

Report

Static Malware Analysis Using PEStudio

Sakarie Sa'ad Osman (Sap iD:30025)

Riphah International University

Date: 18 May 2024

Table of Contents

Executive Summary	3
Introduction.....	4
Objective:	4
Detailed Analysis:	5
Sections:	6
Imports:	7
Libraries:	7
Strings:	8
VirusTotal Results:	9
Conclusion:	12

Executive Summary

Overview:

This report provides a comprehensive analysis of PackerParadox.zip using PEStudio.

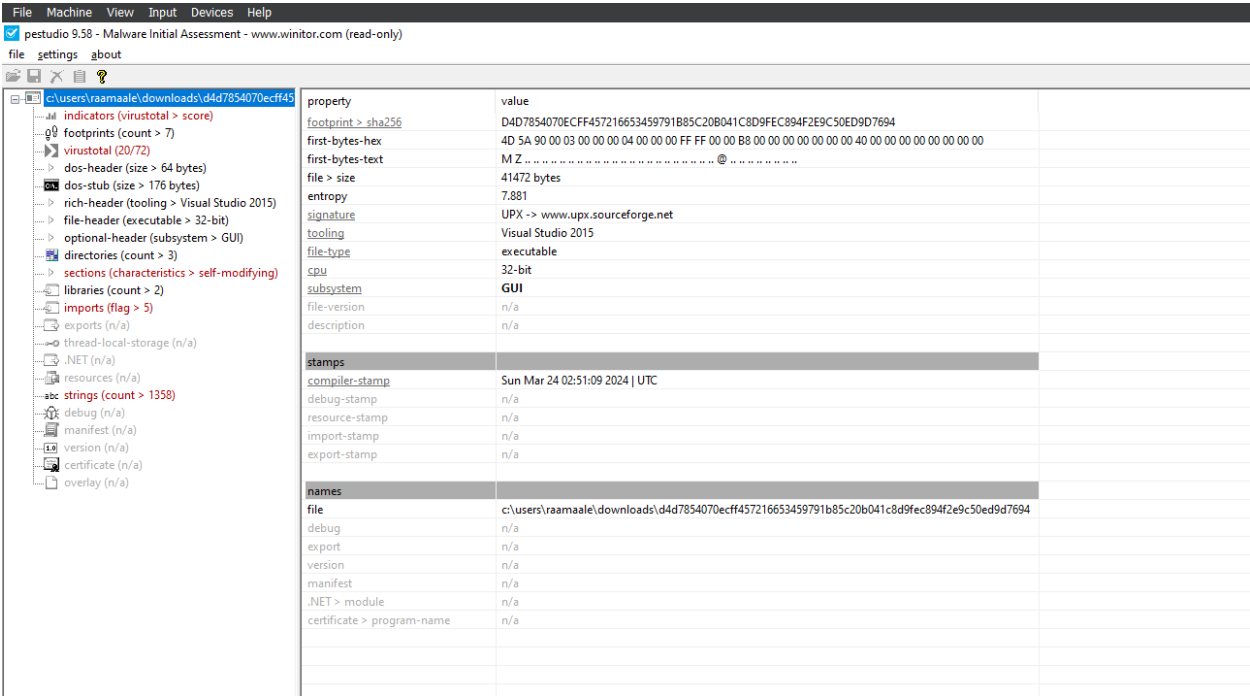
The primary purpose of this analysis was to determine the potential threat posed by this file.

Key findings indicate several suspicious imports and anomalies in the PE structure.

