ID: 1383029
Sample Name: z8lHAECIcU.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:05:11
Date: 30/01/2024
Version: 39.0.0 Ruby

Table of Contents

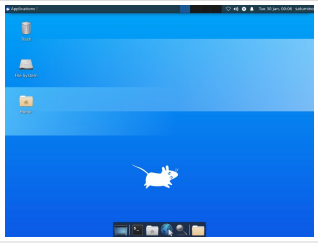
Linux Analysis Report

z8lHAECIcU.elf

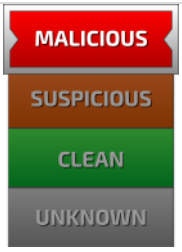
Overview

General Information

Sample name:	z8lHAECIcU.elfrenamed because original name is a hash value
Original sample name:	b70c1e3b204c…
Analysis ID:	1383029
MD5:	b70c1e3b204c…
SHA1:	3a0544996684…
SHA256:	7829c72ee62b…
Tags:	32 elf mirai powerpc
Infos:	



Detection



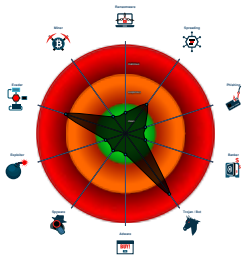
Mirai

Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Detected Mirai
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Yara detected Mirai
- Sample is packed with UPX
- Uses known network protocols on n…
- Detected TCP or UDP traffic on non…
- ELF contains segments with high en…
- Enumerates processes within the "p…

Classification



Analysis Advice

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

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

General Information

Joe Sandbox version:	39.0.0 Ruby
Analysis ID:	1383029
Start date and time:	2024-01-30 00:05:11 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 6m 44s
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 name:	z8lHAECIcU.elfrenamed because original name is a hash value
Original Sample Name:	b70c1e3b204c6b5b706f49347cb1f35a.elf
Detection:	MAL
Classification:	mal96.troj.evad.linELF@0/0@2/0

Warnings

Runtime Messages

Command:	/tmp/z8lHAECIcU.elf
PID:	5487

Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- z8lHAECIcU.elf (PID: 5487, Parent: 5410, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/z8lHAECIcU.elf
  - z8lHAECIcU.elf New Fork (PID: 5489, Parent: 5487)
    - z8lHAECIcU.elf New Fork (PID: 5606, Parent: 5489)
    - z8lHAECIcU.elf New Fork (PID: 5608, Parent: 5489)
      - z8lHAECIcU.elf New Fork (PID: 5610, Parent: 5608)
        - z8lHAECIcU.elf New Fork (PID: 5627, Parent: 5610)
        - z8lHAECIcU.elf New Fork (PID: 5628, Parent: 5610)
      - z8lHAECIcU.elf New Fork (PID: 5611, Parent: 5608)
      - z8lHAECIcU.elf New Fork (PID: 5614, Parent: 5608)
    - z8lHAECIcU.elf New Fork (PID: 5491, Parent: 5487)
    - z8lHAECIcU.elf New Fork (PID: 5493, Parent: 5487)
      - z8lHAECIcU.elf New Fork (PID: 5495, Parent: 5493)
        - z8lHAECIcU.elf New Fork (PID: 5602, Parent: 5495)
        - z8lHAECIcU.elf New Fork (PID: 5604, Parent: 5495)
      - z8lHAECIcU.elf New Fork (PID: 5497, Parent: 5493)
      - z8lHAECIcU.elf New Fork (PID: 5498, Parent: 5493)
- **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

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
5627.1.00007f7f8800b000.00007f7f88010000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x41d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x41e4:$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 • 0x41f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x420c:$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 • 0x4220:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4234:$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 • 0x4248:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x425c:$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 • 0x4270:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4284:$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 • 0x4298:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42ac:$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 • 0x42c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42d4:$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 • 0x42e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42fc:$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 • 0x4310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4324:$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 • 0x4338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x434c:$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 • 0x4360:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
5627.1.00007f7f8800b000.00007f7f88010000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x4728:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64
5602.1.00007f7f8800b000.00007f7f88010000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x41d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x41e4:$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 • 0x41f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x420c:$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 • 0x4220:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4234:$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 • 0x4248:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x425c:$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 • 0x4270:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4284:$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 • 0x4298:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42ac:$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 • 0x42c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42d4:$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 • 0x42e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42fc:$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 • 0x4310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4324:$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 • 0x4338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x434c:$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 • 0x4360:$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

