JoeSandbox Cloud BASIC

ID: 1532894
Sample Name: arm6.nn-20241014-0317.elf
Cookbook: defaultlinuxfilecookbook.jbs
Time: 05:18:12
Date: 14/10/2024
Version: 41.0.0 Charoite

Table of Contents

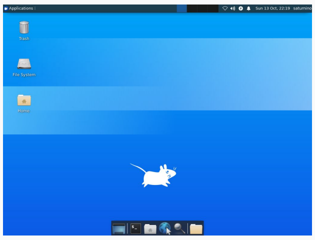
Linux Analysis Report

arm6.nn-20241014-0317.elf

Overview

General Information

Sample name:	arm6.nn-20241014-0317.elf
Analysis ID:	1532894
MD5:	34d5e2386084..
SHA1:	393adfe7a0fd6..
SHA256:	55bce839ded9...
Tags:	user-elfdigest
Infos:	YARA



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

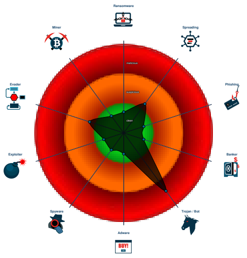
Mirai, Okiru

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for subm...
- Yara detected Mirai
- Yara detected Okiru
- Found strings indicative of a multi-p...
- Sample contains strings indicative o...
- Sample has stripped symbol table
- Tries to connect to HTTP servers, b...
- Uses the "uname" system call to qu...

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1532894
Start date and time:	2024-10-14 05:18:12 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 38s
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:	arm6.nn-20241014-0317.elf
Detection:	MAL
Classification:	mal72.troj.linELF@0/0@2/0

Runtime Messages

Command:	/tmp/arm6.nn-20241014-0317.elf
PID:	5512
Exit Code:	139
Exit Code Info:	SIGSEGV (11) Segmentation fault invalid memory reference
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 11 (Segmentation fault) - core dumped

Process Tree

- **system is lnxubuntu20**

- arm6.nn-20241014-0317.elf (PID: 5512, Parent: 5435, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm6.nn-20241014-0317.elf
- **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

Initial Sample

Source	Rule	Description	Author	Strings
arm6.nn-20241014-0317.elf	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	
arm6.nn-20241014-0317.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5512.1.00007f63a4017000.00007f63a4032000.r-x.sdmp	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	
5512.1.00007f63a4017000.00007f63a4032000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Process Memory Space: arm6.nn-20241014-0317.elf PID: 5512	JoeSecurity_Okiru	Yara detected Okiru	Joe Security	

