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

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.

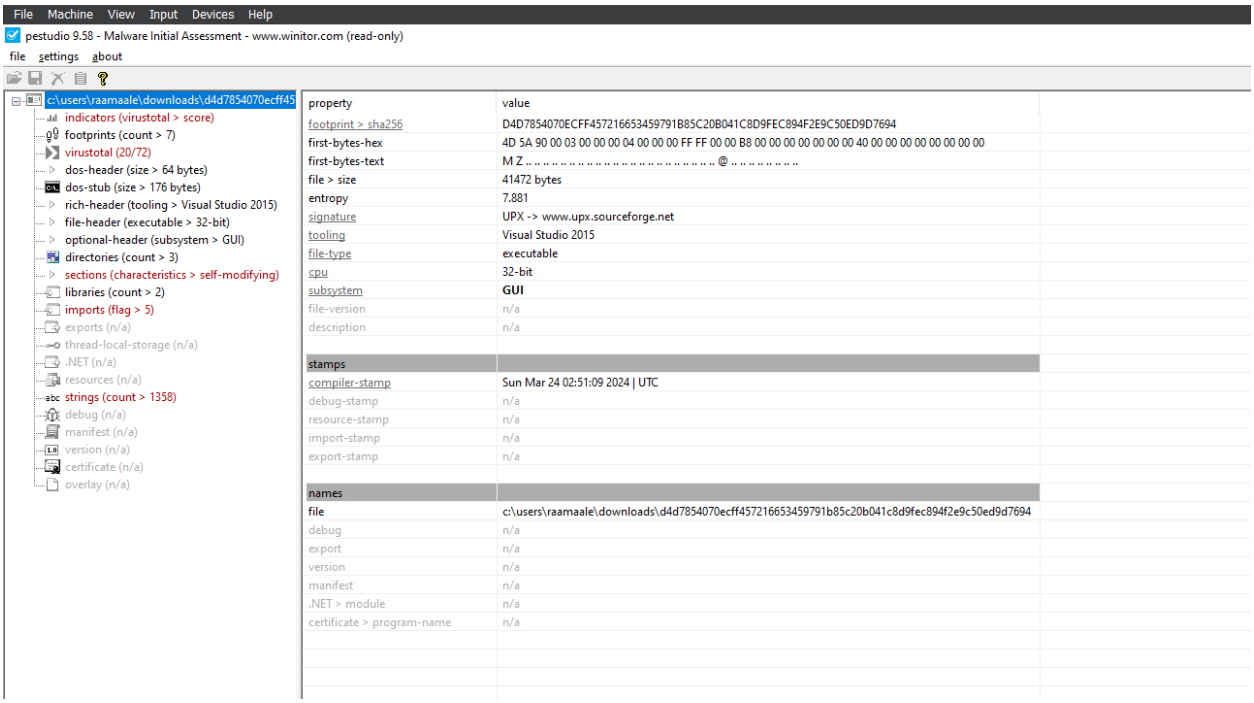
-MD5: dd11788ec438eff8455536caef6ce565

-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.