Source	Rule	Description	Author	Strings
5602.1.00007f7f8800b000.00007f7f88010000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x4728:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64
5487.1.00007f7f8800b000.00007f7f88010000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x41d0:$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 • 0x41e4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x41f8:$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 • 0x420c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4220:$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 • 0x4234:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4248:$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 • 0x425c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4270:$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 • 0x4284:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4298:$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 • 0x42ac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42c0:$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 • 0x42d4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42e8:$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 • 0x42fc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4310:$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 • 0x4324:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4338:$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 • 0x434c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4360:$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
Click to see the 22 entries				

Snort Signatures

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.14 - Destination IP: 89.213.31.121

Timestamp:	192.168.2.1489.213.31.12140526232829347 01/30/24-00:09:17.253981
SID:	2829347
Source Port:	40526
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Information Leak

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.14 - Destination IP: 178.163.132.143

Timestamp:	192.168.2.14178.163.132.14338860232829347 01/30/24-00:08:46.579114
SID:	2829347
Source Port:	38860
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Information Leak

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.14 - Destination IP: 121.120.101.1

Timestamp:	192.168.2.14121.120.101.140538232829347 01/30/24-00:09:06.090881
SID:	2829347
Source Port:	40538
Destination Port:	23
Protocol:	TCP

Classtype:	Attempted Information Leak

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.13 - Destination IP: 186.39.129.4

Timestamp:	192.168.2.13186.39.129.456244232829347 01/30/24-00:08:32.204233
SID:	2829347
Source Port:	56244
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Information Leak

ET TROJAN Possible Linux.Mirai Login Attempt (klv123) - Source IP: 192.168.2.14 - Destination IP: 187.168.4.70

Timestamp:	192.168.2.14187.168.4.7039762232023443 01/30/24-00:08:47.045048
SID:	2023443
Source Port:	39762
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Administrator Privilege Gain

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.14 - Destination IP: 171.34.207.12

Timestamp:	192.168.2.14171.34.207.1247532232829347 01/30/24-00:09:06.318964
SID:	2829347
Source Port:	47532
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Information Leak

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.13 - Destination IP: 201.176.27.87

Timestamp:	192.168.2.13201.176.27.8736480232829347 01/30/24-00:07:53.255345
SID:	2829347
Source Port:	36480
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Information Leak

ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723) - Source IP: 192.168.2.14 - Destination IP: 37.98.227.163

Timestamp:	192.168.2.1437.98.227.16349802232829347 01/30/24-00:08:57.073420
SID:	2829347
Source Port:	49802
Destination Port:	23
Protocol:	TCP
Classtype:	Attempted Information Leak

