DIGITAL FORENSIC PROJECT

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

STATIC AND DYNAMIC MALWARE ANALYSIS

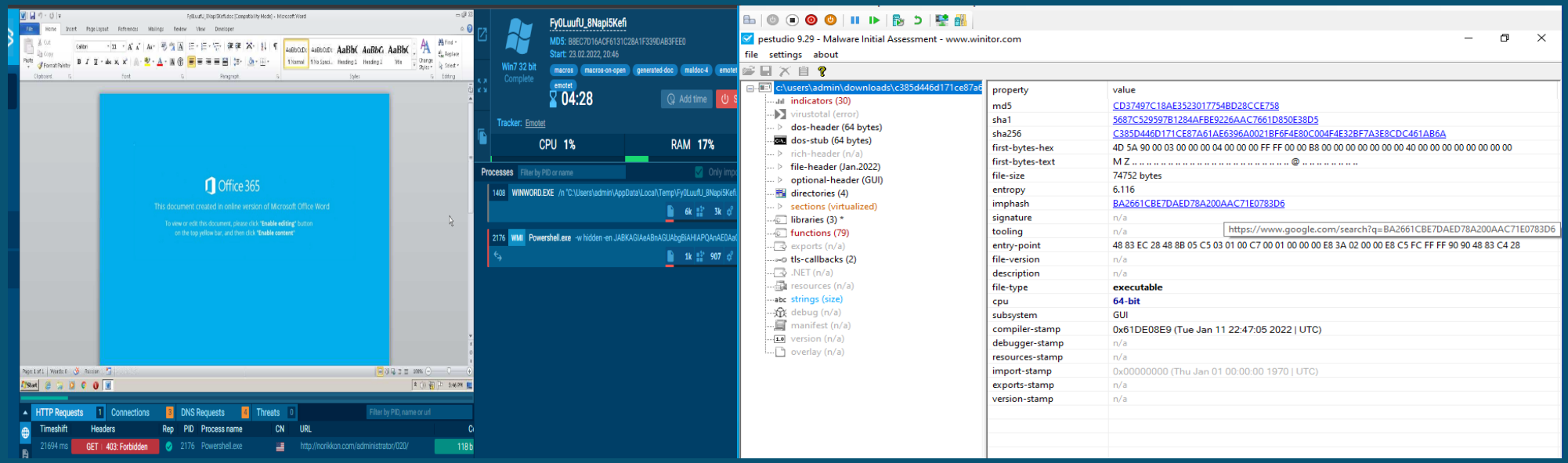
STATIC AND DYNAMIC MALWARE ANALYSIS

Project Name: Static And Dynamic Malware Analysis

Tool Used: Static Analysis: Peid,Pestudio, CFF Explorer, EXEinfoPE **Dynamic Analysis:** Any.run

