ID: 551039
Sample Name: bin.sh
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 18:58:52
Date: 11/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

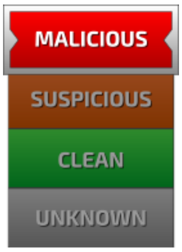
Linux Analysis Report bin.sh

Overview

General Information

Sample Name:	bin.sh
Analysis ID:	551039
MD5:	a73ddd6ec22462..
SHA1:	ac6962542a4b23..
SHA256:	b5cf68c7cb5bb2d..
Infos:	

Detection

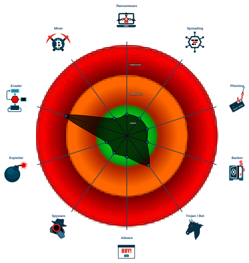


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- 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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551039
Start date:	11.01.2022
Start time:	18:58:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bin.sh
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:	mal60.evad.linSH@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - bin.sh (PID: 5223, Parent: 5120, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/bin.sh
- **cleanup**

Yara Overview

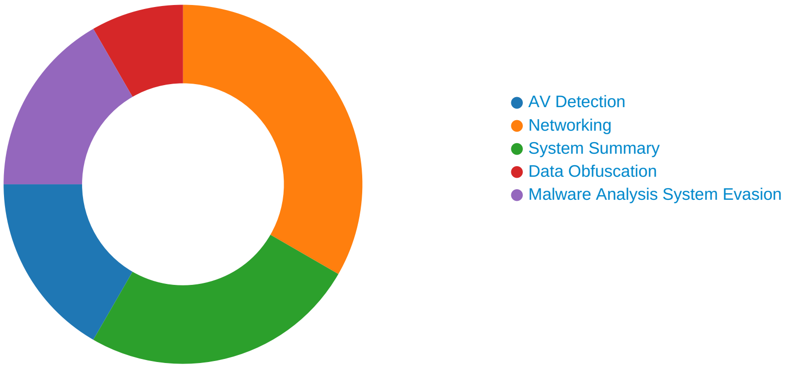
Initial Sample

Source	Rule	Description	Author	Strings
bin.sh	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x206f8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20767:$s2: $Id: UPX • 0x20718:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
5223.1.00000000b8716a1c.00000000a1a19d0b.r-x.sdmp	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x206f8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20767:$s2: $Id: UPX • 0x20718:$s3: $Info: This file is packed with the UPX executable packer

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Data Obfuscation:

Sample is packed with UPX

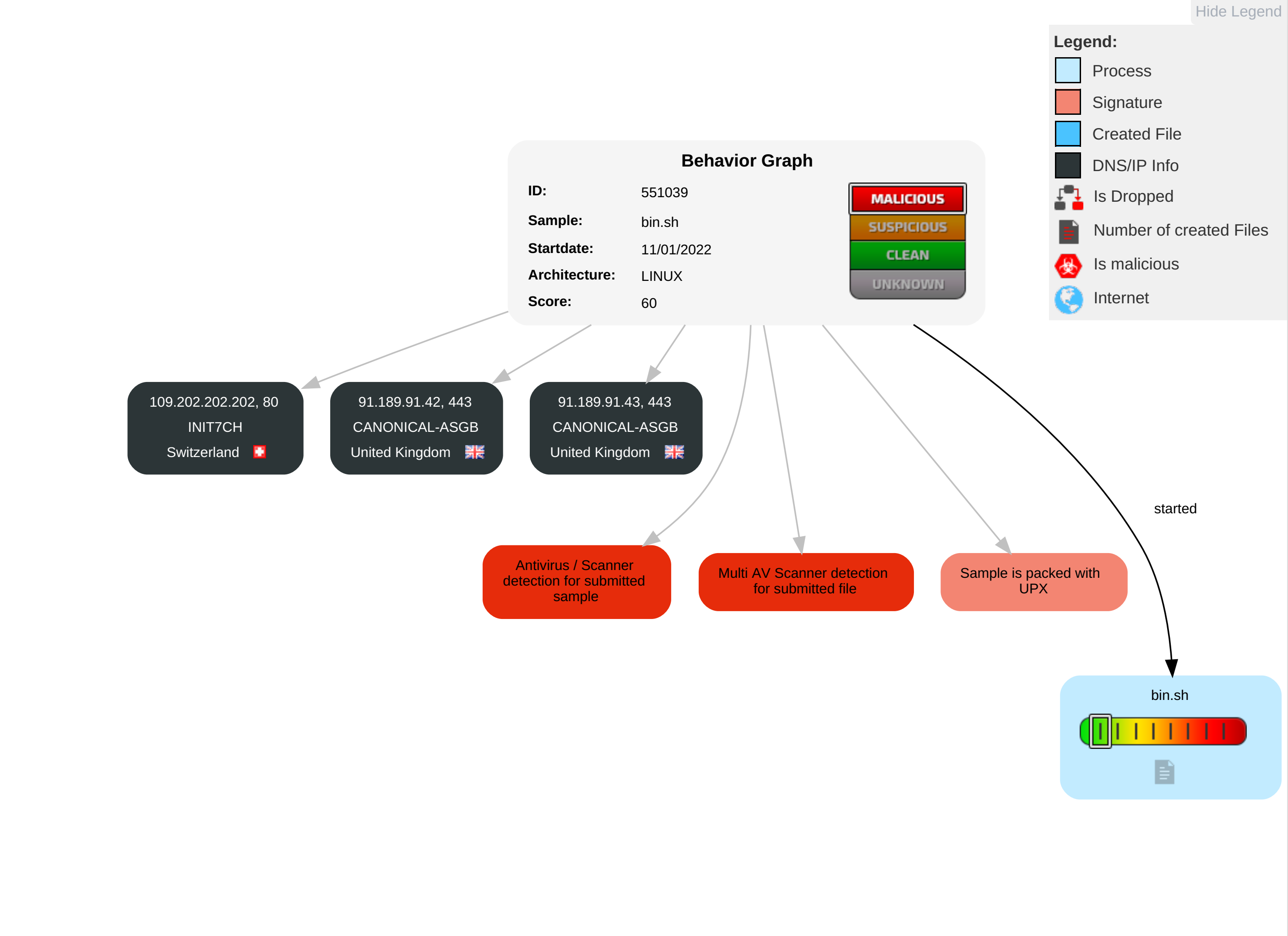
Mitre Att&ck Matrix

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
bin.sh	18%	Metadefender		Browse
bin.sh	79%	ReversingLabs	Linux.Trojan.Mirai	
bin.sh	100%	Avira	LINUX/Mirai.ccjqy	

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/bin.sh
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 5 (Trace/breakpoint trap) - core dumped

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 MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.813637944981102
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	bin.sh
File size:	135472
MD5:	a73ddd6ec22462db955439f665cad4e6
SHA1:	ac6962542a4b23ac13bddff22f8df9aeb702ef12
SHA256:	b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605
SHA512:	92a52f68a7324c4d5876e1f7e2cb87d14b8604b057ceee2 e537815568faa96abf576a22111c5c976eff72ab9015f126 1b2331d4b4d711f4e62c8eb403c2377aa
SSDEEP:	3072:2glZ3FtCKXhkmHtZ9TEKzjfj/WMngyIfsJ0F7xPtoM:2IIKXhZtL7jOTyIG87Xl
File Content Preview:	.ELF....................B.x...4.........4. ...(.............@...@..................................C...C...................*.*UPX!.X.....................]....|.$..ELF..........@.`....4...p... ...(......<...@......[v......H...`.t/._...dt.Q.....].M........P......

Static ELF Info

ELF header

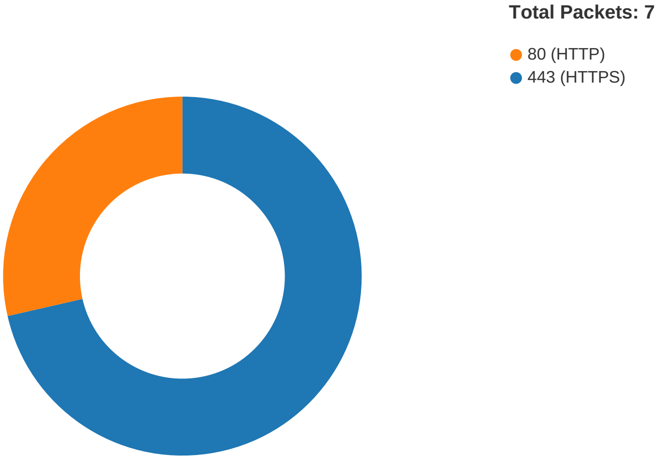
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x420578
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
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	0x400000	0x400000	0x20fc2	0x20fc2	4.4499	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x91f18	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: bin.sh PID: 5223 Parent PID: 5120

General

Start time:	18:59:38
Start date:	11/01/2022
Path:	/tmp/bin.sh
Arguments:	/tmp/bin.sh
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read