Suricata Signatures

⊘ **No Suricata rule has matched**

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample ▼

Multi AV Scanner detection for submitted file ▼

Stealing of Sensitive Information

Yara detected Mirai ▼

Yara detected Okiru ▼

Remote Access Functionality

Yara detected Mirai ▼

Yara detected Okiru ▼

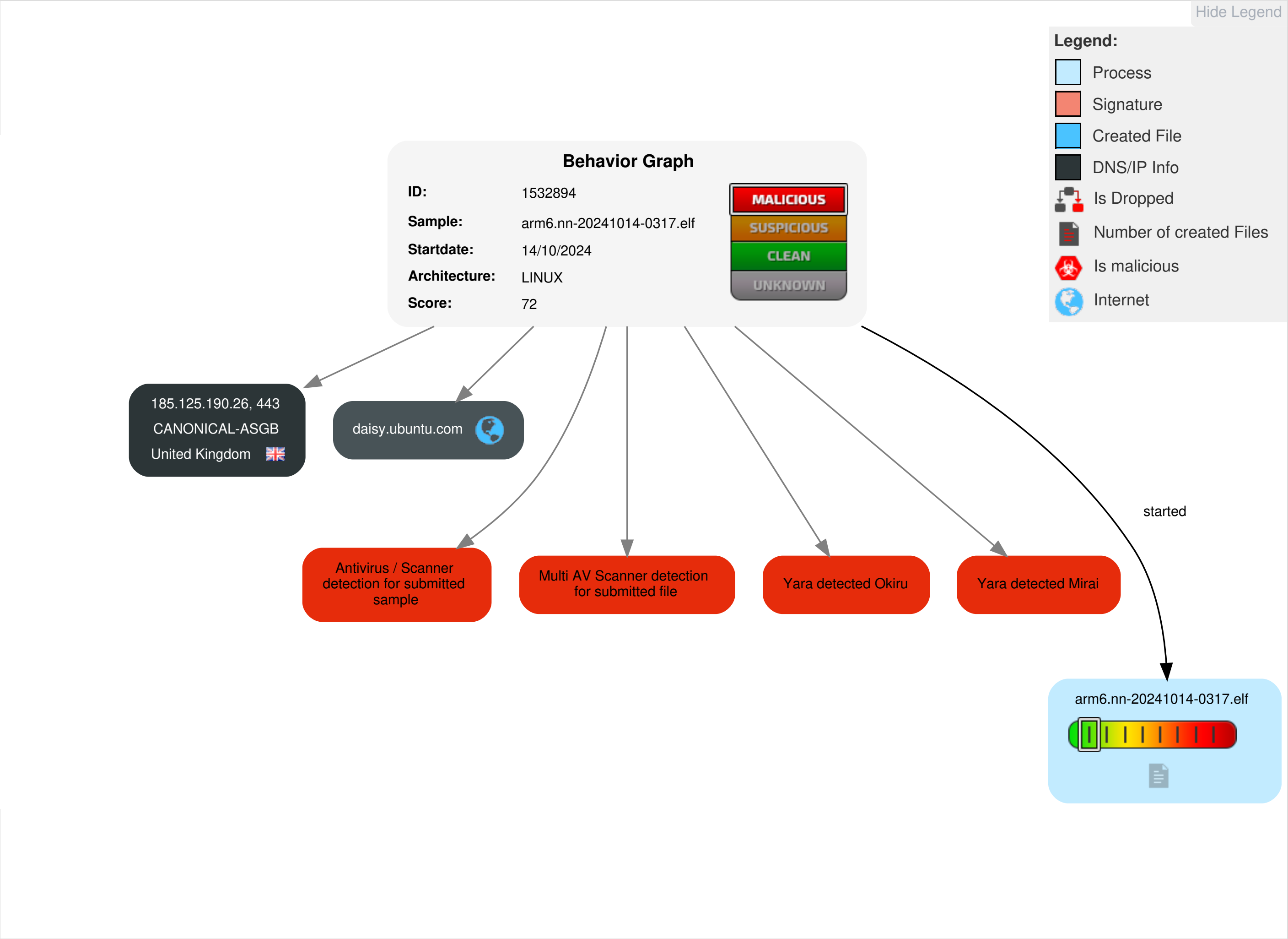
Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	1 Scripting	Valid Accounts	Windows Management Instrumentation	1 Scripting	Path Interception	Direct Volume Access	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 Non-Application Layer Protocol	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	2 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact