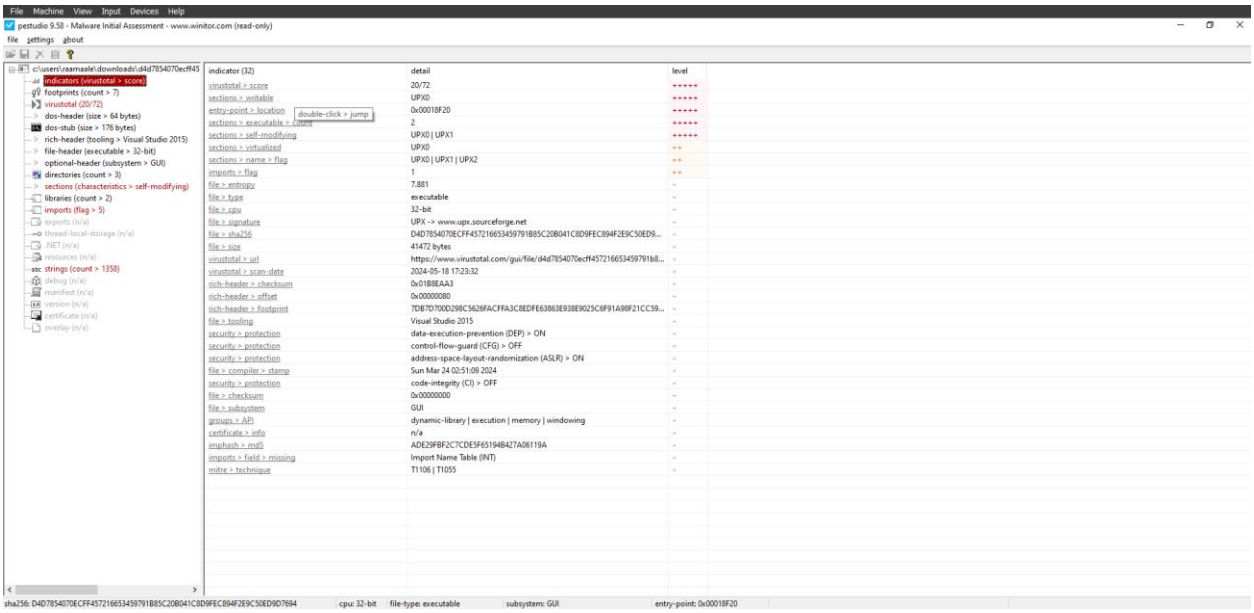
Detailed Analysis:

Indicators:

In the indicators tab, the tool highlights data within the sample that may be malicious.

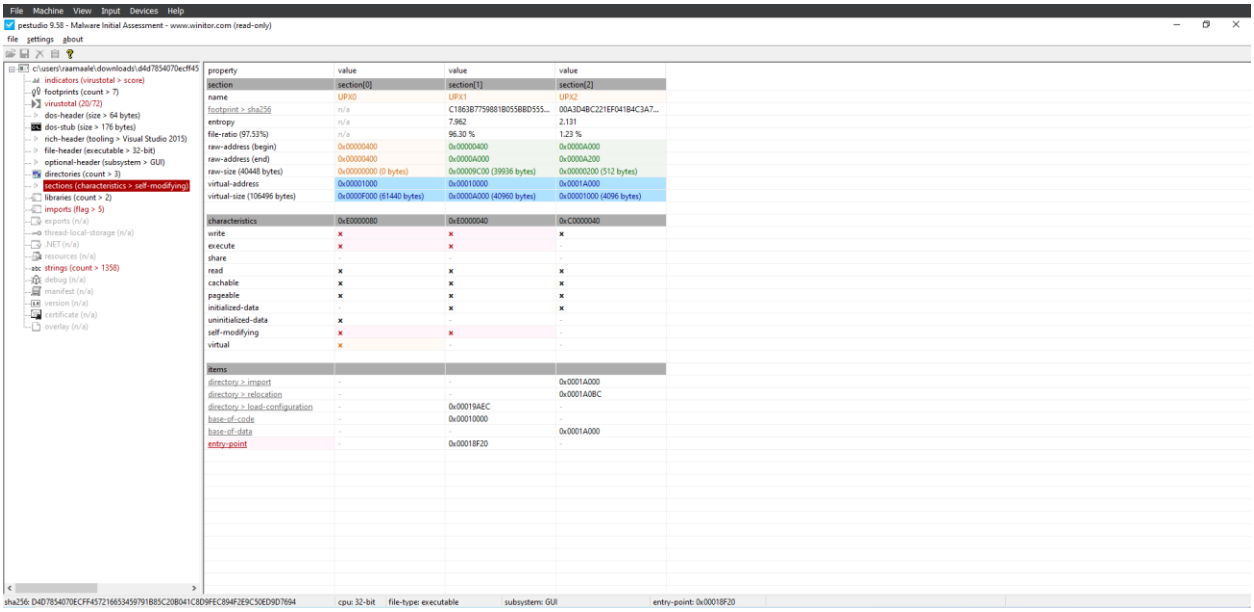
The given below image shows how PeStudio has identified several indicators in the level column. Which indicates the level of severity.

