ID: 528752
Sample Name: ND41FX6xbB
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 18:33:14
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

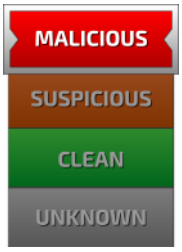
Linux Analysis Report ND41FX6xbB

Overview

General Information

Sample Name:	ND41FX6xbB
Analysis ID:	528752
MD5:	12043cc1462a78..
SHA1:	e4130164d83e59..
SHA256:	f1a4ed45d580688.
Tags:	32 arm elf mirai
Infos:	

Detection

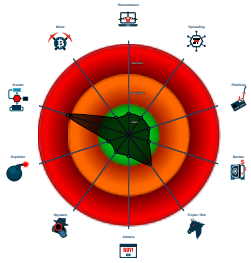


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…

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**
- **Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture**

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528752
Start date:	25.11.2021
Start time:	18:33:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ND41FX6xbB
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:	mal52.evad.lin@0/0@0/0

Process Tree

- **system is lnxubuntu20**
  - ND41FX6xbB (PID: 5220, Parent: 5105, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/ND41FX6xbB
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ND41FX6xbB	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0xce24:$s1: PROT_EXEC\|PROT_WRITE failed. • 0xce93:$s2: $Id: UPX • 0xce44:$s3: $Info: This file is packed with the UPX executable packer

Jbx Signature Overview

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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Sample is packed with UPX

