Static Analysis

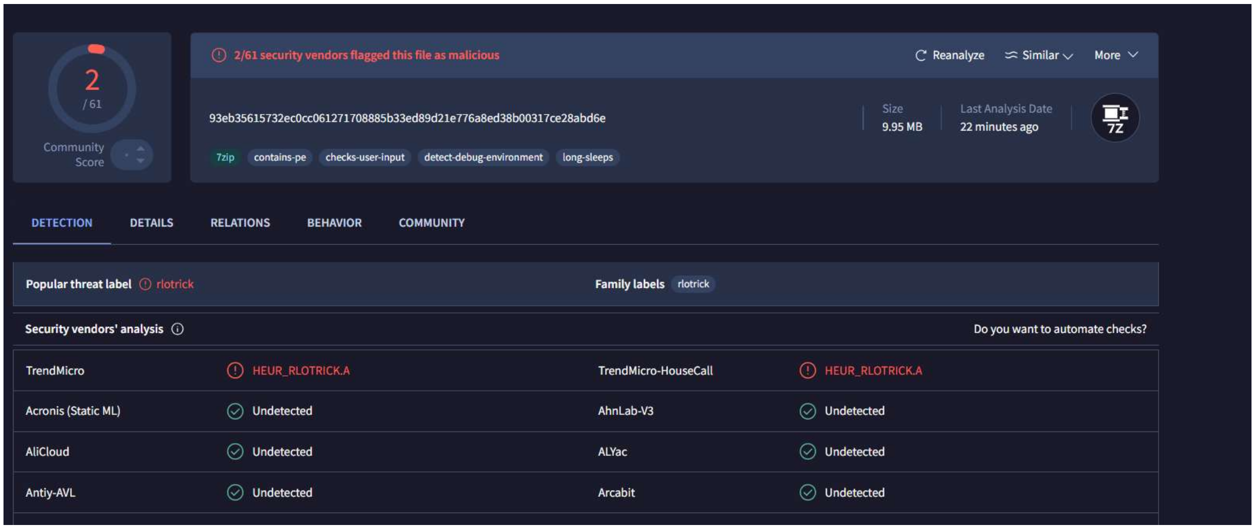
1. Virus Total Analysis

Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
  - MD5: 11ffc201d1c88b50fa9ba2a0471d7ef5
  - SHA-1: e676f29544b1ae41b8cd8a7551716b4682a5c8a2
  - SHA-256: 93eb35615732ec0cc061271708885b33ed89d21e776a8ed38b00317ce28abd6e
- Method of hash acquisition: [Describe process] I used VirusTotal and confirmed that it matches the hash values in Detect-It-Easy
- [Link to VirusTotal results]
  - https://www.virustotal.com/gui/file/93eb35615732ec0cc061271708885b33ed89d21e776a8ed38b00317ce28abd6e/detection

Vendor Analysis

- Number of vendors flagging as malicious: [2/61]



2/61 security vendors flagged this file as malicious

93eb35615732ec0cc061271708885b33ed89d21e776a8ed38b00317ce28abd6e

7zip contains-pe checks-user-input detect-debug-environment long-sleeps

Size 9.95 MB

Last Analysis Date 22 minutes ago

Popular threat label rlotrick

Family labels rlotrick

Security vendors' analysis

TrendMicro	HEUR_RLOTRICK.A	TrendMicro-HouseCall	HEUR_RLOTRICK.A
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected

- Analysis of vendor results:
  - [Discuss patterns in detection]
    - 7zip
    - contains-pe
    - checks-user-input
    - Detect-debug-environment
    - long-sleeps
  - [Common malware names identified]
    - HEUR_RLOTRICK.A
    - rlotrick
  - [Notable vendor disagreements]
    - Many vendors did not detect it, but two did- TrendMicro and TrendMicro-HouseCall

