

# 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

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.



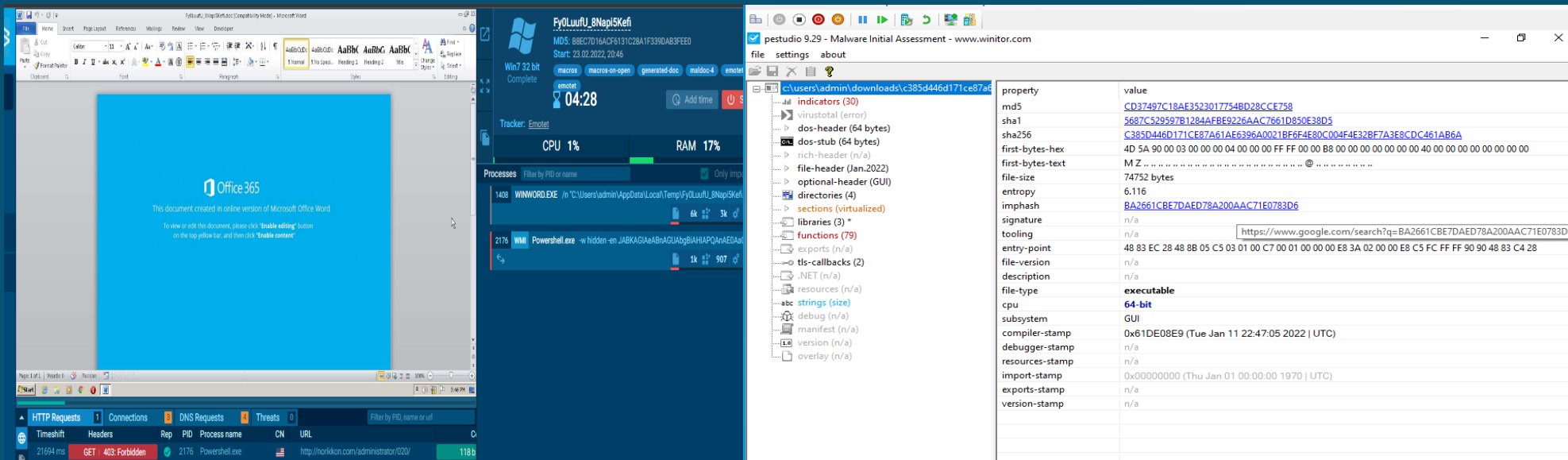
# STATIC AND DYNAMIC MALWARE ANALYSIS

**Project Name:** Static And Dynamic Malware Analysis

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

**Platform:** Windows

**Work Around Existence:** Any.run | Cookoo sandBox



The screenshot displays a Windows desktop environment used for malware analysis. On the left, a Microsoft Word document is open. In the center, a process tracker shows the following active processes:

Process ID	Process Name	Architecture	Session	Working Set	Private Bytes	Private Bytes (Private Bytes / Working Set)
1408	WINWORD.EXE	x64	0	12K	3K	1.5
2176	PowerShell.exe	x64	0	1K	907	0.9

On the right, the Pesticide tool displays the file properties for a PE file:

property	value
md5	CD37497C18A63523017754BD28CC6758
sha1	5687C529597B1284AFB9226AAC7661D850E38D5
sha256	C385D446D171CE87A61AE6396A0021BF6F4E80C004F4E32BF7A3E8CDC461A86A
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z .....
file-size	74752 bytes
entropy	6.116
imphash	BA2661CBE7DAED78A200AAC71E0783D6
signature	n/a
tooling	n/a
entry-point	48 83 EC 28 48 8B 05 C5 03 01 00 C7 00 01 00 00 00 E8 3A 02 00 00 E8 C5 FC FF FF 90 90 48 83 C4 28
file-version	n/a
description	n/a
file-type	executable
cpu	64-bit
subsystem	GUI
compiler-stamp	0x61DE08E9 (Tue Jan 11 22:47:05 2022   UTC)
debugger-stamp	n/a
resources-stamp	n/a
import-stamp	0x00000000 (Thu Jan 01 00:00:00 1970   UTC)
exports-stamp	n/a
version-stamp	n/a

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

Exeinfo PE - ver.0.0.6.7 by A.S.L - 1102+114 sign 2021.10.02

File : c385d446d171ce87a61ae6396a0021bf6f4e80c004f4e32bf7a3e8

Entry Point : 000014D0 EP Section : .text

File Offset : 000008D0 First Bytes : 48.83.EC.28.4E

Linker Info : 2.30 SubSystem : Windows GUI

File Size : 00012400h Overlay : NO 00000000

Image is 64 bit executable RES/OVL : 0 / 0 % 2022

x64 - MinGW-w64 GCC: (GNU) compiler (exe) - [v.7.3-wi - no libgcj-1.x] -

Lamer Info - Help Hint - Unpack info 15 ms.

Big sec. 1 .text , Not packed , try www.ollydbg.de or x64 debug www.x64

CFF Explorer VIII - [c385d446d171ce87a61ae6396a0021bf6f4e80c004f4e32bf7a3e8cdc461ab6a.exe]

File Settings ?

File: c385d446d171ce87a61ae6396a0021bf6f4e80c004f4e32bf7a3e8cdc461ab6a.exe

Property	Value
File Name	C:\Users\admin\Downloads\c385d446d171ce87a61ae6396a0021bf6f4e80c004f4e32bf7a3e8cdc461ab6a.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	73.00 KB (74752 bytes)
PE Size	73.00 KB (74752 bytes)
Created	Friday 25 February 2022, 19.36.30
Modified	Friday 25 February 2022, 14.35.58
Accessed	Friday 25 February 2022, 20.27.59
MD5	CD37497C18AE3523017754BD28CCE758
SHA-1	5687C529597B1284AFBE9226AAC7661D850E38D5

Property	Value
Empty	No additional info available



# 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 <span>3</span>
<b>Contacted URLs</b> ⓘ				
<b>Scanned</b> 2022-02-25	<b>Detections</b> 18 / 94	<b>Status</b> 404	<b>URL</b> http://file-coin-host-12.com/	
<b>Contacted Domains</b> ⓘ				
<b>Domain</b> file-coin-host-12.com	<b>Detections</b> 17 / 90	<b>Created</b> 2021-11-23	<b>Registrar</b> -	
	host-data-coin-11.com	17 / 90	2021-11-23 -	
<b>Contacted IP Addresses</b> ⓘ				
<b>IP</b> 80.66.64.170	<b>Detections</b> 0 / 90	<b>Autonomous System</b> 57416	<b>Country</b> TR	
<b>Execution Parents</b> ⓘ				
<b>Scanned</b> 2022-02-25	<b>Detections</b> 36 / 70	<b>Type</b> Win32 EXE	<b>Name</b> win_setup__62188a40dd146.exe	
	2022-02-25	40 / 68	Win32 EXE setup_installer.exe	

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.