Malware Configuration

⊘ **No configs have been found**

Behavior Graph



Behavior Graph

ID: 1532894

Sample: arm6.nn-20241014-0317.elf

Startdate: 14/10/2024

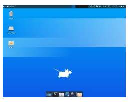
Architecture: LINUX

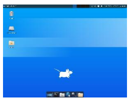
Score: 72

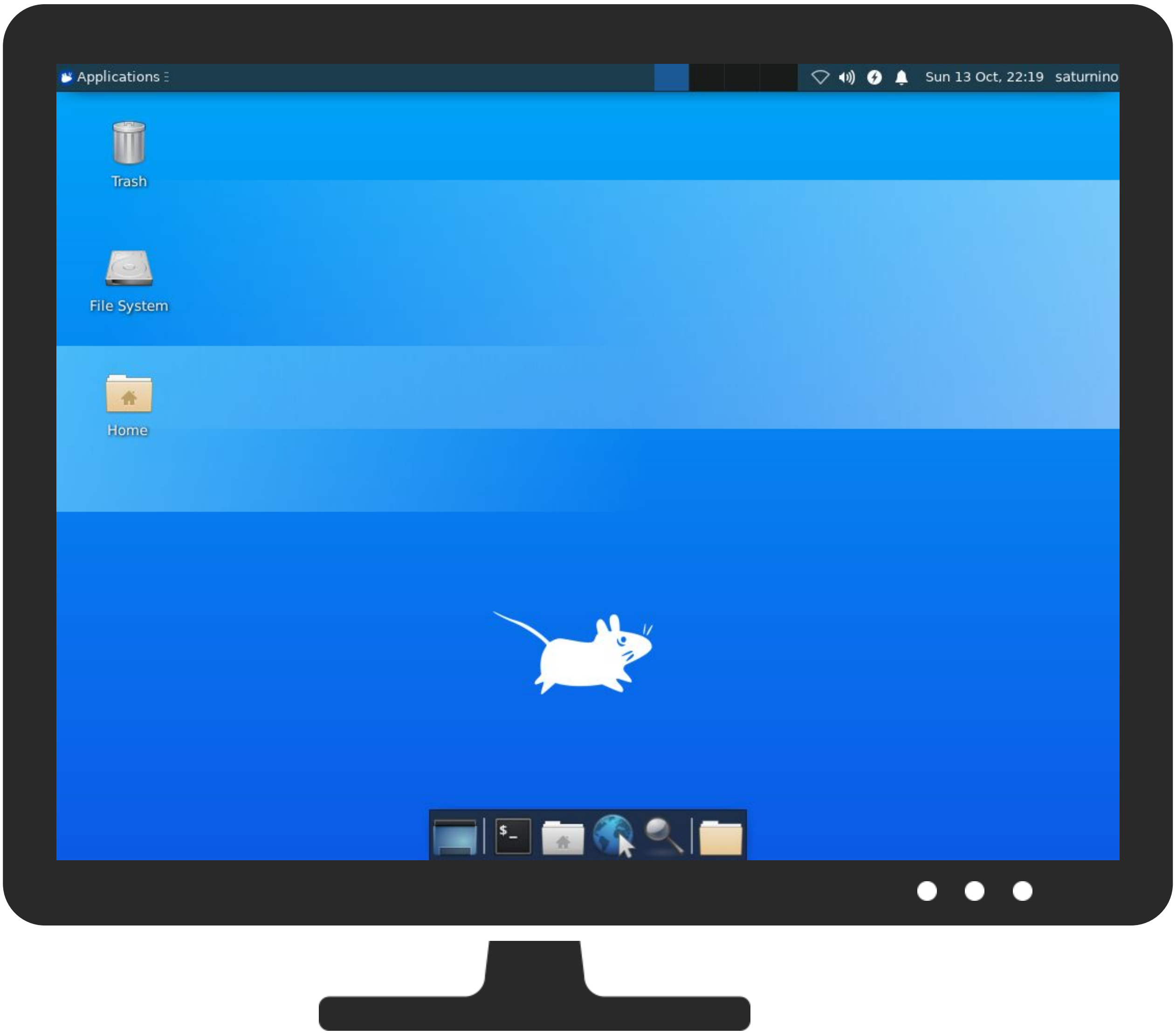
Screenshots

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
arm6.nn-20241014-0317.elf	45%	ReversingLabs	Linux.Backdoor.Mirai	
arm6.nn-20241014-0317.elf	100%	Avira	EXP/ELF.Mirai.W	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
daisy.ubuntu.com	0%	Virustotal		Browse

URLs

No Antivirus matches

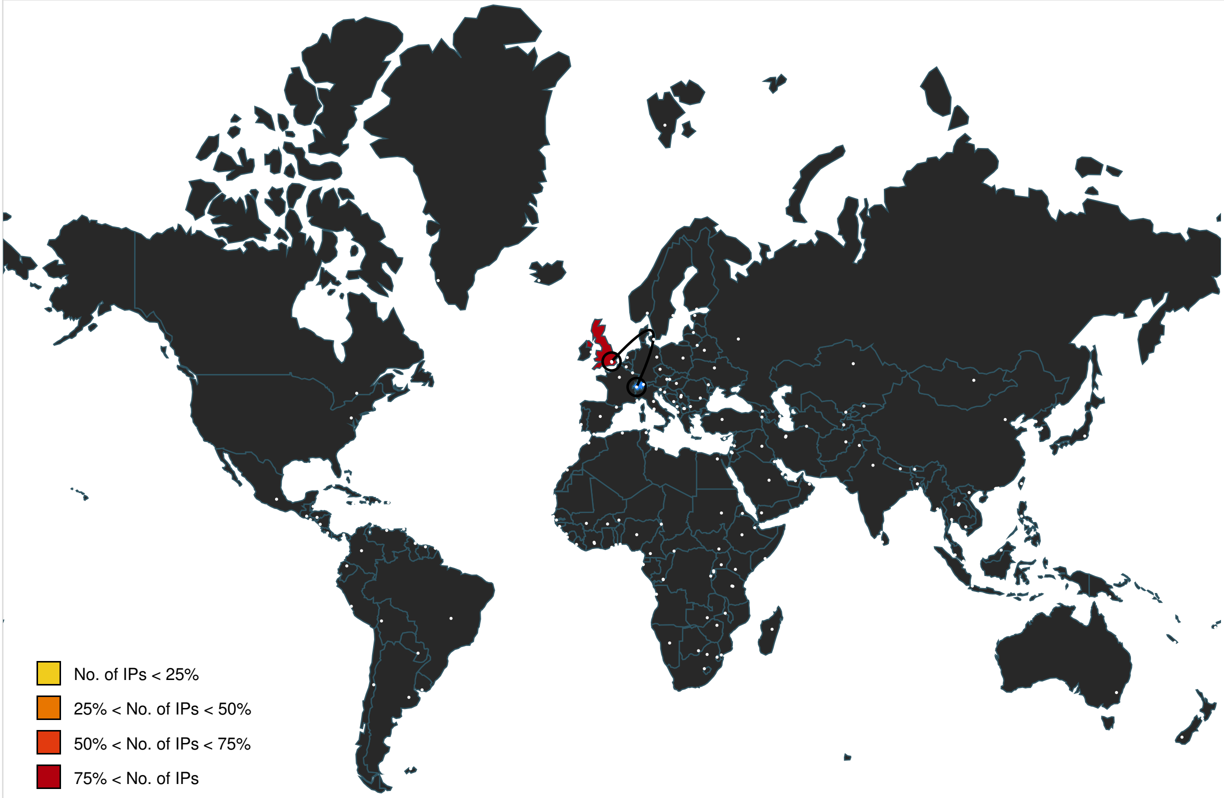
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.35.25	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.125.190.26	unknown	United Kingdom	🇬🇧	41231	CANONICAL-ASGB	false