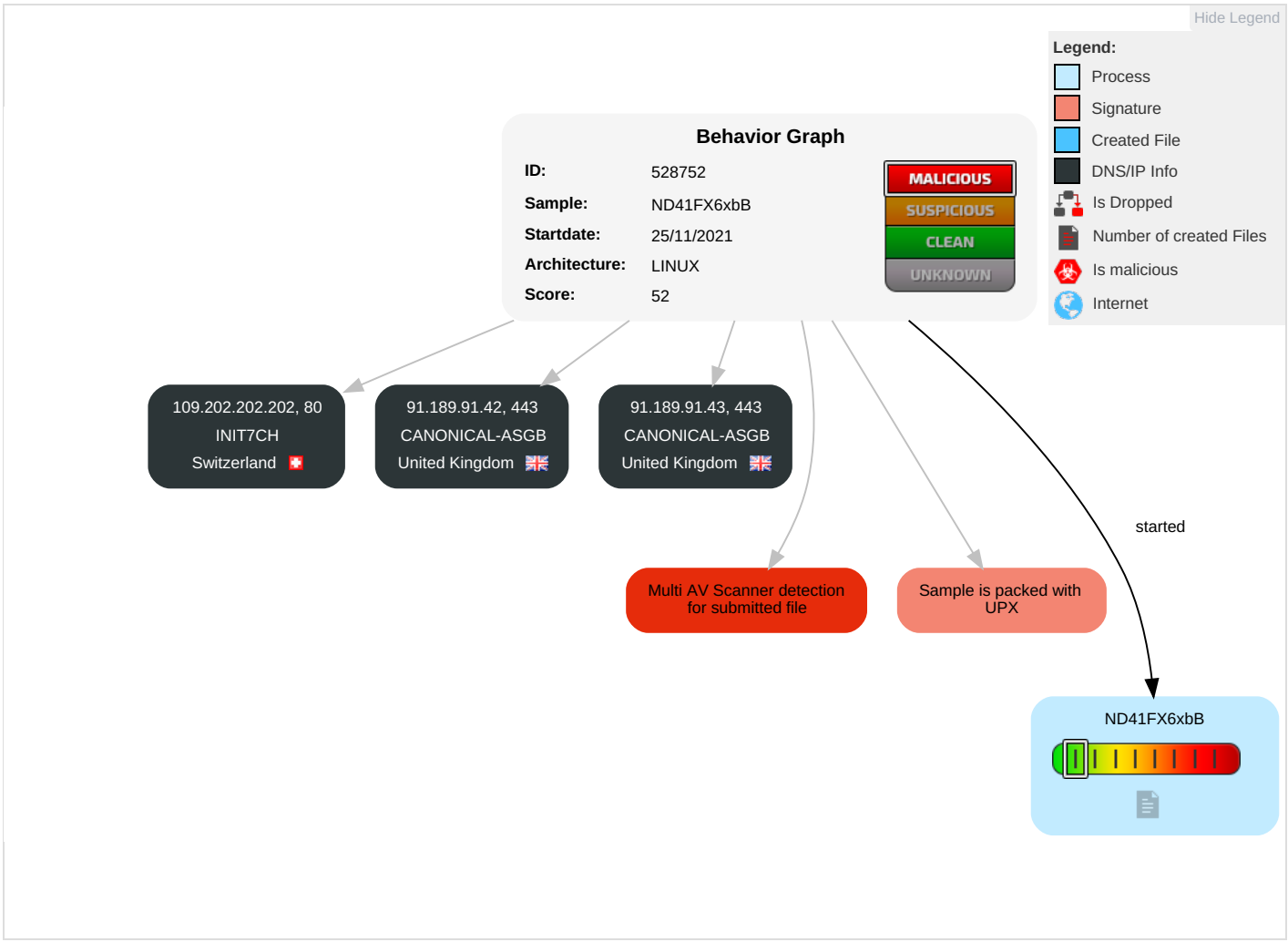
Mitre Att&ck Matrix

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	Obfuscated Files or Information 1	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
ND41FX6xbB	30%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/ND41FX6xbB
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

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
109.202.202.202	rY6NBuBYiv	Get hash	malicious	Browse	
	DZhVesq972	Get hash	malicious	Browse	
	nOQliIST3n	Get hash	malicious	Browse	
	Ar71Zq4WOl	Get hash	malicious	Browse	
	i.5.8.6	Get hash	malicious	Browse	
	x.8.6	Get hash	malicious	Browse	
	Nkl22sQjFw	Get hash	malicious	Browse	
	m.i.p.s	Get hash	malicious	Browse	
	uKc673FWAM	Get hash	malicious	Browse	
	A7ZUziZ5jx	Get hash	malicious	Browse	
	jTVzI4fJDk	Get hash	malicious	Browse	
	OSGxiHdGIF	Get hash	malicious	Browse	
	a.r.m.v.7.l	Get hash	malicious	Browse	
	a.r.m.v.6.l	Get hash	malicious	Browse	
	m.i.p.s.e.l	Get hash	malicious	Browse	
	a.r.m.v.5.l	Get hash	malicious	Browse	
	a.r.m.v.4.l	Get hash	malicious	Browse	
	i.6.8.6	Get hash	malicious	Browse	
	2MzNonluPU	Get hash	malicious	Browse	
	EWUJrwD61l	Get hash	malicious	Browse	
91.189.91.43	rY6NBuBYiv	Get hash	malicious	Browse	
	DZhVesq972	Get hash	malicious	Browse	
	nOQliIST3n	Get hash	malicious	Browse	
	Ar71Zq4WOl	Get hash	malicious	Browse	
	i.5.8.6	Get hash	malicious	Browse	
	x.8.6	Get hash	malicious	Browse	
	Nkl22sQjFw	Get hash	malicious	Browse	
	m.i.p.s	Get hash	malicious	Browse	
	uKc673FWAM	Get hash	malicious	Browse	
	A7ZUziZ5jx	Get hash	malicious	Browse	
	jTVzI4fJDk	Get hash	malicious	Browse	
	OSGxiHdGIF	Get hash	malicious	Browse	
	a.r.m.v.7.l	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a.r.m.v.6.l	Get hash	malicious	Browse	
	m.i.p.s.e.l	Get hash	malicious	Browse	
	a.r.m.v.5.l	Get hash	malicious	Browse	
	a.r.m.v.4.l	Get hash	malicious	Browse	
	i.6.8.6	Get hash	malicious	Browse	
	2MzNonluPU	Get hash	malicious	Browse	
	EWUJrwD61l	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	rY6NBuBYiv	Get hash	malicious	Browse	• 91.189.91.42
	DZhVesq972	Get hash	malicious	Browse	• 91.189.91.42
	nOQliIST3n	Get hash	malicious	Browse	• 91.189.91.42
	Ar71Zq4WOl	Get hash	malicious	Browse	• 91.189.91.42
	i.5.8.6	Get hash	malicious	Browse	• 91.189.91.42
	x.8.6	Get hash	malicious	Browse	• 91.189.91.42
	Nkl22sQjFw	Get hash	malicious	Browse	• 91.189.91.42
	m.i.p.s	Get hash	malicious	Browse	• 91.189.91.42
	uKc673FWAM	Get hash	malicious	Browse	• 91.189.91.42
	A7ZUziZ5jx	Get hash	malicious	Browse	• 91.189.91.42
	jTVzI4fJDk	Get hash	malicious	Browse	• 91.189.91.42
	OSGxiHdGIF	Get hash	malicious	Browse	• 91.189.91.42
	a.r.m.v.7.l	Get hash	malicious	Browse	• 91.189.91.42
	a.r.m.v.6.l	Get hash	malicious	Browse	• 91.189.91.42
	m.i.p.s.e.l	Get hash	malicious	Browse	• 91.189.91.42
	a.r.m.v.5.l	Get hash	malicious	Browse	• 91.189.91.42
	a.r.m.v.4.l	Get hash	malicious	Browse	• 91.189.91.42
	i.6.8.6	Get hash	malicious	Browse	• 91.189.91.42
	2MzNonluPU	Get hash	malicious	Browse	• 91.189.91.42
	EWUJrwD61l	Get hash	malicious	Browse	• 91.189.91.42
INIT7CH	rY6NBuBYiv	Get hash	malicious	Browse	• 109.202.202.202
	DZhVesq972	Get hash	malicious	Browse	• 109.202.202.202
	nOQliIST3n	Get hash	malicious	Browse	• 109.202.202.202
	Ar71Zq4WOl	Get hash	malicious	Browse	• 109.202.202.202
	i.5.8.6	Get hash	malicious	Browse	• 109.202.202.202
	x.8.6	Get hash	malicious	Browse	• 109.202.202.202
	Nkl22sQjFw	Get hash	malicious	Browse	• 109.202.202.202
	m.i.p.s	Get hash	malicious	Browse	• 109.202.202.202
	uKc673FWAM	Get hash	malicious	Browse	• 109.202.202.202
	A7ZUziZ5jx	Get hash	malicious	Browse	• 109.202.202.202
	jTVzI4fJDk	Get hash	malicious	Browse	• 109.202.202.202
	OSGxiHdGIF	Get hash	malicious	Browse	• 109.202.202.202
	a.r.m.v.7.l	Get hash	malicious	Browse	• 109.202.202.202
	a.r.m.v.6.l	Get hash	malicious	Browse	• 109.202.202.202
	m.i.p.s.e.l	Get hash	malicious	Browse	• 109.202.202.202
	a.r.m.v.5.l	Get hash	malicious	Browse	• 109.202.202.202
	a.r.m.v.4.l	Get hash	malicious	Browse	• 109.202.202.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	i.6.8.6	Get hash	malicious	Browse	• 109.202.202.202
	2MzNonluPU	Get hash	malicious	Browse	• 109.202.202.202
	EWUJrwD61I	Get hash	malicious	Browse	• 109.202.202.202