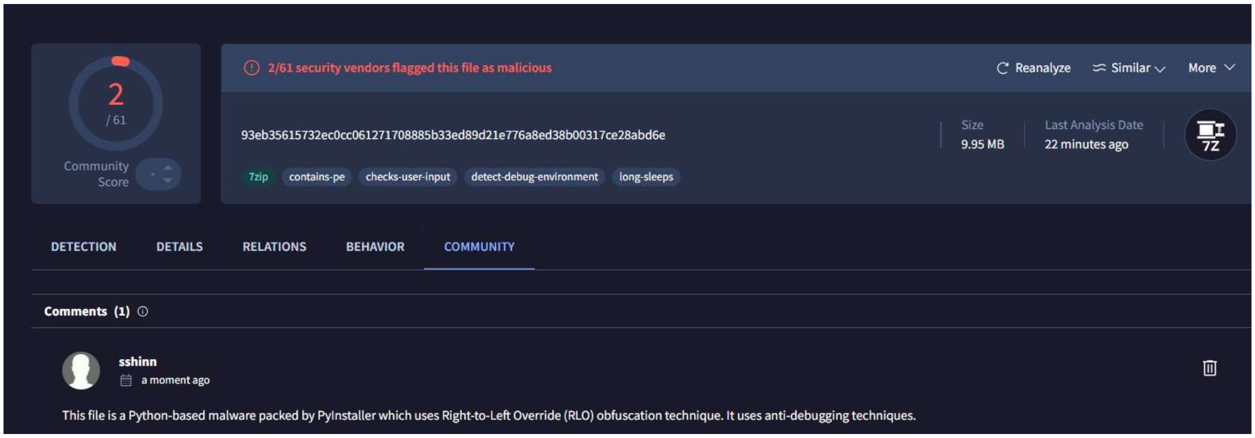
File History

- First Submission Date: [Date]
  - 2025-03-16 01:36:46 UTC
- File Creation Date from Windows: [Date]
  - 2024-11-11 17:36:53
- Analysis of submission timeline:

    - [Discussion of file age]
        - The file is a few months old
    - [Notable resubmissions or changes]
        - I was the first one to submit the file, but it was flagged as malicious by vendors, which means it contains malicious patterns

Community Score

- [Link to your VirusTotal community contribution]
    - https://www.virustotal.com/gui/file/93eb35615732ec0cc061271708885b33ed89d21e776a8ed38b00317ce28abd6e/community
    - Username: sshinn



93eb35615732ec0cc061271708885b33ed89d21e776a8ed38b00317ce28abd6e

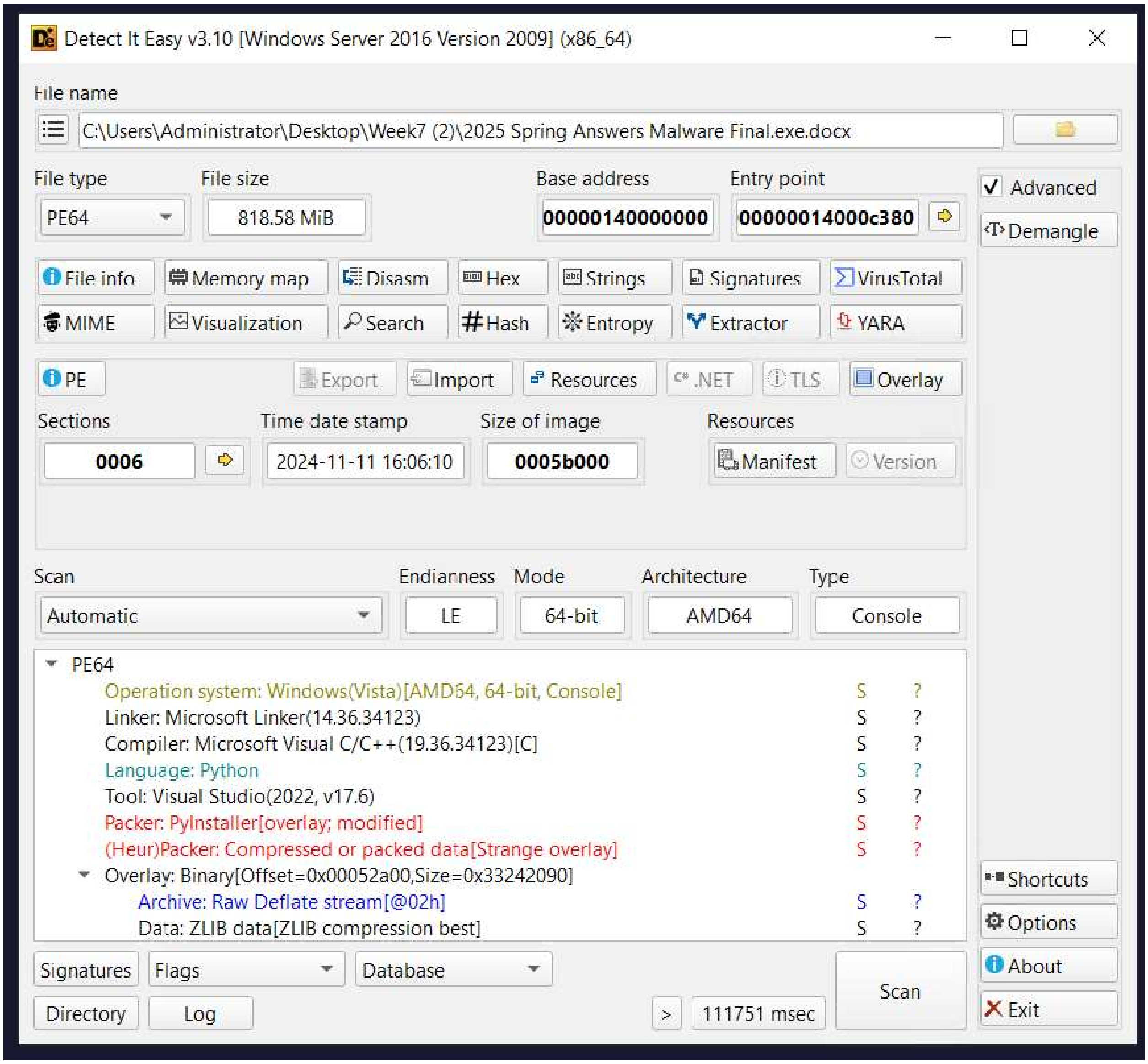
This file is a Python-based malware packed by PyInstaller which uses Right-to-Left Override (RLO) obfuscation technique. It uses anti-debugging techniques.