Introduction

File Information:

- Names: PackerParadox.zip or PackerParadox (1).zip.
- MD5: dd11788ec438eff8455536caef6ce565
- SHA-1: a4cffff7acaafa547b373383e7688abead9e5c1d
- SHA-256: 4719e3f390a56e746fbc7721396d11cea113133f967eea572f0d1b8ba28907d0
- File Type: ZIP, Compressed, zip
- Size: 38.42 KB (39337 bytes)



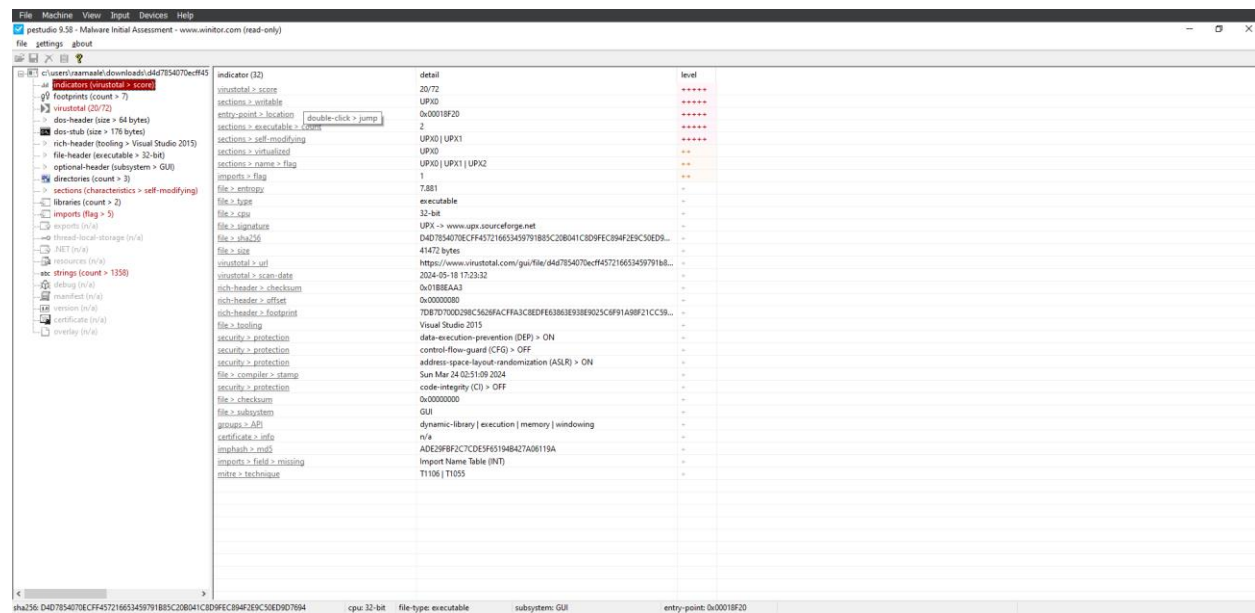
Objective:

The objective of this analysis is to assess the potential malicious nature of PackerParadox.zip and provide detailed insights into its structure and behavior.

Indicators:

The given below image shows how PeStudio has identified several indicators in the level column. Which indicates the level of severity.

You can find the names, imports, strings, and even sections within the sample that PESTudio finds suspicious



Sections:

As usual section contains .text .data, rdata, and other file names but for this specific malware it contains UPX file names (UPX0, UPX1, and UPX2). Which could mean the same as .data and others because UPX is an open-source executable packer that compresses and encrypts executable files, to reduce their size and make reverse engineering hard.