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Detected Mirai

Yara detected Mirai

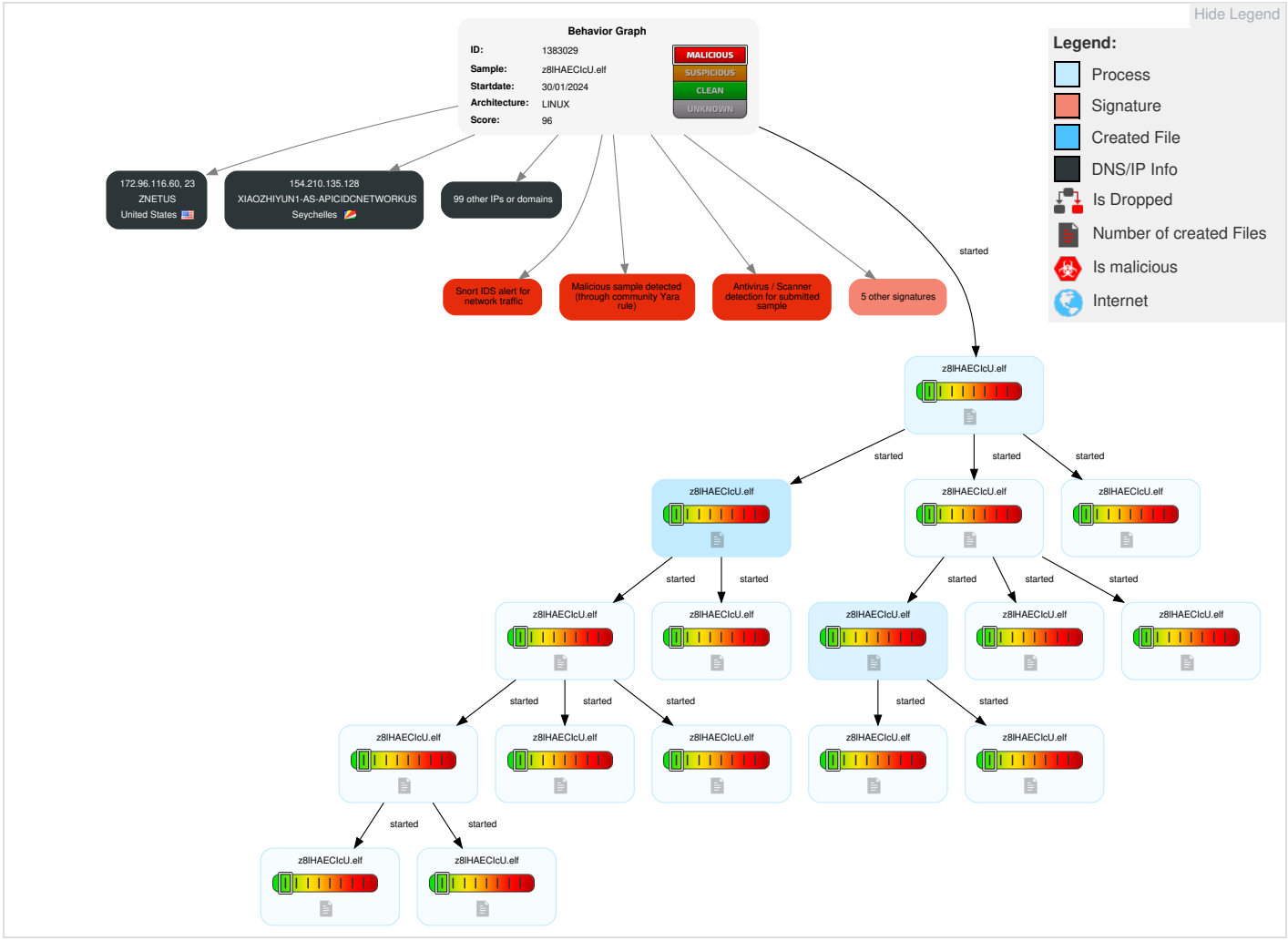
Mitre Att&ck Matrix

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated Files or Information	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	1 1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	2 Application Layer Protocol	Traffic Duplication	Data Destruction

