
157.117.145.231	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
41.195.197.57	unknown	South Africa		16637	MTNNS-ASZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.24.86.1	unknown	South Africa		36994	Vodacom-VBZA	false
197.57.40.27	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.252.195.39	unknown	United States		3592	TRINCOLL-ASUS	false
75.180.90.80	unknown	United States		10796	TWC-10796-MIDWESTUS	false
41.190.129.200	unknown	Mauritius		36997	INFOCOM-UG	false
157.168.229.19	unknown	Switzerland		22192	SSHENETUS	false
197.90.198.169	unknown	South Africa		10474	OPTINETZA	false
197.211.114.208	unknown	Malawi		37187	SKYBANDMW	false
169.228.238.170	unknown	United States		7377	UCSDUS	false
157.236.83.1	unknown	United Kingdom		4704	SANNETRakutenMobileIncJP	false
115.38.238.72	unknown	Japan		18126	CTCXChubuTelecommunicationsCompanyIncJP	false
197.231.174.170	unknown	South Africa		37055	EMIDZA	false
41.85.32.176	unknown	South Africa		22355	FROGFOOTZA	false
63.169.198.175	unknown	United States		1239	SPRINTLINKUS	false
41.154.82.108	unknown	South Africa		37079	SMMTZA	false
157.145.56.98	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
217.56.211.180	unknown	Italy		3269	ASN-IBSNAZIT	false
157.212.14.231	unknown	United States		4704	SANNETRakutenMobileIncJP	false
41.55.86.167	unknown	South Africa		37168	CELL-CZA	false
197.20.220.125	unknown	Tunisia		37693	TUNISIANATN	false
41.203.88.30	unknown	Nigeria		37148	globacom-asNG	false
41.53.150.198	unknown	South Africa		37168	CELL-CZA	false
197.173.143.35	unknown	South Africa		37168	CELL-CZA	false
197.247.28.16	unknown	Morocco		36925	ASMediMA	false
157.109.178.100	unknown	Japan		37919	SEGASEGAHoldingsCoLtdJP	false
138.251.7.144	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
157.129.41.254	unknown	Finland		41701	CAP-FIN-ASFI	false
197.173.131.66	unknown	South Africa		37168	CELL-CZA	false
157.133.97.49	unknown	United States		133767	SAP_DC_SYDSAPAU	false
197.239.56.166	unknown	Uganda		37075	ZAINUGASUG	false
53.35.84.18	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
197.38.15.101	unknown	Egypt		8452	TE-ASTE-ASEG	false
96.99.206.144	unknown	United States		7922	COMCAST-7922US	false
187.128.208.242	unknown	Mexico		28283	AdylnetTelecomBR	false
70.7.125.183	unknown	United States		10507	SPCSUS	false
197.51.4.216	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.255.96.213	unknown	Ghana		37074	UG-ASGH	false
157.37.189.48	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
197.60.132.87	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.180.144.76	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
41.72.21.40	unknown	Angola		37155	NETONEAO	false
194.72.164.158	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
169.37.67.179	unknown	Switzerland		37611	AfrihostZA	false
41.133.169.251	unknown	South Africa		10474	OPTINETZA	false
41.243.103.151	unknown	Congo The Democratic Republic of The		37684	ANGANI-ASKE	false
41.88.141.232	unknown	Egypt		33771	SAFARICOM-LIMITEDKE	false
157.21.202.207	unknown	United States		53446	EVMSUS	false
157.135.154.175	unknown	United States		600	OARNET-ASUS	false
41.196.1.100	unknown	Egypt		24863	LINKdotNET-ASEG	false
43.26.93.139	unknown	Japan		4249	LILLY-ASUS	false
17.220.123.235	unknown	United States		714	APPLE-ENGINEERINGUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
121.18.220.148	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
157.215.239.15	unknown	United States		4704	SANNETRakutenMobileIncJP	false
197.189.59.11	unknown	Congo The Democratic Republic of The		37598	EbaleCD	false
197.143.173.239	unknown	Algeria		36891	ICOSNET-ASDZ	false
90.243.221.86	unknown	United Kingdom		5378	VodafoneGB	false
157.101.64.14	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	false
197.223.247.155	unknown	Egypt		37069	MOBINILEG	false
197.131.139.241	unknown	Morocco		6713	IAM-ASMA	false
197.249.217.5	unknown	Mozambique		25139	TVCABO-ASEU	false
47.39.49.244	unknown	United States		20115	CHARTER-20115US	false
41.187.12.178	unknown	Egypt		20928	NOOR-ASEG	false
41.168.23.240	unknown	South Africa		36937	Neotel-ASZA	false
41.235.194.79	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.121.74.199	unknown	Egypt		36992	ETISALAT-MISREG	false
157.253.237.105	unknown	Colombia		3603	UniversitydeLosAndesCO	false
41.39.34.249	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.41.93.128	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.246.44.154	unknown	South Africa		5713	SAIX-NETZA	false
197.21.42.101	unknown	Tunisia		37693	TUNISIANATN	false
34.167.178.222	unknown	United States		2686	ATGS-MMD-ASUS	false
157.98.55.36	unknown	United States		3527	NIH-NETUS	false
32.150.51.8	unknown	United States		2686	ATGS-MMD-ASUS	false
157.28.31.173	unknown	Italy		8968	BT-ITALIAIT	false
41.61.164.249	unknown	South Africa		36943	GridhostZA	false
107.46.141.66	unknown	United States		16567	NETRIX-16567US	false
41.33.29.216	unknown	Egypt		8452	TE-ASTE-ASEG	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.442878534201549
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	mbl5k2b7z8.elf
File size:	84780
MD5:	d7f3432247daa3564a2f9f282fd892ca
SHA1:	58ddd0d4593d6362f371acb8877671edb8463d99
SHA256:	686fb10624e0f6001922f5a7da9d6c10671b960e04da8cb6300bd81671d4407d
SHA512:	3a08fec1a6e3e892ff9f4e08cc2d1ed1fbc0c321c84440e82a34cb348e2e20456e1e508bf52c146d485765f46354daa041389a9ea722ec12d0ad5534a19c38e0
SSDEEP:	768:2ty6IP7M/kq0INRhfuN2Eo9tl/de2YlwHKRH0I84EH6UTU77ZDYovZ73x/nL8y89:Rakdn2Eo3ePu5GTgRYo99Be037Wj/
TLSH:	2B83A51E7E228FADF76D823147B74E25A69833C627E1D641E16CD6012E6034E641FFE8
File Content Preview:	.ELF.....@.`...4..H.....4. ...(.....@...@....6`..6`.....@..E@..E@.....+.....dt.Q.....<...'..\...!'.....<...'..8...!... ....'9... .....<...'.....!.....'9.