- Summary of initial findings posted to the community:
    - [Key observations]
        - RLO family of malware
        - anti-debugging
    - [Potential indicators of compromise]
        - Packed with PyInstaller
        - Invalid characters used in filename
        - Difficult to unpack

2. Detect It Easy (DIE) Analysis

File information

- File type: [Type] PE64
- Architecture: [Architecture] AMD64
- Compiler: [Compiler information]
    - Compiler: Microsoft Visual C/C++(19.36.34123)[C]
- Additional relevant information:
    - [List notable file characteristics]
        - Operation system: Windows(Vista)[AMD64, 64-bit, Console]
        - Packer: PyInstaller[overlay; modified]
        - File has an invalid character in the filename
            - It looks like this has a filename with reversed characters due to the Right-to-Left Override (RLO) trick. This means the malware might be disguising itself by flipping part of its filename using the U+202E Unicode character. Flagged as ".eman ni" by Ghidra



File name: C:\Users\Administrator\Desktop\Week7 (2)\2025 Spring Answers Malware Final.exe.docx

File type: PE64 | File size: 818.58 MiB | Base address: 0000000140000000 | Entry point: 000000014000c380

Sections: 0006 | Time date stamp: 2024-11-11 16:06:10 | Size of image: 0005b000

Scan: Automatic | Endianness: LE | Mode: 64-bit | Architecture: AMD64 | Type: Console

```
PE64
    Operation system: Windows(Vista)[AMD64, 64-bit, Console]        S   ?
    Linker: Microsoft Linker(14.36.34123)                           S   ?
    Compiler: Microsoft Visual C/C++(19.36.34123)[C]                S   ?
    Language: Python                                                S   ?
    Tool: Visual Studio(2022, v17.6)                                S   ?
    Packer: PyInstaller[overlay; modified]                          S   ?
    (Heur)Packer: Compressed or packed data[Strange overlay]         S   ?
    Overlay: Binary[Offset=0x00052a00,Size=0x33242090]
        Archive: Raw Deflate stream[@02h]                           S   ?
        Data: ZLIB data[ZLIB compression best]                      S   ?
```