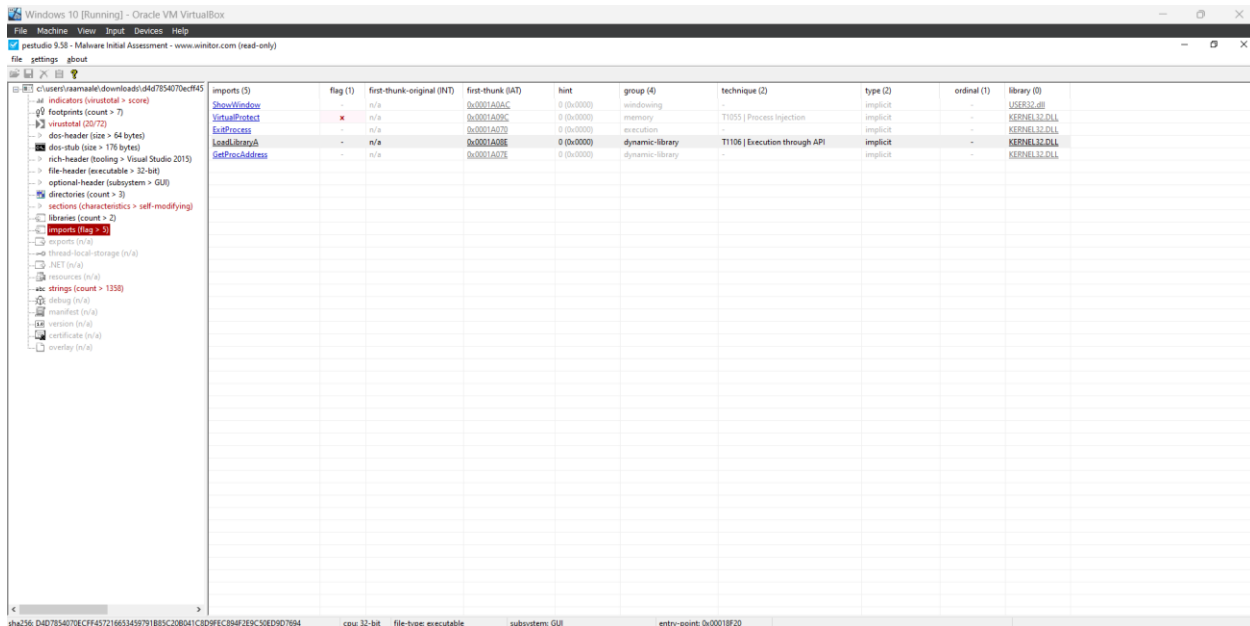
The screenshot displays the PE sections of a malware executable. The sections list on the left includes UPX0, UPX1, and UPX2, which are UPX packer sections. The characteristics table shows the executable is writable, executable, and has various other flags. The items table shows the entry point at 0x0010F20.

property	value	value	value
section	section[0]	section[1]	section[2]
name	UPX0	UPX1	UPX2
timestamp - sha126	n/a	C18638775988180558B0555...	00A3D4BC221EF041B4C3A7...
entropy	n/a	7.862	2.131
file-ratio (97.53%)	n/a	96.30 %	1.23 %
raw-address (begin)	0x00000400	0x00000400	0x0000A000
raw-address (end)	0x00000400	0x0000A000	0x0000A200
raw-size (60448 bytes)	0x00000000 (0 bytes)	0x00009C30 (39936 bytes)	0x00000200 (512 bytes)
virtual-address	0x00010000	0x00010000	0x0001A000
virtual-size (100496 bytes)	0x0000F000 (61440 bytes)	0x0000A000 (40960 bytes)	0x00001000 (4096 bytes)
Characteristics	0x00000080	0x00000040	0x00000040
write	x	x	x
execute	x	x	x
share	-	-	-
read	x	x	x
cacheable	x	x	x
pageable	x	x	x
initialized-data	-	x	x
uninitialized-data	x	-	-
self-modifying	x	x	-
virtual	x	-	-
Items			
directory - import	-	-	0x0001A000
directory - relocation	-	-	0x0001A000
directory - load-configuration	-	0x00019AEC	-
base-of-code	-	0x00010000	-
base-of-data	-	-	0x0001A000
entry-point	-	0x00010F20	-

sha256: D4D754D78EC4F37218653458791885C208041C8D9FC804F28C50ED9D7694 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x00010F20

Imports:

This one lists the imported DLLs and functions, it also highlights any suspicious or unusual imports.