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.160322098706338
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm6.nn-20241014-0317.elf
File size:	112'692 bytes
MD5:	34d5e238608444ac45291803bf143825
SHA1:	393adfe7a0fd6287b19e1fa7ee82a17a7cefe598
SHA256:	55bce839ded928cdf0a87339ae335aa9efbdd0e6928c949f4916cd7a7ab9b2ff
SHA512:	51aaaad3fe50a9c3b63df286e0f9620bedeea2f3486e7ba527dfaa57297d89edd1236912f0012e94d6ad890176db293da5bfbefb5391fb9f4821a862ae5e521b
SSDEEP:	3072:qgg82i5pRl/nKKoe76aXxm6tN5vCPL4nqlL:qgg0mPemaBmuGPN
TLSH:	CDB32B47B881DB12C5C516BEF91E018D331317B8D3DF72169D14AF247B8A96B0E3BA45
File Content Preview:	.ELF..............(.....T...4...T.......4. ...(...,...........Q.td...................................-...L..................@-.,@...0....S..... 0....S.........../..0...0...@..../...............-.@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:	0x8154
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	112212
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x174c8	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1f578	0x17578	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1f588	0x17588	0x3388	0x0	0x2	A	0	0	8
.init_array	INIT_ARRAY	0x2b004	0x1b008	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x2b008	0x1b00c	0x4	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x2b010	0x1b014	0x7c	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x2b08c	0x1b090	0x554	0x0	0x3	WA	0	0	4

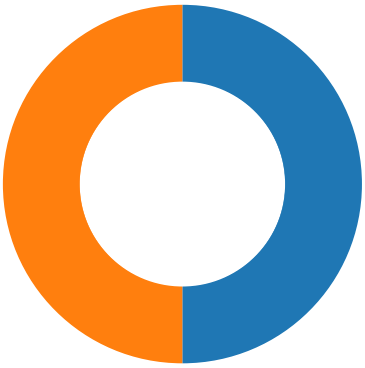
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.bss	NOBITS	0x2b5e0	0x1b5e4	0x2550	0x0	0x3	WA	0	0	4
.ARM.attributes	ARM_ATTRIBUTES	0x0	0x1b5e4	0x10	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x1b5f4	0x5d	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x1a910	0x1a910	6.2178	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x1b004	0x2b004	0x2b000	0x5e0	0xab2c	5.6462	0x6	RW	0x8000		.init_array .fini_array .got .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



Total Packets: 4

- ● 53 (DNS)
- ● 443 (HTTPS)

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 14, 2024 05:19:00.318769932 CEST	192.168.2.14	1.1.1.1	0x279f	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)	false
Oct 14, 2024 05:19:00.318769932 CEST	192.168.2.14	1.1.1.1	0x2c91	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
Oct 14, 2024 05:19:00.327035904 CEST	1.1.1.1	192.168.2.14	0x279f	No error (0)	daisy.ubuntu.com		162.213.35.25	A (IP address)	IN (0x0001)	false
Oct 14, 2024 05:19:00.327035904 CEST	1.1.1.1	192.168.2.14	0x279f	No error (0)	daisy.ubuntu.com		162.213.35.24	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: arm6.nn-20241014-0317.elf

PID: **5512**, Parent PID: **5435**

General

Start time (UTC):	03:18:58
Start date (UTC):	14/10/2024
Path:	/tmp/arm6.nn-20241014-0317.elf
Arguments:	/tmp/arm6.nn-20241014-0317.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read ▼