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 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.981306555590721
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	ND41FX6xbB
File size:	54876
MD5:	12043cc1462a781e9ea20eb5eeb55e5e
SHA1:	e4130164d83e593541b6965e28c081bafa618ede
SHA256:	f1a4ed45d580688ed0acc2e7e0aabeb44ead0011661b9a1f51fdaaa8b64bb70f
SHA512:	3689790d6be15cfdaf4a6c6eeefeeaa1fb8d7f7edc08fb0e1142867dfafa7ed8c77488f63cdfc50d7d31e6ab2637179ff893c2a8835aa8bc2f9b0680feeb0c09
SSDEEP:	1536:5j/3kZTB21uJJ6aZpma9brpEaE//dpUmv1PnLq:2ZTksJ3+ad6aE//d2mdfLq
File Content Preview:	.ELF.....(.....0C..4.....4. ...(.....D...D...D.....Q.td.....sUPX!.....6...6.....T.....?.E.h;....#..$..1)....v{$\l.rV.i...+1E.....d..[.....S....w.4L1

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 - Linux
ABI Version:	0
Entry Point Address:	0x14330
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0

ELF header

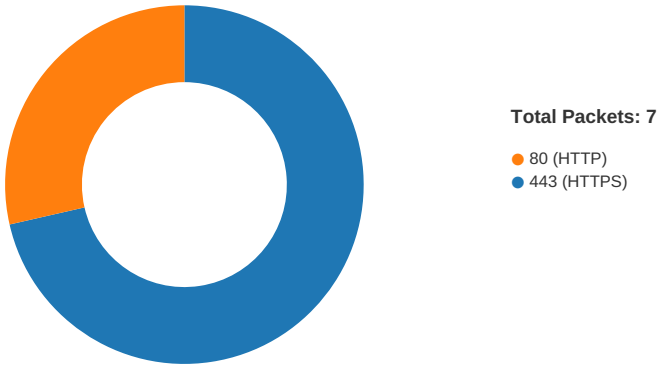
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0xd51d	0xd51d	4.0231	0x5	R E	0x8000		
LOAD	0x1c44	0x41c44	0x41c44	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: ND41FX6xbB PID: 5220 Parent PID: 5105

General

Start time:	18:34:00
Start date:	25/11/2021
Path:	/tmp/ND41FX6xbB
Arguments:	/tmp/ND41FX6xbB
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read