Malware Configuration

No configs have been found

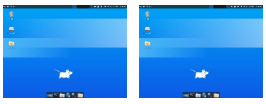
Behavior Graph

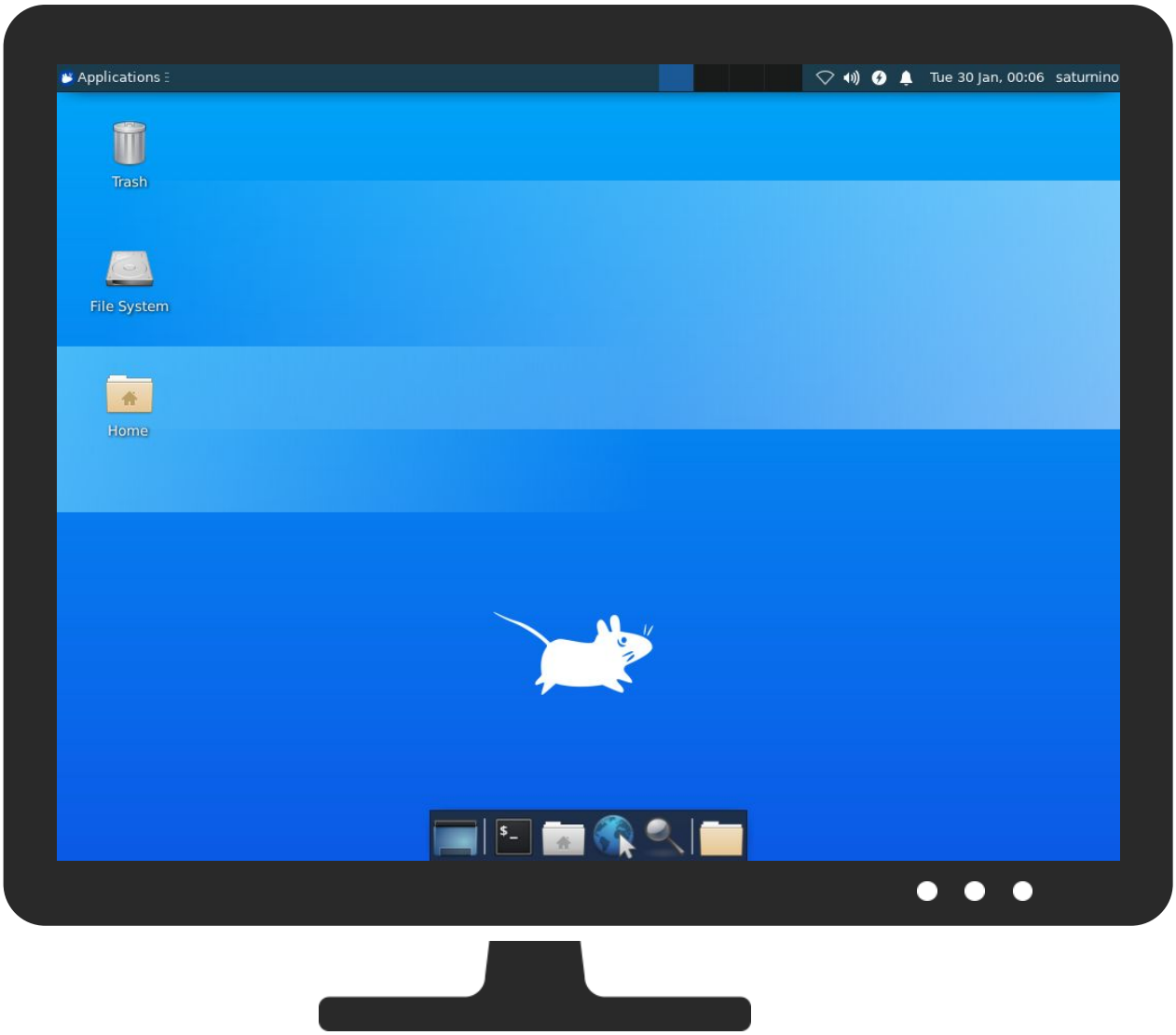


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
z8lHAEClcU.elf	55%	ReversingLabs	Linux.Trojan.Mirai	
z8lHAEClcU.elf	100%	Avira	EXP/ELF.Agent.Gen.F	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