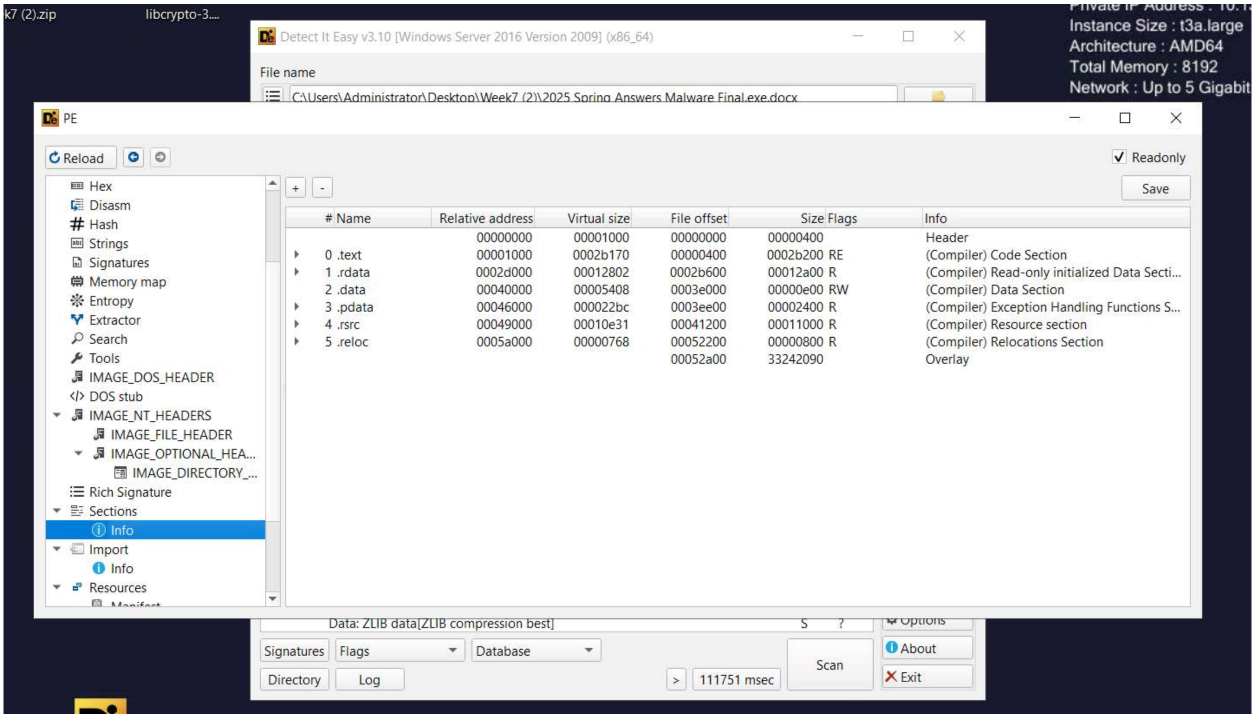
> 111751 msec

- [Unusual headers or structures]
    - // Author: DosX
    - // E-Mail: collab@kay-software.ru
    - // GitHub: https://github.com/DosX-dev
    - // Telegram: @DosX_dev
    - // ==
    - // ================== [DONATE] ==================
    - // Did you like my work? :D Thank you! But what
    - // about donation? I'll be very grateful <3
    - //
    - // >> Payeer: P1066822521 [Recommended]
    - //
    - // >> BTC: 37uRiHBqK3QiJ2jamqmmk1Q3sCmAmWngcC
    - // 0,0005 BTC minimum

- //
- // >> LTC: MCwRK1Z7K4GYHt9ZrbTR2SMCEqzqQaTbRF
- // 0,001 LTC minimum
- //
- // >> USDT: TUVH7QkcZws78QMC3XyAwfuzxUbaeLnfAC
- // TRC-20 5 USDT minimum
- // ==
- // ================= [CONTACTS] =================
- // Author: DosX
- // E-Mail: collab@kay-software.ru
- // GitHub: https://github.com/DosX-dev
- // Telegram: @DosX_dev
- // ==
- // If I don't respond to email, message to Telegram
- // ==
- // For the script to work correctly, the following
- // official Detect It Easy components are required:
- // "language", "FASM", "RosASM", "SpASM", "FPC"
- // "PE\linker.6.sg", "Microsoft.6.sg"
- // Please do not read the code out loud unless you have exorcism skills
- // Author: LinXP, Kaens (TG@kaens)

