ID: 553497
Sample Name:
UnHAnaAW.arm5
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:55:11
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

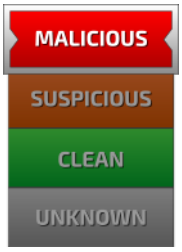
Linux Analysis Report UnHAnaAW.arm5

Overview

General Information

Sample Name:	UnHAnaAW.arm5
Analysis ID:	553497
MD5:	1ab9ba9183a1cfc..
SHA1:	0f89abb25355402.
SHA256:	0e96c432e77949..
Infos:	

Detection

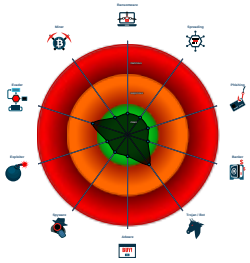


Score:	48
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Sample has stripped symbol table

Classification



Analysis Advice

- **Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures**
- **All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work**
- **Non-zero exit code suggests an error during the execution. Lookup the error code for hints.**
- **Static ELF header machine description suggests that the sample might not execute correctly on this machine**

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553497
Start date:	15.01.2022
Start time:	02:55:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UnHAnaAW.arm5
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:	mal48.linARM5@0/0@0/0

Process Tree

- **system is lnxubuntu20**
  - UnHAnaAW.arm5 (PID: 5200, Parent: 5114, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/UnHAnaAW.arm5
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

- AV Detection
- Networking
- System Summary
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