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x115d0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x4116f0	0x116f0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x411750	0x11750	0x1f10	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x454000	0x14000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x454008	0x14008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x454014	0x14014	0x44	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x454060	0x14060	0x3a0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x454400	0x14400	0x498	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x454898	0x14898	0x1c	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x4548c0	0x14898	0x2250	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x9c6	0x14898	0x0	0x0	0x0		0	0	1

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.shstrtab	STRTAB	0x0	0x14898	0x64	0x0	0x0		0	0	1

Program Segments

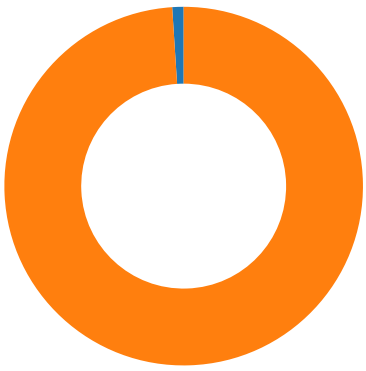
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x13660	0x13660	5.5807	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x14000	0x454000	0x454000	0x898	0x2b10	3.8882	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23195.133.40.2023617656999203049003/20/23-16:24:46.219802	TCP	2030490	ET TROJAN ELF/MooBot Mirai DDoS Variant CnC Checkin M1 (Group String Len 1)	36176	56999	192.168.2.23	195.133.40.202
192.168.2.23163.18.94.2406067037215283522203/20/23-16:25:01.651288	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60670	37215	192.168.2.23	163.18.94.240
195.133.40.202192.168.2.235699936176203048903/20/23-16:25:13.708877	TCP	2030489	ET TROJAN ELF/MooBot Mirai DDoS Variant Server Response	56999	36176	195.133.40.202	192.168.2.23
192.168.2.2334.128.181.635426437215283522203/20/23-16:25:15.146221	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	54264	37215	192.168.2.23	34.128.181.63
192.168.2.2341.37.71.183347837215283522203/20/23-16:25:08.055278	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33478	37215	192.168.2.23	41.37.71.18

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:24:46.162062883 CET	192.168.2.23	8.8.8.8	0xdcc8	Standard query (0)	test.zxyes.xyz	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 16:24:46.186434984 CET	8.8.8.8	192.168.2.23	0xdcc8	No error (0)	test.zxyes.xyz		195.133.40.202	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: mbl5k2b7z8.elf PID: 6231, Parent PID: 6130

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/tmp/mbl5k2b7z8.elf
Arguments:	/tmp/mbl5k2b7z8.elf
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: mbl5k2b7z8.elf PID: 6233, Parent PID: 6231

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/tmp/mbl5k2b7z8.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sh PID: 6233, Parent PID: 6231

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/busybox && mkdir bin; >bin/busybox && mv /tmp/mbl5k2b7z8.elf bin/busybox; chmod 777 bin/busybox"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 6235, Parent PID: 6233

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 6235, Parent PID: 6233

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/usr/bin/rm
Arguments:	rm -rf bin/busybox
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: sh PID: **6236**, Parent PID: **6233**

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **6236**, Parent PID: **6233**

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/usr/bin/mkdir
Arguments:	mkdir bin
File size:	88408 bytes
MD5 hash:	088c9d1df5a28ed16c726eca15964cb7

File Activities

File Read

Directory Created

Analysis Process: sh PID: **6237**, Parent PID: **6233**

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: **6237**, Parent PID: **6233**

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/usr/bin/mv
Arguments:	mv /tmp/mbl5k2b7z8.elf bin/busybox
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: 6238, Parent PID: 6233

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: 6238, Parent PID: 6233

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/usr/bin/chmod
Arguments:	chmod 777 bin/busybox
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Permission Modified

Analysis Process: mbl5k2b7z8.elf PID: 6239, Parent PID: 6231

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/tmp/mbl5k2b7z8.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: mbl5k2b7z8.elf PID: 6241, Parent PID: 6239

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/tmp/mbl5k2b7z8.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: mbl5k2b7z8.elf PID: 6243, Parent PID: 6239

General

Start time:	16:24:45
Start date:	20/03/2023
Path:	/tmp/mbl5k2b7z8.elf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c