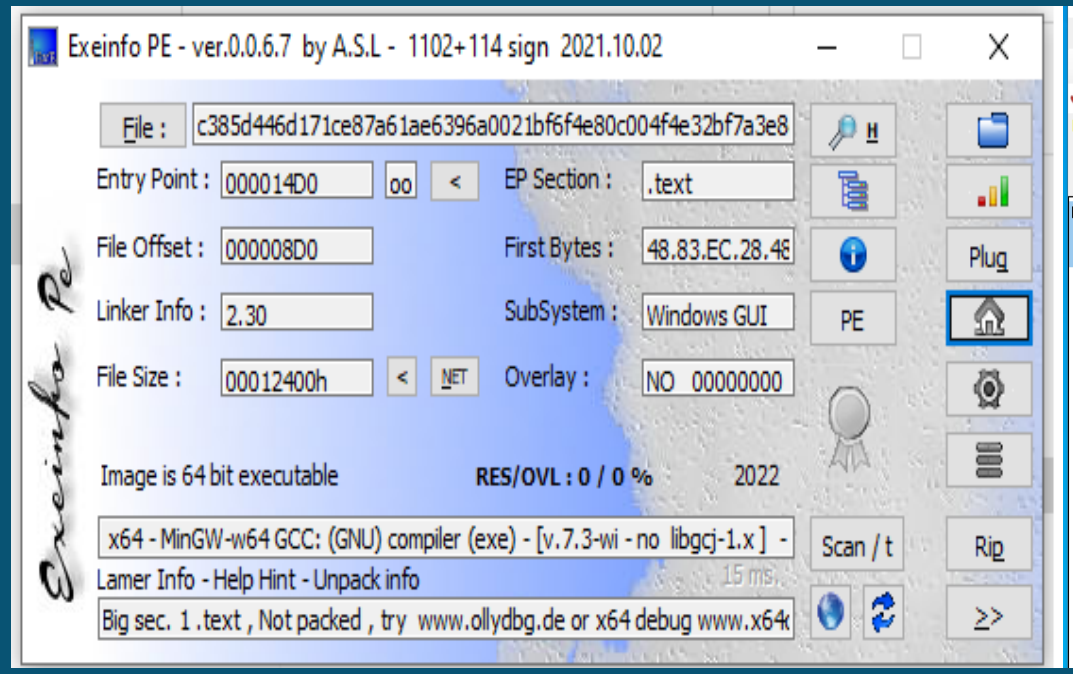
Platform: Windows

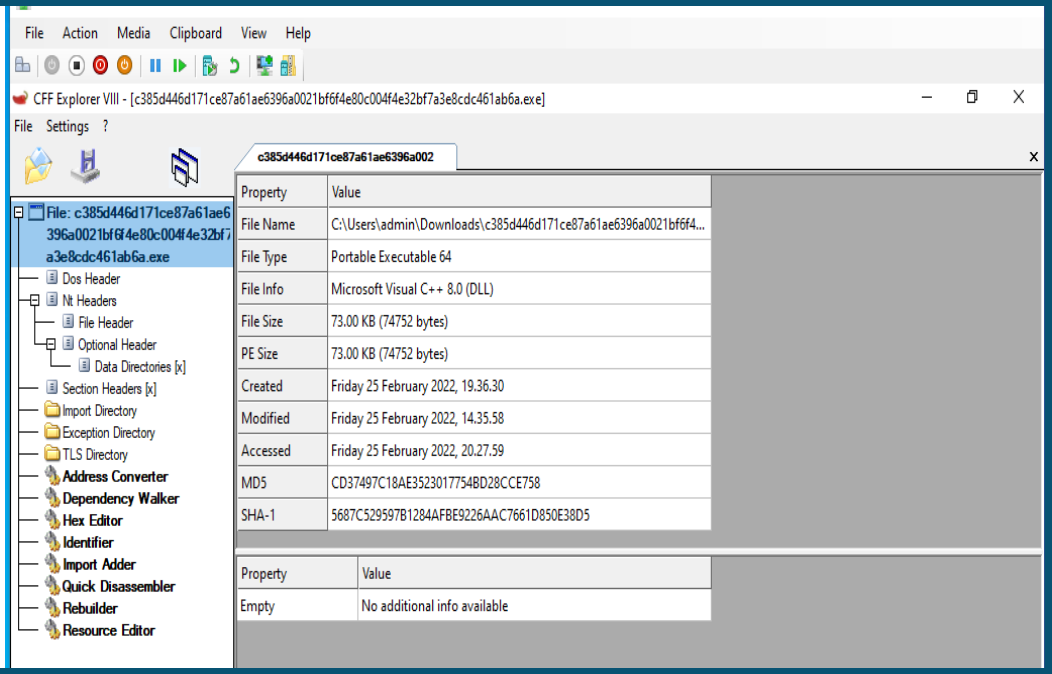
Work Around Existence: Any.run | Cookoo sandBox



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

STATIC AND DYNAMIC MALWARE ANALYSIS





STATIC AND DYNAMIC MALWARE ANALYSIS

DESCRIPTION :

The malware analysis with advanced static analysis tools PEstudio, EXEinfope, PEid and CFF Explorer are capable of providing more complete information about characteristics of malware, such as the information of malware to infect another programs, as well as modifying the registry and create new files and folders. Whereas on basic methods of malware dynamic analysis can discover DLL of malware, the process of malware inside the system, as well as the network connection performed by malware against the server.

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 3

Contacted URLs

Scanned	Detections	Status	URL
2022-02-25	18 / 94	404	http://file-coin-host-12.com/

Contacted Domains

Domain	Detections	Created	Registrar
file-coin-host-12.com	17 / 90	2021-11-23	-
host-data-coin-11.com	17 / 90	2021-11-23	-

Contacted IP Addresses

IP	Detections	Autonomous System	Country
80.66.64.170	0 / 90	57416	TR

Execution Parents

Scanned	Detections	Type	Name
2022-02-25	36 / 70	Win32 EXE	win_setup__62188a40dd146.exe
2022-02-25	40 / 68	Win32 EXE	setup_installer.exe