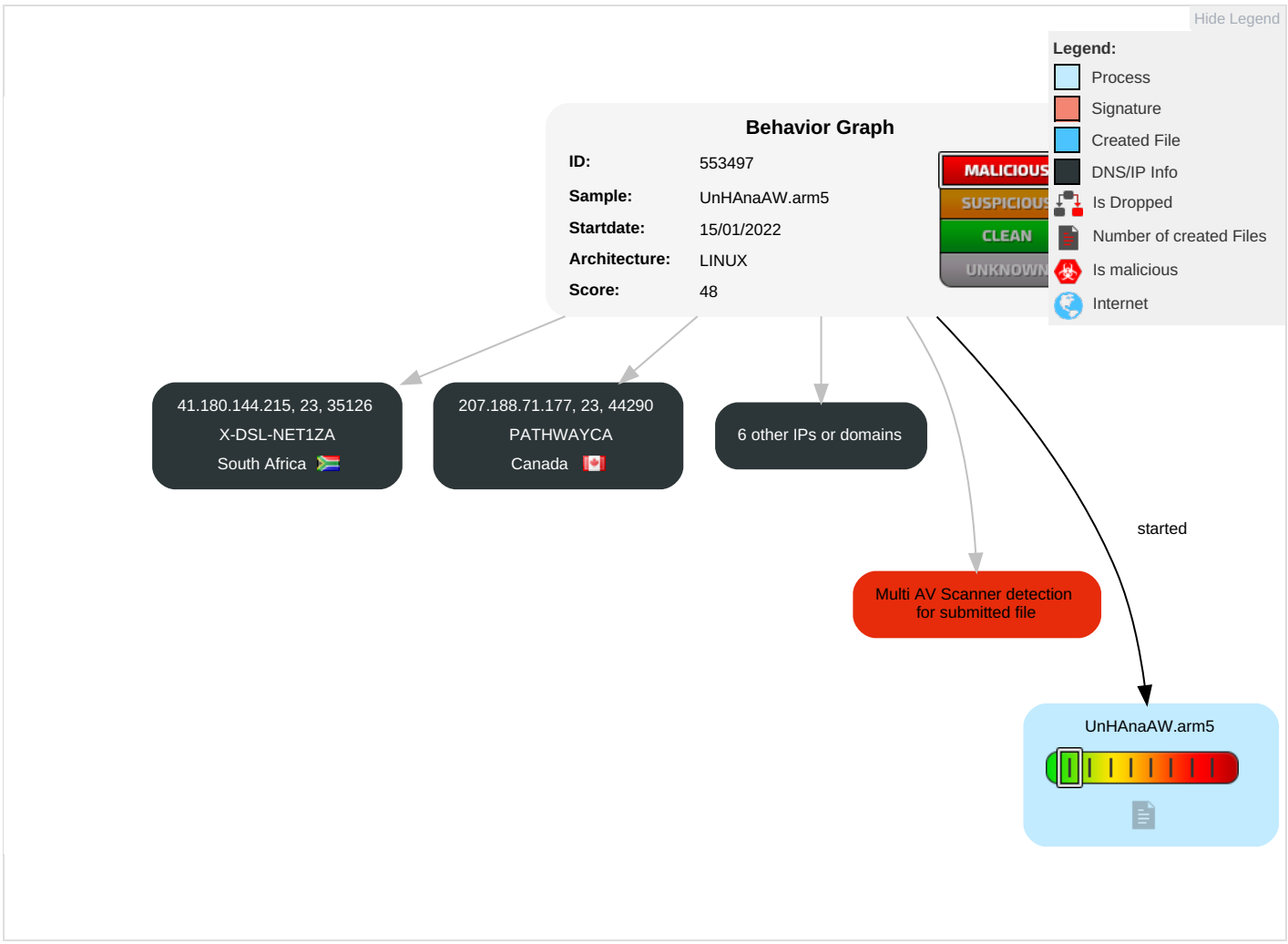
Mitre Att&ck Matrix

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	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	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	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
UnHAnaAW.arm5	49%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.188.71.177	unknown	Canada		11342	PATHWAYCA	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
207.134.109.11	unknown	Canada		852	ASN852CA	false
197.234.233.181	unknown	South Africa		37546	MIA-TELECOMsZA	false
41.180.144.215	unknown	South Africa		36916	X-DSL-NET1ZA	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
121.131.157.253	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/UnHAnaAW.arm5
Exit Code:	255
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	/lib/ld-uClibc.so.0: No such file or directory

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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, version 1 (ARM), dynamically linked, interpreter /lib/ld-uClibc.so.0, stripped
Entropy (8bit):	5.94982589822901

General

TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	UnHAnaAW.arm5
File size:	66800
MD5:	1ab9ba9183a1cfc793e53d95c053a94f
SHA1:	0f89abb2535540236747f7509c00e7730805132b
SHA256:	0e96c432e77949a73df5b0b52a741ce1d10e74aa5b2e707345dfd577d07a96c
SHA512:	005a5516047e719e70278945aec4a17cd0ba536551e89251d466dd513c3aa5ac4977a1565cc751baa224fee267aa6481f9dce5463260c8f8eede07243952e569
SSDEEP:	1536:8nv4uuJp2KtGn9bJlRwl5aSXPACkA60erlTny4N6Fnydoh+WFy7BKeK:8n4l+BT3MpyahpSY
File Content Preview:	.ELF...a.....(.....4... .....4. ...(.....4...4...4.....4...4.....H.....Q.td...../lib/ld-uCl

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:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8ee8
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	6
Section Header Offset:	66080
Section Header Size:	40
Number of Section Headers:	18
Header String Table Index:	17