Memory Map Analysis

- Section breakdown:
    - [.text section analysis]
        - Size: 0002b200
        - Permissions:RE
    - [.data section analysis]
        - Size:00000e00
        - Permissions:RW
    - [.rsrc section analysis]
        - Size:00011000
        - Permissions:R
    - [Other relevant sections]
        - .rdata:
            - Size:00012a00
            - Permissions:R
        - .pdata:
            - Size:00002400
            - Permissions:R
        - .reloc:
            - Size:00000800
            - Permissions:R
- Notable findings:
    - [Unusual section permissions]
        - .text had Read, Execute permissions
        - .data had Read, Write permissions
    - [Section size anomalies]
        - .text was the largest
        - .rsrc is also large
        - .text being executable and .data being writable, is this suspicious?



Private IP Address : 10.1
Instance Size : t3a.large
Architecture : AMD64
Total Memory : 8192
Network : Up to 5 Gigabit

Detect It Easy v3.10 [Windows Server 2016 Version 2009] (x86_64)

File name
C:\Users\Administrator\Desktop\Week7 (2)\2025 Spring Answers Malware Final.exe.docx

☑ Readonly

#	Name	Relative address	Virtual size	File offset	Size	Flags	Info
		00000000	00001000	00000000	00000400		Header
0	.text	00001000	0002b170	00000400	0002b200	RE	(Compiler) Code Section
1	.rdata	0002d000	00012802	0002b600	00012a00	R	(Compiler) Read-only initialized Data Secti...
2	.data	00040000	00005408	0003e000	00000e00	RW	(Compiler) Data Section
3	.pdata	00046000	000022bc	0003ee00	00002400	R	(Compiler) Exception Handling Functions S...
4	.rsrc	00049000	00010e31	00041200	00011000	R	(Compiler) Resource section
5	.reloc	0005a000	00000768	00052200	00000800	R	(Compiler) Relocations Section
				00052a00	33242090		Overlay

Data: ZLIB data[ZLIB compression best] S ?

111751 msec

String Analysis

- Notable strings discovered:
  - [URLs/IPs]
    - network unreachable
    - network reset
    - network down
    - connection reset
    - connection refused
    - connection already in progress
    - connection aborted
  - [File paths]
    - Path of ucrtbase.dll (%s) and its name exceed buffer size (%d)
    - Path of Python shared library (%s) and its name (%s) exceed buffer size (%d)
    - kernel32, KERNEL32.dll, kernelbase, ntdll
    - lib-dynload (Python dynamic library folder)
  - [Command lines]
    - GetCommandLineW, GetCommandLineA → Captures command-line arguments
    - CreateProcessW → Can spawn new processes, a common behavior for malware executing payloads
    - TerminateProcess → Can forcefully kill processes, possibly AV evasion
    - OpenProcessToken, GetTokenInformation → Suggests privilege manipulation or access control queries
    - Execute format error → Possibly a malformed command execution attempt
    - Not enough space, File too large, No space left on device → Could indicate checks for disk space before writing files
  - [API calls]
    - LoadLibraryExW, LoadLibrary → Dynamic DLL loading, used for

        - both legitimate and malicious code execution
        - GetProcAddress, GetModuleHandleW → Used for resolving API functions dynamically (common in malware to evade detection)

        - QueryPerformanceCounter, QueryPerformanceFrequency → Used for anti-debugging timing checks
        - IsDebuggerPresent → Direct debugger detection
        - RaiseException → Can be used to crash debuggers or handle errors in a controlled manner