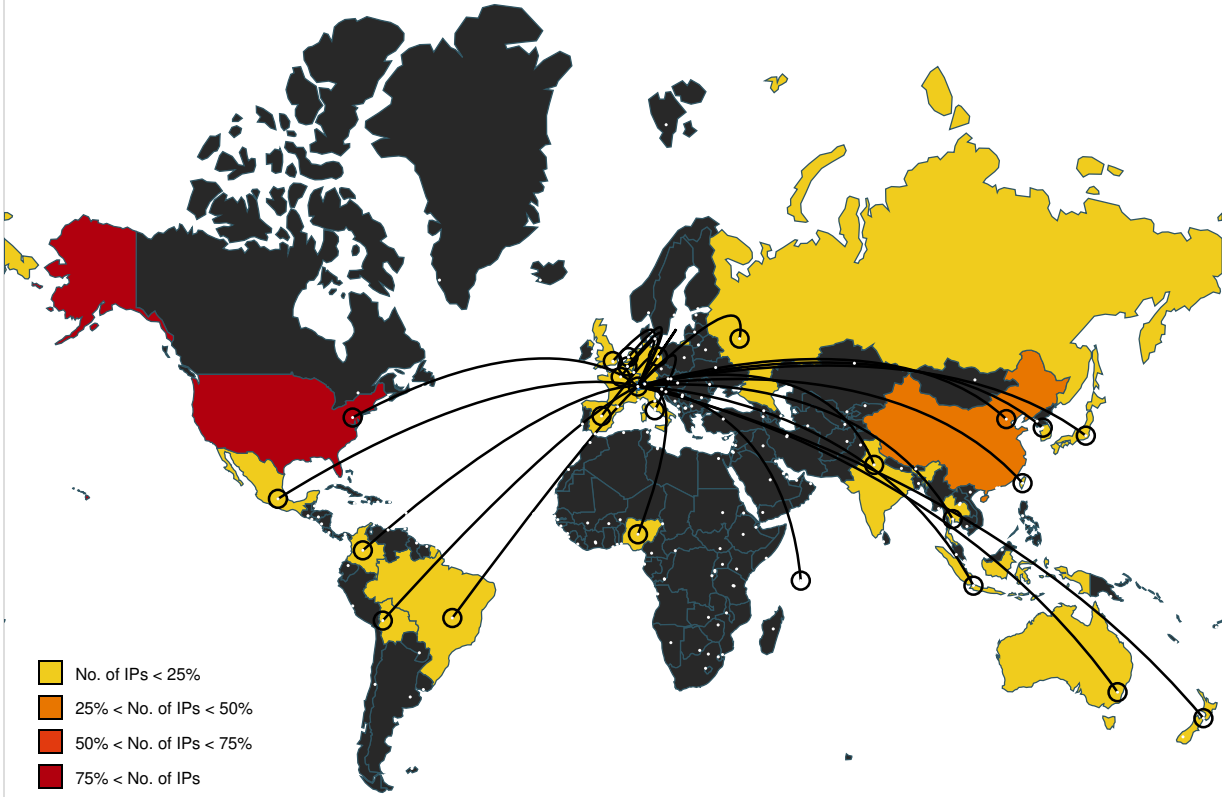
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.35.25	true	false		high