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.interp	PROGBITS	0x80f4	0xf4	0x14	0x0	0x2	A	0	0	1
.hash	HASH	0x8108	0x108	0x22c	0x4	0x2	A	3	0	4
.dynsym	DYNSYM	0x8334	0x334	0x460	0x10	0x2	A	4	1	4
.dynstr	STRTAB	0x8794	0x794	0x237	0x0	0x2	A	0	0	1
.rel.plt	REL	0x89cc	0x9cc	0x1a0	0x8	0x2	A	3	7	4
.init	PROGBITS	0x8b6c	0xb6c	0x18	0x0	0x6	AX	0	0	4
.plt	PROGBITS	0x8b84	0xb84	0x284	0x4	0x6	AX	0	0	4
.text	PROGBITS	0x8e08	0xe08	0xe6e8	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x174f0	0xf4f0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x17504	0xf504	0xa30	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x18000	0x10000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x18008	0x10008	0x8	0x0	0x3	WA	0	0	4
.dynamic	DYNAMIC	0x18014	0x10014	0x98	0x8	0x3	WA	4	0	4
.got	PROGBITS	0x180ac	0x100ac	0xdc	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x18188	0x10188	0x24	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x181ac	0x101ac	0x19c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x101ac	0x73	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
PHDR	0x34	0x8034	0x8034	0xc0	0xc0	1.4521	0x5	R E	0x4		
INTERP	0xf4	0x80f4	0x80f4	0x14	0x14	3.6842	0x4	R	0x1	/lib/ld-uClibc.so.0	.interp
LOAD	0x0	0x8000	0x8000	0xff34	0xff34	3.1002	0x5	R E	0x8000		.interp .hash .dynsym .dynstr .rel.plt .init .plt .text .fini .rodata
LOAD	0x10000	0x18000	0x18000	0x1ac	0x348	1.0335	0x6	RW	0x8000		.ctors .dtors .dynamic .got .data .bss
DYNAMIC	0x10014	0x18014	0x18014	0x98	0x98	1.4001	0x6	RW	0x4		.dynamic
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Dynamic Tags

Type	Meta	Value	Tag
DT_NEEDED	sharedlib	libc.so.0	0x1
DT_INIT	value	0x8b6c	0xc
DT_FINI	value	0x174f0	0xd
DT_HASH	value	0x8108	0x4
DT_STRTAB	value	0x8794	0x5
DT_SYMTAB	value	0x8334	0x6
DT_STRSZ	bytes	567	0xa
DT_SYMENT	bytes	16	0xb
DT_DEBUG	value	0x0	0x15
DT_PLTGOT	value	0x180ac	0x3
DT_PLTRELSZ	bytes	416	0x2
DT_PLTREL	pltrel	DT_REL	0x14
DT_JMPREL	value	0x89cc	0x17
DT_NULL	value	0x0	0x0