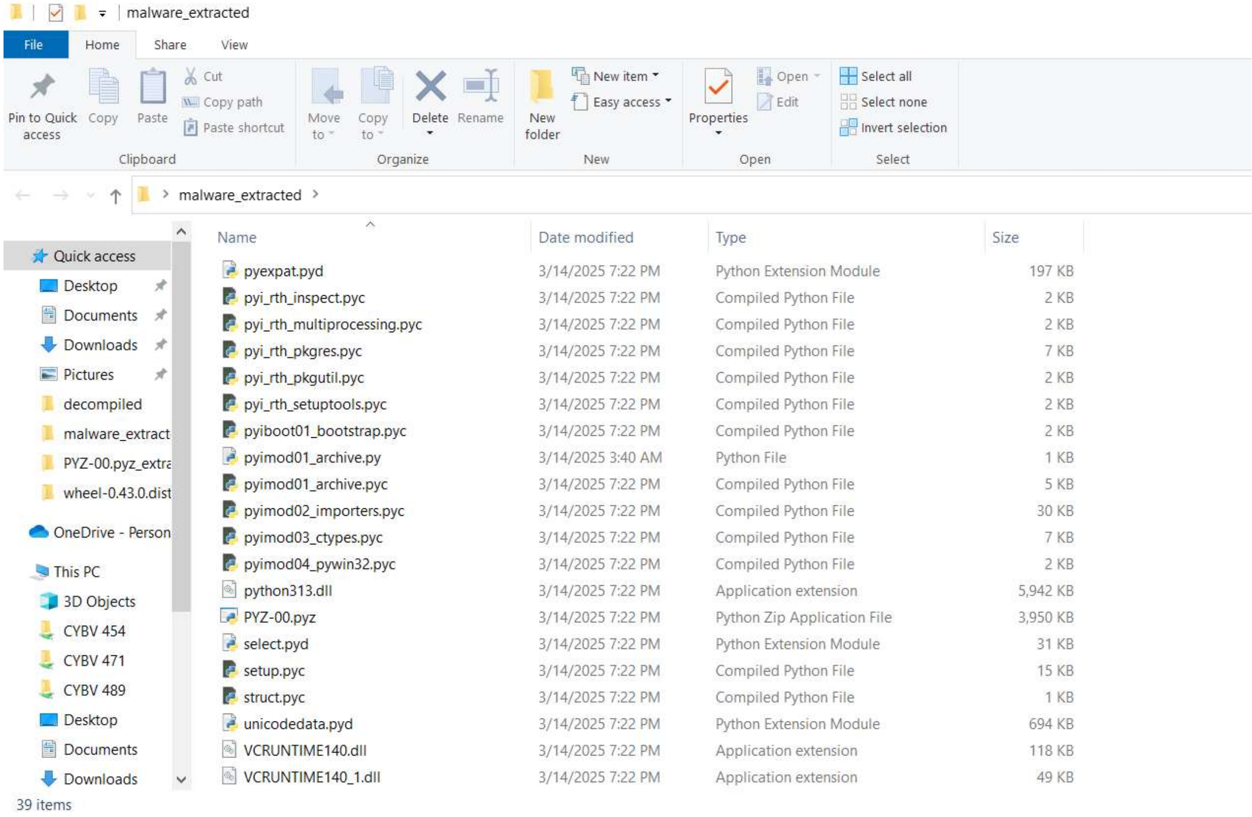
        - CreateFileW, DeleteFileW, FindFirstFileW, FindNextFileW → Indicates file scanning, creation, and deletion capabilities
        - FlushFileBuffers → Can force writes to disk

- Analysis of string findings:
    - [Potential functionality indicated]
        - Based on the API calls and commands found, this executable appears to:
        - Create, read, write, and delete files
        - Manipulate processes, potentially injecting or executing code
        - Check system/network conditions (disk space, network availability)
        - Uses anti-debugging techniques
        - Resolve API calls dynamically (possible evasion technique)
        - Interact with Python (PyInstaller) - Definitely a packed executable
    - [Suspicious patterns]
        - PyInstaller Packing: Multiple references to _MEIPASS, PYZ archive, pyi-runtime-tmpdir, and PyInstallerOnefileHiddenWindow indicate this binary is packaged using PyInstaller. Malware frequently uses PyInstaller to bundle Python scripts into executables, making static analysis harder.
        - Possible Persistence or Privilege Escalation. OpenProcessToken, GetTokenInformation indicate access control manipulation. If paired with registry modifications, this could mean persistence mechanisms
        - Process Injection / Code Execution: LoadLibraryExW, GetProcAddress all indicate the ability to execute code dynamically. If WriteProcessMemory were present, this would confirm process injection
        - File System Interaction. DeleteFileW, WriteFile, FlushFileBuffers could mean log cleaning, wiping evidence, or dropping payloads