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



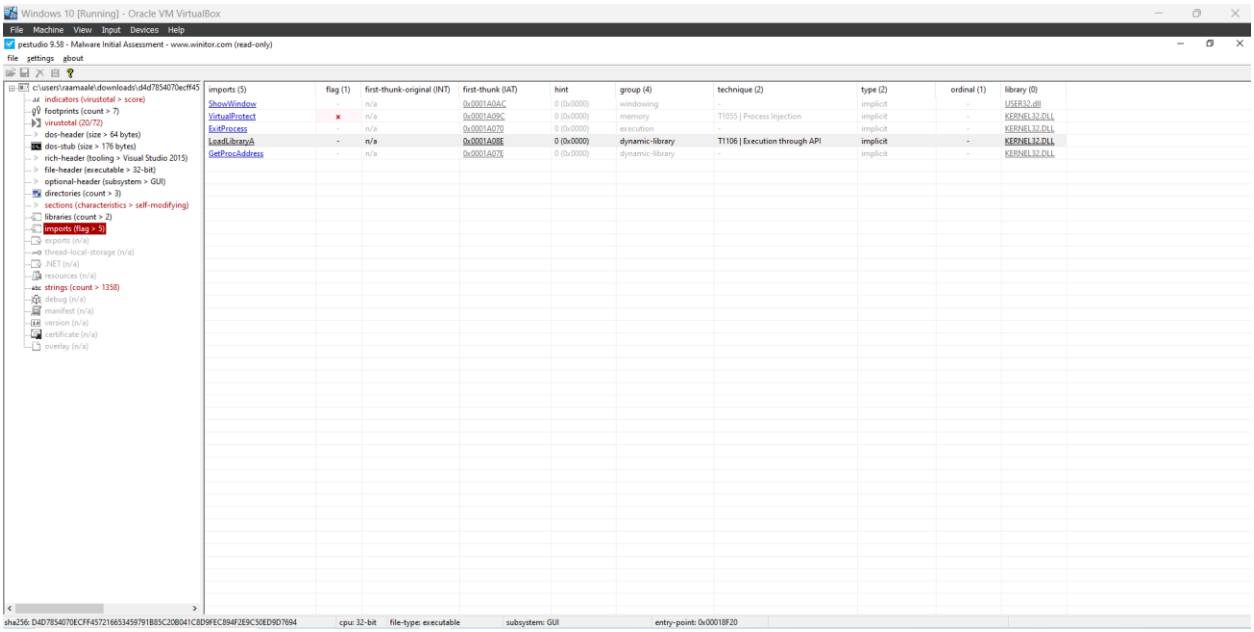
Sections:

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.



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:

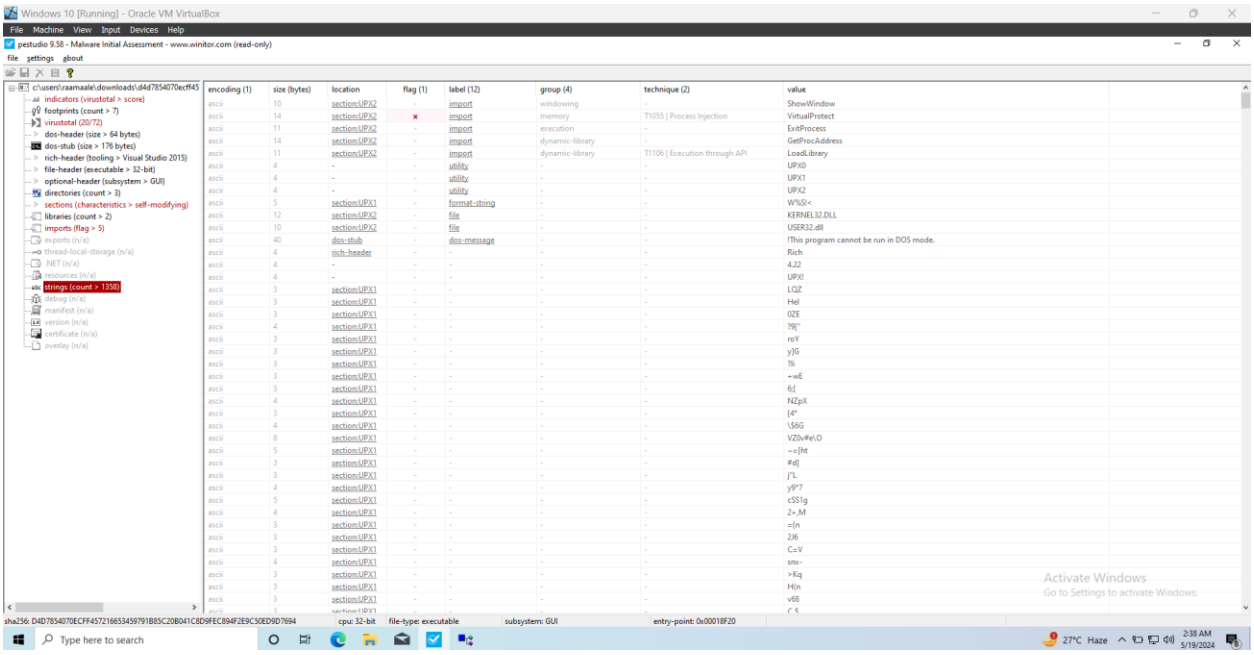
- implements the Windows USER component that creates and manipulates the standard elements of the Windows user interface, such as the desktop, windows, and menus.

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.

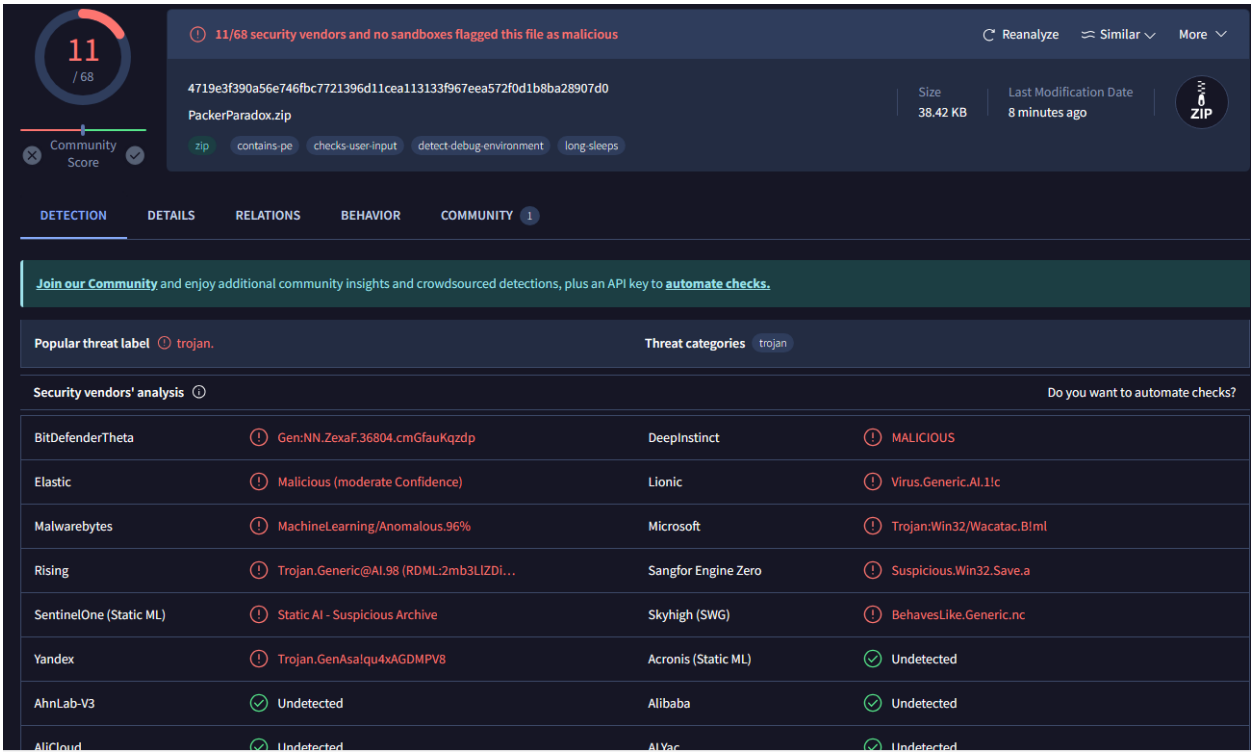
Strings:

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

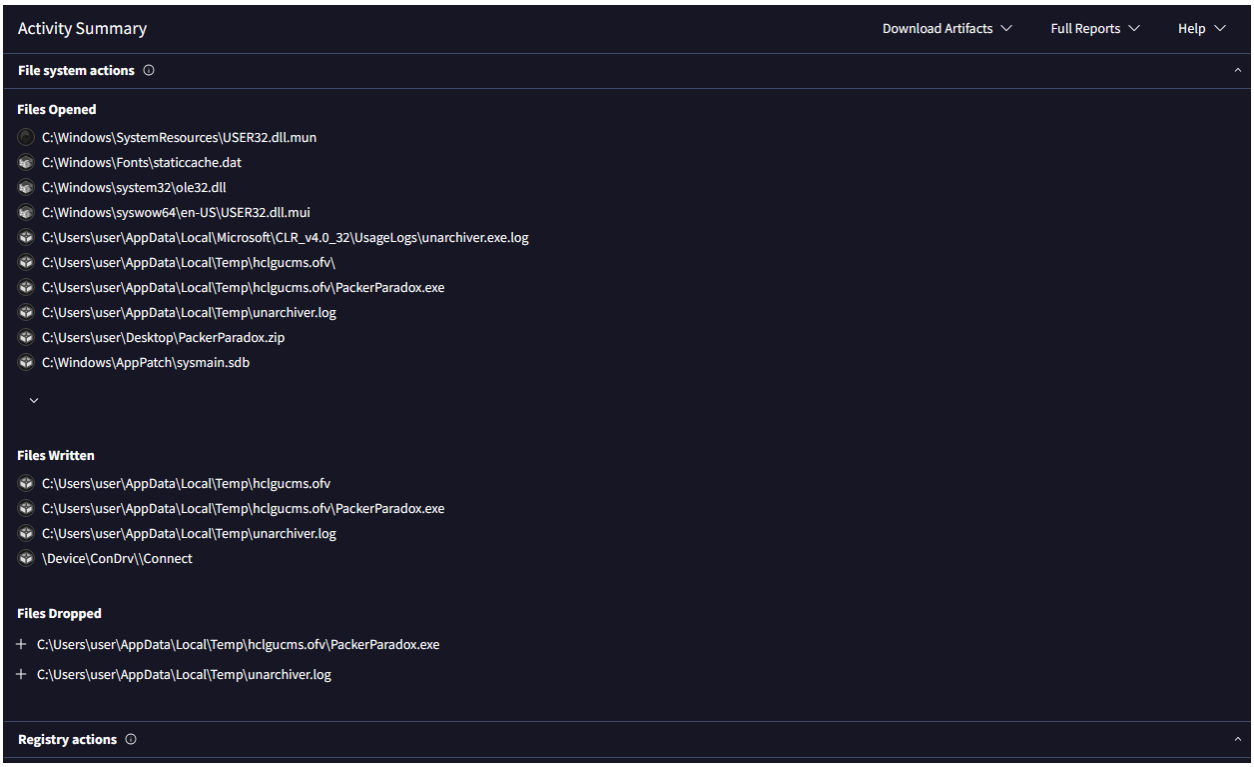


VirusTotal Results:

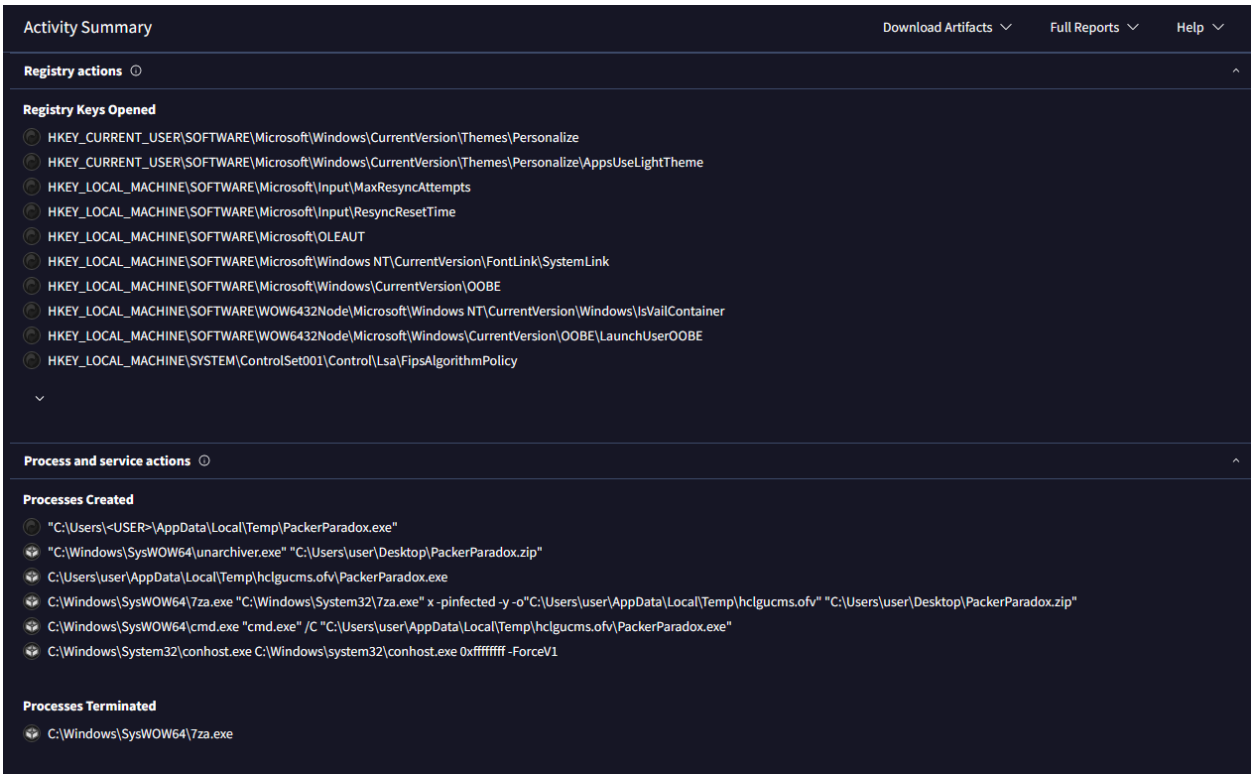
Detection



Details: File system actions.



Window Registry:



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.