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.20.10.217	unknown	United States		264008	LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR	false
62.15.62.97	unknown	Spain		12479	UNI2-ASES	false
14.116.8.18	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
182.248.9.31	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
139.176.199.183	unknown	China		8968	BT-ITALIAIT	false
252.93.238.106	unknown	Reserved		unknown	unknown	false
5.5.54.254	unknown	Germany		6805	TDDE-ASN1DE	false
146.207.94.223	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
48.41.224.232	unknown	United States		2686	ATGS-MMD-ASUS	false
12.128.179.252	unknown	United States		7018	ATT-INTERNET4US	false
134.245.99.183	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
158.30.183.12	unknown	United States		1504	DNIC-AS-01504US	false
207.24.250.138	unknown	United States		701	UUNETUS	false
159.192.195.151	unknown	Thailand		131090	CAT-IDC-4BYTENET-AS-APCATTELECOMPublicCompanyLtdCATT	false
147.179.51.115	unknown	United States		12257	EMC-AS12257US	false
194.110.153.106	unknown	Russian Federation		57364	KMARUDA-ASRU	false
191.66.127.159	unknown	Colombia		26611	COMCELSACO	false
114.3.173.36	unknown	Indonesia		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.210.135.128	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	false
126.13.86.249	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
48.105.48.124	unknown	United States		2686	ATGS-MMD-ASUS	false
126.119.158.153	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
99.18.205.102	unknown	United States		7018	ATT-INTERNET4US	false
1.135.197.42	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
113.54.159.212	unknown	China		24355	CNGI-CD-IX-AS-APCERNET2IXatUniversityofElectronicScie	false
31.191.242.155	unknown	Italy		24608	WINDTRE-ASIT	false
82.74.104.213	unknown	Netherlands		33915	TNF-ASNL	false
172.96.116.60	unknown	United States		21859	ZNETUS	false
158.99.140.158	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
192.73.27.27	unknown	United States		1569	DNIC-ASBLK-01550-01601US	false
101.68.105.103	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
253.3.96.45	unknown	Reserved		unknown	unknown	false
54.104.203.186	unknown	United States		16509	AMAZON-02US	false
92.154.45.128	unknown	France		3215	FranceTelecom-OrangeFR	false
121.98.36.77	unknown	New Zealand		9790	VOCUSGROUPNZVocusGroupNZ	false
101.222.153.72	unknown	India		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
169.9.204.236	unknown	United States		203	CENTURYLINK-LEGACY-LVLT-203US	false
17.71.130.172	unknown	United States		714	APPLE-ENGINEERINGUS	false
243.251.148.233	unknown	Reserved		unknown	unknown	false
179.59.217.116	unknown	Bolivia		28024	NuevatelPCSdeBoliviaSABO	false
183.156.204.184	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
135.188.153.89	unknown	United States		14962	NCR-252US	false
23.198.151.244	unknown	United States		16625	AKAMAI-ASUS	false
205.190.14.132	unknown	United States		1239	SPRINTLINKUS	false
68.114.229.58	unknown	United States		20115	CHARTER-20115US	false
163.214.108.250	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
74.34.248.50	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
145.199.203.218	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
150.69.156.165	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
246.125.75.217	unknown	Reserved		unknown	unknown	false
169.82.172.59	unknown	United States		37611	AfrihostZA	false
195.223.214.33	unknown	Italy		3269	ASN-IBSNAZIT	false
70.13.65.109	unknown	United States		10507	SPCSUS	false
9.87.14.68	unknown	United States		3356	LEVEL3US	false
218.120.121.238	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
63.86.208.103	unknown	United States		701	UUNETUS	false
9.3.186.54	unknown	United States		3356	LEVEL3US	false
153.92.252.240	unknown	France		200484	SENDINBLUE-ASNFR	false
182.235.249.50	unknown	Taiwan; Republic of China (ROC)		9416	MULTIMEDIA-AS-APHoshinMultimediaCenterIncTW	false
31.92.237.234	unknown	United Kingdom		12576	EELtdGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
187.146.129.146	unknown	Mexico		8151	UninetSAdeCVMX	false
107.115.136.122	unknown	United States		7018	ATT-INTERNET4US	false
218.218.215.102	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
106.143.252.179	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
250.18.6.146	unknown	Reserved		unknown	unknown	false
8.228.87.35	unknown	United States		3356	LEVEL3US	false
247.238.11.84	unknown	Reserved		unknown	unknown	false
208.147.74.180	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
243.167.131.128	unknown	Reserved		unknown	unknown	false
14.212.146.48	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
19.193.194.127	unknown	United States		3	MIT-GATEWAYSUS	false
161.2.87.46	unknown	United Kingdom		15914	BritishAirwaysGB	false
68.225.43.93	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
206.243.250.156	unknown	United States		3356	LEVEL3US	false
58.217.149.0	unknown	China		134769	CHINANET-JIANGSU-CHANGZHOU-IDCChinaNetJiangsuChangzhouID	false
99.35.249.6	unknown	United States		7018	ATT-INTERNET4US	false
100.191.250.217	unknown	United States		21928	T-MOBILE-AS21928US	false
169.81.123.251	unknown	United States		37611	AfrihostZA	false
124.87.226.93	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
184.108.200.170	unknown	United States		7922	COMCAST-7922US	false
184.119.120.53	unknown	United States		7922	COMCAST-7922US	false
177.122.19.188	unknown	Brazil		26615	TIMSABR	false
123.246.197.174	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
57.255.57.243	unknown	Belgium		2686	ATGS-MMD-ASUS	false
60.3.74.81	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
9.170.63.8	unknown	United States		3356	LEVEL3US	false
65.32.152.106	unknown	United States		33363	BHN-33363US	false
178.130.18.68	unknown	Russian Federation		41691	SUMTEL-AS-RIPEMoscowRussiaRU	false
152.72.236.20	unknown	United States		21558	SC-JOHNSONUS	false
176.250.112.170	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
1.151.84.116	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
34.38.58.159	unknown	United States		2686	ATGS-MMD-ASUS	false
121.61.138.101	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
218.52.94.110	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
54.24.234.54	unknown	United States		14618	AMAZON-AESUS	false
250.122.249.195	unknown	Reserved		unknown	unknown	false
105.120.247.83	unknown	Nigeria		36873	VNL1-ASNG	false
213.69.38.204	unknown	Germany		702	UUNETUS	false
209.181.93.110	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
114.240.125.107	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (GNU/Linux), statically linked, no section header
Entropy (8bit):	7.925460713571166
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	z8lHAECIcU.elf
File size:	26'232 bytes
MD5:	b70c1e3b204c6b5b706f49347cb1f35a
SHA1:	3a05449966842a616b2903d7e405528ec64b4e19
SHA256:	7829c72ee62b574dbba327de3a60b4063b31851c858327b1eeb05a9740e30456
SHA512:	f04ca1d58d59f76a87d044338dd568b1e7473d650006c42a20bb91781ee41a2c3cacb690700cbe04f209a6e374a8d2bcb4c9d592ba63c6c6936d177b04841f70
SSDEEP:	384:ZWez9/6Jgn9yMGEGHV4u/DT8HgPEt6seDYc/OPM4uVcqgw05VxJc0j:AG959yM0HWubJsWDYcGk4uVcqgw09S0j
TLSH:	E4C2E191E1B62E96FB766E505A75C2C177B00E9EB777CDD2254CAF0808A321B47057CC
File Content Preview:	.ELF.....S....4.....4. ...(.....e...e.....L...L...L.....dt.Q.....UPX!.....T.....?.E.h4...@b.....i.&...Us..S?.....{.u....b.. .O.dR...'.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x105398