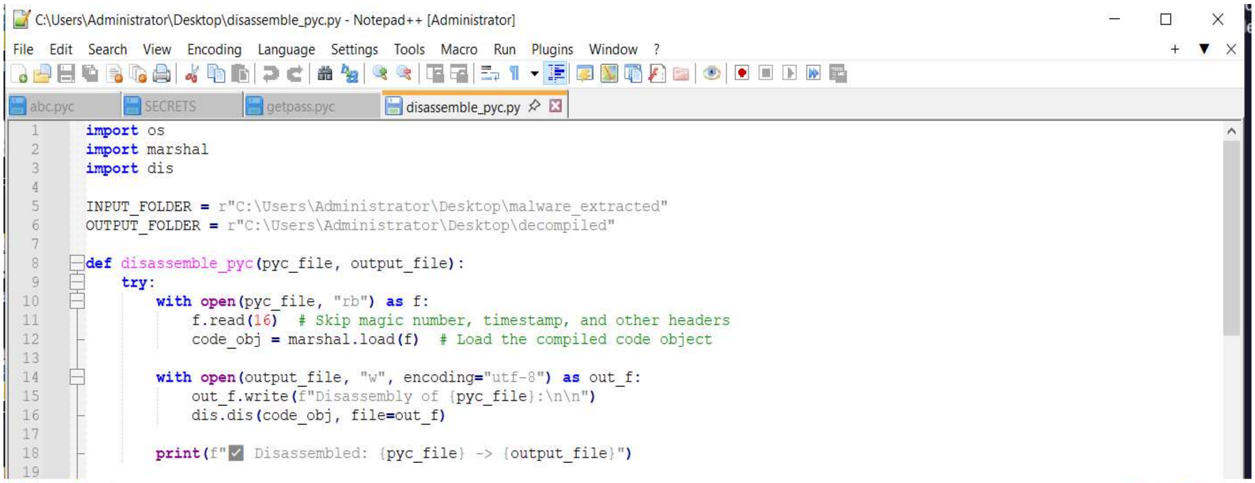
Entropy Analysis

- Overall entropy score: [Score]
    - .19394 (very low)
- Section-specific entropy:
    - [List sections with unusual entropy]
        - .text section: 6.49860

- Packing analysis:
  - [Packed/Unpacked determination]
    - Detect-It-Easy entropy analysis says it is not packed, but in Detect-It-Easy file info it says packed with PyInstaller. I know for sure it is packed, because I unpacked it several times until I had the python bytecode of every .pyc file
  - [Packer identified (if applicable)]
    - PyInstaller
  - [Unpacking methodology (if attempted)]
    - I used pyinstxtractor using Python 3.13 (it was packed with Python 3.13 so I had to use pyinstxtractor with python 3.13) and it successfully unzipped the file, including PYZ-00.pyz, which was not easy and I struggled with PYZ-00.pyz for many hours. I then attempted to decompile all of the .pyc files
  - [Alternative unpacking approaches (if needed)]
    - I could not decompile the .pyc files because all of the tools were not updated enough by their developers to work with Python 3.13, and I needed to use Python 3.13 because that is what it was packed with using PyInstaller. I tried decompyle, uncompyle, decomyple++, and pycdc.