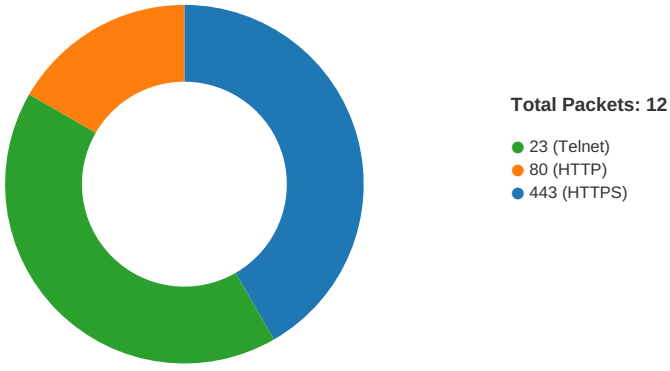
Symbols

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
			.dynsym	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__aeabi_idiv0			.dynsym	0x174b0	4	FUNC	<unknown>	DEFAULT	8
__aeabi_ldiv0			.dynsym	0x174b0	4	FUNC	<unknown>	DEFAULT	8
__aeabi_uidiv			.dynsym	0x171f0	0	FUNC	<unknown>	DEFAULT	8
__aeabi_uidivmod			.dynsym	0x172e8	24	FUNC	<unknown>	DEFAULT	8
__bss_end__			.dynsym	0x18348	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__bss_start			.dynsym	0x181ac	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__bss_start__			.dynsym	0x181ac	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__data_start			.dynsym	0x18188	0	NOTYPE	<unknown>	DEFAULT	17
__div0			.dynsym	0x174b0	4	FUNC	<unknown>	DEFAULT	8
__end__			.dynsym	0x18348	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__errno_location			.dynsym	0x8d78	32	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__modsi3			.dynsym	0x173cc	228	FUNC	<unknown>	DEFAULT	8
__uClibc_main			.dynsym	0x8d30	488	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__udivsi3			.dynsym	0x171f0	248	FUNC	<unknown>	DEFAULT	8
__umodsi3			.dynsym	0x17300	204	FUNC	<unknown>	DEFAULT	8
_bss_end__			.dynsym	0x18348	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_edata			.dynsym	0x181ac	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_end			.dynsym	0x18348	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
_start			.dynsym	0x8ee8	80	FUNC	<unknown>	DEFAULT	8
abort			.dynsym	0x8c70	352	FUNC	<unknown>	DEFAULT	SHN_UNDEF
accept			.dynsym	0x8c7c	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
atoi			.dynsym	0x8d90	12	FUNC	<unknown>	DEFAULT	SHN_UNDEF
bind			.dynsym	0x8cac	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
calloc			.dynsym	0x8c88	88	FUNC	<unknown>	DEFAULT	SHN_UNDEF
clock			.dynsym	0x8da8	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
close			.dynsym	0x8dd8	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
closedir			.dynsym	0x8dc0	196	FUNC	<unknown>	DEFAULT	SHN_UNDEF
connect			.dynsym	0x8bbc	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
exit			.dynsym	0x8d84	172	FUNC	<unknown>	DEFAULT	SHN_UNDEF
fcntl			.dynsym	0x8dcc	116	FUNC	<unknown>	DEFAULT	SHN_UNDEF
fork			.dynsym	0x8d24	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
free			.dynsym	0x8de4	288	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getpid			.dynsym	0x8be0	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
getppid			.dynsym	0x8d48	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getsockname			.dynsym	0x8dfc	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getsockopt			.dynsym	0x8d6c	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
inet_addr			.dynsym	0x8cb8	36	FUNC	<unknown>	DEFAULT	SHN_UNDEF
ioctl			.dynsym	0x8ba4	80	FUNC	<unknown>	DEFAULT	SHN_UNDEF
kill			.dynsym	0x8ca0	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
listen			.dynsym	0x8d18	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
malloc			.dynsym	0x8c10	400	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memcpy			.dynsym	0x8bf8	4	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memmove			.dynsym	0x8bd4	4	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memset			.dynsym	0x8d3c	156	FUNC	<unknown>	DEFAULT	SHN_UNDEF
open			.dynsym	0x8d9c	92	FUNC	<unknown>	DEFAULT	SHN_UNDEF
opendir			.dynsym	0x8d60	264	FUNC	<unknown>	DEFAULT	SHN_UNDEF
prctl			.dynsym	0x8bec	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
rand			.dynsym	0x8cd0	4	FUNC	<unknown>	DEFAULT	SHN_UNDEF
read			.dynsym	0x8ce8	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
readdir			.dynsym	0x8c4c	224	FUNC	<unknown>	DEFAULT	SHN_UNDEF
readlink			.dynsym	0x8c04	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
realloc			.dynsym	0x8d0c	312	FUNC	<unknown>	DEFAULT	SHN_UNDEF
recv			.dynsym	0x8bb0	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
recvfrom			.dynsym	0x8c28	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
select			.dynsym	0x8c40	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
send			.dynsym	0x8c64	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sendto			.dynsym	0x8d00	52	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsid			.dynsym	0x8db4	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsockopt			.dynsym	0x8cc4	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sigaddset			.dynsym	0x8c58	48	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sigemptyset			.dynsym	0x8bc8	24	FUNC	<unknown>	DEFAULT	SHN_UNDEF
signal			.dynsym	0x8cdc	200	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sigprocmask			.dynsym	0x8df0	84	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sleep			.dynsym	0x8c1c	420	FUNC	<unknown>	DEFAULT	SHN_UNDEF
socket			.dynsym	0x8c34	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strcpy			.dynsym	0x8b98	28	FUNC	<unknown>	DEFAULT	SHN_UNDEF
time			.dynsym	0x8d54	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
unlink			.dynsym	0x8cf4	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF
write			.dynsym	0x8c94	44	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: UnHAnaAW.arm5 PID: 5200 Parent PID: 5114

General

Start time:	02:55:49
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.arm5
Arguments:	/tmp/UnHAnaAW.arm5
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read