ELF header	
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x6580	0x6580	7.9290	0x5	R E	0x10000		
LOAD	0xfb4c	0x1001fb4c	0x1001fb4c	0x0	0x0	0.0000	0x6	RW	0x10000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

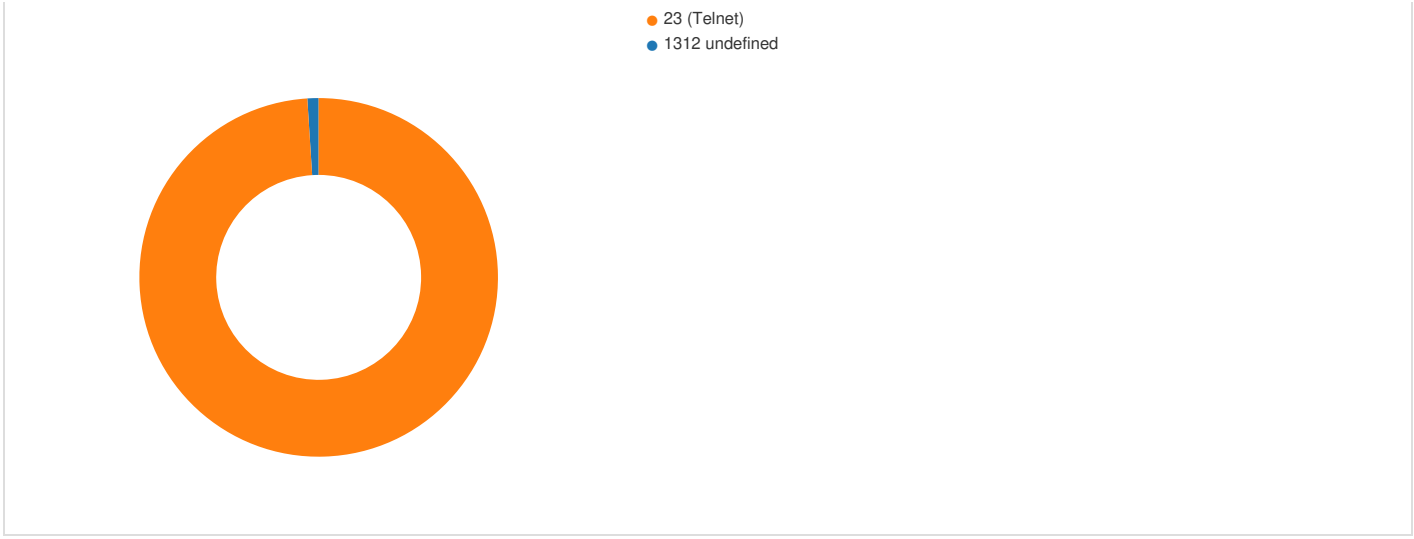
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.1489.213.31.12140526232829347 01/30/24-00:09:17.253981	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	40526	23	192.168.2.14	89.213.31.121
192.168.2.14178.163.132.14338860232829347 01/30/24-00:08:46.579114	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	38860	23	192.168.2.14	178.163.132.143
192.168.2.14121.120.101.140538232829347 01/30/24-00:09:06.090881	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	40538	23	192.168.2.14	121.120.101.1
192.168.2.13186.39.129.456244232829347 01/30/24-00:08:32.204233	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	56244	23	192.168.2.13	186.39.129.4
192.168.2.14187.168.4.7039762232023443 01/30/24-00:08:47.045048	TCP	2023443	ET TROJAN Possible Linux.Mirai Login Attempt (klv123)	39762	23	192.168.2.14	187.168.4.70
192.168.2.14171.34.207.1247532232829347 01/30/24-00:09:06.318964	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	47532	23	192.168.2.14	171.34.207.12
192.168.2.13201.176.27.8736480232829347 01/30/24-00:07:53.255345	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	36480	23	192.168.2.13	201.176.27.87
192.168.2.1437.98.227.16349802232829347 01/30/24-00:08:57.073420	TCP	2829347	ETPRO EXPLOIT Master IP CAM 01 Hardcoded Password for Root Account (CVE-2018-5723)	49802	23	192.168.2.14	37.98.227.163