As you can see from the image the functions use either one of these DLLs

Libraries:

USER32.dll:

- implements the Windows USER component that creates and manipulates the standard elements of the Windows user interface, such as the desktop, windows, and menus.

KERNEL32.DLL

- exposes to applications most of the Win32 base APIs, such as memory management, input/output (I/O) operations, process and thread creation, and synchronization functions.

Strings:

This section is always looked at because it can possibly contain File Names, FilePaths, Commands, IP Addresses, Domain Names, etc.

Windows 10 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

petstudio 9.58 - Malware Initial Assessment - www.sansir.com (read-only)

file settings about

Encoding (1) size (bytes) location flag (1) label (12) group (4) technique (2) value

encoding (1)	size (bytes)	location	flag (1)	label (12)	group (4)	technique (2)	value
ascii	10	section:UPX2	-	import	windowing	-	ShowWindow
ascii	14	section:UPX2	x	import	memory	T1055 Process Injection	VirtualProtect
ascii	11	section:UPX4	-	import	execution	-	ExitProcess
ascii	14	section:UPX2	-	import	dynamic-library	-	GetProcAddress
ascii	11	section:UPX2	-	import	dynamic-library	T1106 Execution through API	LoadLibrary
ascii	4	-	-	utility	-	-	UPX0
ascii	4	-	-	utility	-	-	UPX1
ascii	4	-	-	utility	-	-	UPX2
ascii	5	section:UPX1	-	format-string	-	-	VW%Q<
ascii	12	section:UPX2	-	file	-	-	KERNEL32.DLL
ascii	10	section:UPX2	-	file	-	-	USER32.dll
ascii	40	dos-stub	-	dos-message	-	-	This program cannot be run in DOS mode.
ascii	4	rich-header	-	-	-	-	Rich
ascii	4	-	-	-	-	-	4.22
ascii	4	-	-	-	-	-	UPX0
ascii	3	section:UPX1	-	-	-	-	LOZ
ascii	3	section:UPX1	-	-	-	-	Hd
ascii	3	section:UPX1	-	-	-	-	OZE
ascii	4	section:UPX1	-	-	-	-	79c
ascii	3	section:UPX1	-	-	-	-	reV
ascii	3	section:UPX1	-	-	-	-	yIS
ascii	3	section:UPX1	-	-	-	-	79
ascii	3	section:UPX1	-	-	-	-	wE
ascii	3	section:UPX1	-	-	-	-	6i
ascii	4	section:UPX1	-	-	-	-	N2pX
ascii	3	section:UPX1	-	-	-	-	14
ascii	4	section:UPX1	-	-	-	-	V\$6G
ascii	8	section:UPX1	-	-	-	-	V20w#e,0
ascii	5	section:UPX1	-	-	-	-	~3[Rt
ascii	3	section:UPX1	-	-	-	-	4d
ascii	3	section:UPX1	-	-	-	-	J'L
ascii	4	section:UPX1	-	-	-	-	y97
ascii	5	section:UPX1	-	-	-	-	c55tg
ascii	4	section:UPX1	-	-	-	-	2+M
ascii	3	section:UPX1	-	-	-	-	+In
ascii	3	section:UPX1	-	-	-	-	ZM
ascii	3	section:UPX1	-	-	-	-	C=V
ascii	4	section:UPX1	-	-	-	-	sm-
ascii	3	section:UPX1	-	-	-	-	xq
ascii	3	section:UPX1	-	-	-	-	Hn
ascii	3	section:UPX1	-	-	-	-	v68
ascii	3	section:UPX1	-	-	-	-	r t

Activate Windows
Go to Settings to activate Windows.

sha256: D4D7B54070ECF457218653459791885C208041C8D9FEC84F2B9C30E9D7694

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0010F20

Type here to search

27°C Haze 2:38 AM 5/19/2024

VirusTotal Results:

Detection

11

/ 68

Community

Score

11/68 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

4719e3f390a56e746bc7721396d11cea113133f967eea572f0d1b8ba28907d0

Size38.42 KB

Last Modification Date8 minutes ago

ZIP

PackerParadox.zip

zipcontains-pechecks-user-inputdetect-debug-environmentlong-sleeps

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.