Network Port Distribution

Total Packets: 99



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 30, 2024 00:08:38.346493959 CET	192.168.2.14	1.1.1.1	0xf4d9	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)	false
Jan 30, 2024 00:08:38.346534014 CET	192.168.2.14	1.1.1.1	0xf83d	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 30, 2024 00:08:38.465751886 CET	1.1.1.1	192.168.2.14	0xf4d9	No error (0)	daisy.ubuntu.com		162.213.35.25	A (IP address)	IN (0x0001)	false
Jan 30, 2024 00:08:38.465751886 CET	1.1.1.1	192.168.2.14	0xf4d9	No error (0)	daisy.ubuntu.com		162.213.35.24	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: z8lHAECIcU.elf PID: **5487**, Parent PID: **5410**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	/tmp/z8lHAECIcU.elf
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: z8lHAECIcU.elf PID: **5489**, Parent PID: **5487**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes

MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: z8lHAECIcU.elf PID: **5606**, Parent PID: **5489**

General

Start time (UTC):	23:08:34
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5608**, Parent PID: **5489**

General

Start time (UTC):	23:08:34
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5610**, Parent PID: **5608**

General

Start time (UTC):	23:08:34
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5627**, Parent PID: **5610**

General

Start time (UTC):	23:08:39
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5628**, Parent PID: **5610**

General

Start time (UTC):	23:08:39
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5611**, Parent PID: **5608**

General

Start time (UTC):	23:08:34

Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5614**, Parent PID: **5608**

General

Start time (UTC):	23:08:34
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5491**, Parent PID: **5487**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5493**, Parent PID: **5487**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5495**, Parent PID: **5493**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: z8lHAECIcU.elf PID: **5602**, Parent PID: **5495**

General

Start time (UTC):	23:08:34
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5604**, Parent PID: **5495**

General

Start time (UTC):	23:08:34
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5497**, Parent PID: **5493**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: z8lHAECIcU.elf PID: **5498**, Parent PID: **5493**

General

Start time (UTC):	23:05:51
Start date (UTC):	29/01/2024
Path:	/tmp/z8lHAECIcU.elf
Arguments:	-
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6