Threat categories

trojan

Security vendors' analysis

Do you want to automate checks?

BitDefenderTheta	Gen:NN.ZexaF.36804.cmGfauKqzdp	DeepInstinct	MALICIOUS
Elastic	Malicious (moderate Confidence)	Lionic	Virus.Generic.AI.11c
Malwarebytes	MachineLearning/Anomalous.96%	Microsoft	Trojan:Win32/Wacatac.B!ml
Rising	Trojan.Generic@AI.98 (RDML-2mb3LIZDi...	Sangfor Engine Zero	Suspicious.Win32.Save.a
SentinelOne (Static ML)	Static AI - Suspicious Archive	Skyhigh (SWG)	BehavesLike.Generic.nc
Yandex	Trojan.GenAsaIqu4xAGDMPV8	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
AliCloud	Undetected	AlYar	Undetected

Details: File system actions.

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

File system actions ⓘ

^

Files Opened

🔍

C:\Windows\SystemResources\USER32.dll.mun

🔍

C:\Windows\Fonts\staticcache.dat

🔍

C:\Windows\system32\ole32.dll

🔍

C:\Windows\syswow64\en-US\USER32.dll.mui

🔍

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\unarchiver.exe.log

🔍

C:\Users\user\AppData\Local\Temp\hclgucms.ofv\

🔍

C:\Users\user\AppData\Local\Temp\hclgucms.ofv\PackerParadox.exe

🔍

C:\Users\user\AppData\Local\Temp\unarchiver.log

🔍

C:\Users\user\Desktop\PackerParadox.zip

🔍

C:\Windows\AppPatch\sysmain.sdb

▼

Files Written

🔍

C:\Users\user\AppData\Local\Temp\hclgucms.ofv

🔍

C:\Users\user\AppData\Local\Temp\hclgucms.ofv\PackerParadox.exe

🔍

C:\Users\user\AppData\Local\Temp\unarchiver.log

🔍

\\Device\ConDrv\Connect

Files Dropped

+ C:\Users\user\AppData\Local\Temp\hclgucms.ofv\PackerParadox.exe

+ C:\Users\user\AppData\Local\Temp\unarchiver.log

Registry actions ⓘ

^

Window Registry:

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

Registry actions ⓘ

Registry Keys Opened

- 🔍 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize
- 🔍 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize\AppsUseLightTheme
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Input\MaxResyncAttempts
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Input\ResyncResetTime
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows\IsVailContainer
- 🔍 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\OOBE\LaunchUserOOBE
- 🔍 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy

▾

Process and service actions ⓘ

Processes Created

- 🔍 "C:\Users\<USER>\AppData\Local\Temp\PackerParadox.exe"
- 🔍 "C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Desktop\PackerParadox.zip"
- 🔍 C:\Users\user\AppData\Local\Temp\hclgucms.ofv\PackerParadox.exe
- 🔍 C:\Windows\SysWOW64\7za.exe "C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\hclgucms.ofv" "C:\Users\user\Desktop\PackerParadox.zip"
- 🔍 C:\Windows\SysWOW64\cmd.exe "cmd.exe" /C "C:\Users\user\AppData\Local\Temp\hclgucms.ofv\PackerParadox.exe"
- 🔍 C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Processes Terminated

- 🔍 C:\Windows\SysWOW64\7za.exe

Conclusion:

Summary of Findings:

The analysis of PackerParadox.zip revealed multiple indicators of potentially malicious behavior, including suspicious imports, strings, and a significant number of detections on VirusTotal.

Assessment:

Based on the static analysis, PackerParadox.zip appears to be a high-risk file likely designed for malicious purposes.