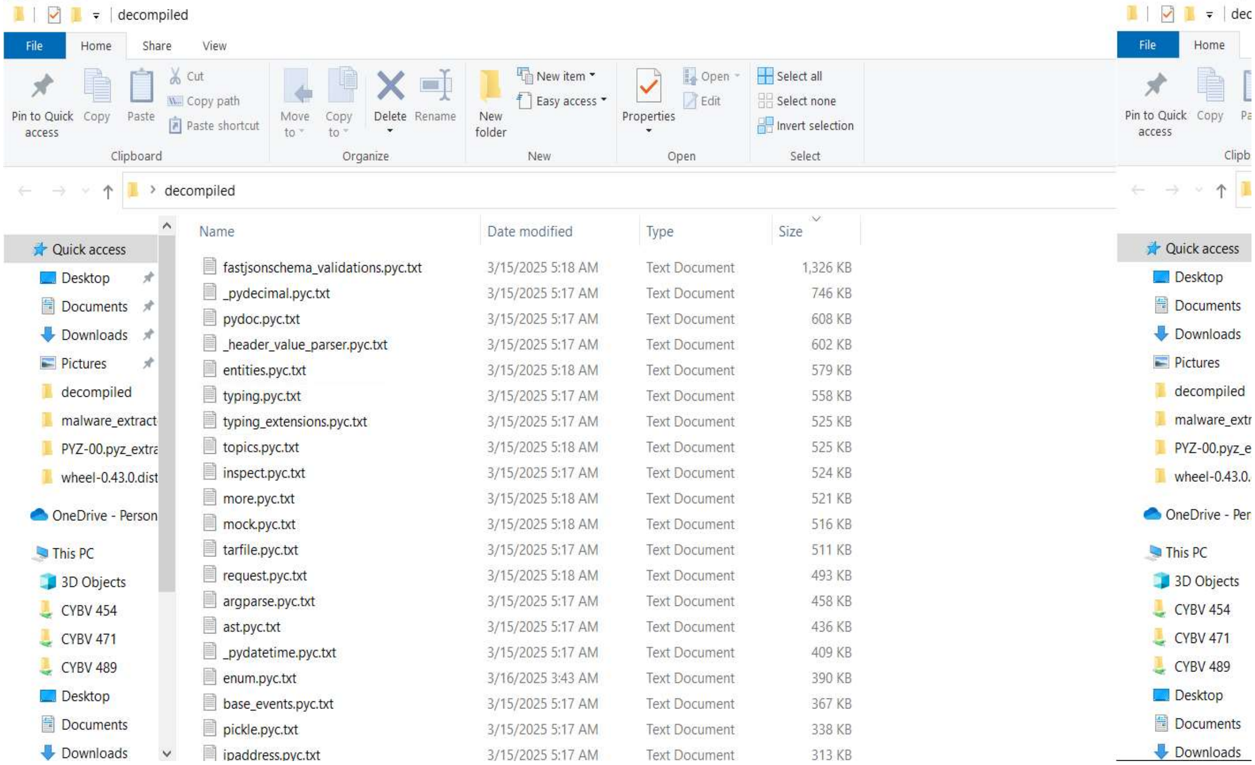


Name	Date modified	Type	Size
pyexpat.pyd	3/14/2025 7:22 PM	Python Extension Module	197 KB
pyi_rth_inspect.pyc	3/14/2025 7:22 PM	Compiled Python File	2 KB
pyi_rth_multiprocessing.pyc	3/14/2025 7:22 PM	Compiled Python File	2 KB
pyi_rth_pkgres.pyc	3/14/2025 7:22 PM	Compiled Python File	7 KB
pyi_rth_pkgutil.pyc	3/14/2025 7:22 PM	Compiled Python File	2 KB
pyi_rth_setuptools.pyc	3/14/2025 7:22 PM	Compiled Python File	2 KB
pyiboot01_bootstrap.pyc	3/14/2025 7:22 PM	Compiled Python File	2 KB
pyimod01_archive.py	3/14/2025 3:40 AM	Python File	1 KB
pyimod01_archive.pyc	3/14/2025 7:22 PM	Compiled Python File	5 KB
pyimod02_importers.pyc	3/14/2025 7:22 PM	Compiled Python File	30 KB
pyimod03_ctypes.pyc	3/14/2025 7:22 PM	Compiled Python File	7 KB
pyimod04_pywin32.pyc	3/14/2025 7:22 PM	Compiled Python File	2 KB
python313.dll	3/14/2025 7:22 PM	Application extension	5,942 KB
PYZ-00.pyz	3/14/2025 7:22 PM	Python Zip Application File	3,950 KB
select.pyd	3/14/2025 7:22 PM	Python Extension Module	31 KB
setup.pyc	3/14/2025 7:22 PM	Compiled Python File	15 KB
struct.pyc	3/14/2025 7:22 PM	Compiled Python File	1 KB
unicodedata.pyd	3/14/2025 7:22 PM	Python Extension Module	694 KB
VCRUNTIME140.dll	3/14/2025 7:22 PM	Application extension	118 KB
VCRUNTIME140_1.dll	3/14/2025 7:22 PM	Application extension	49 KB

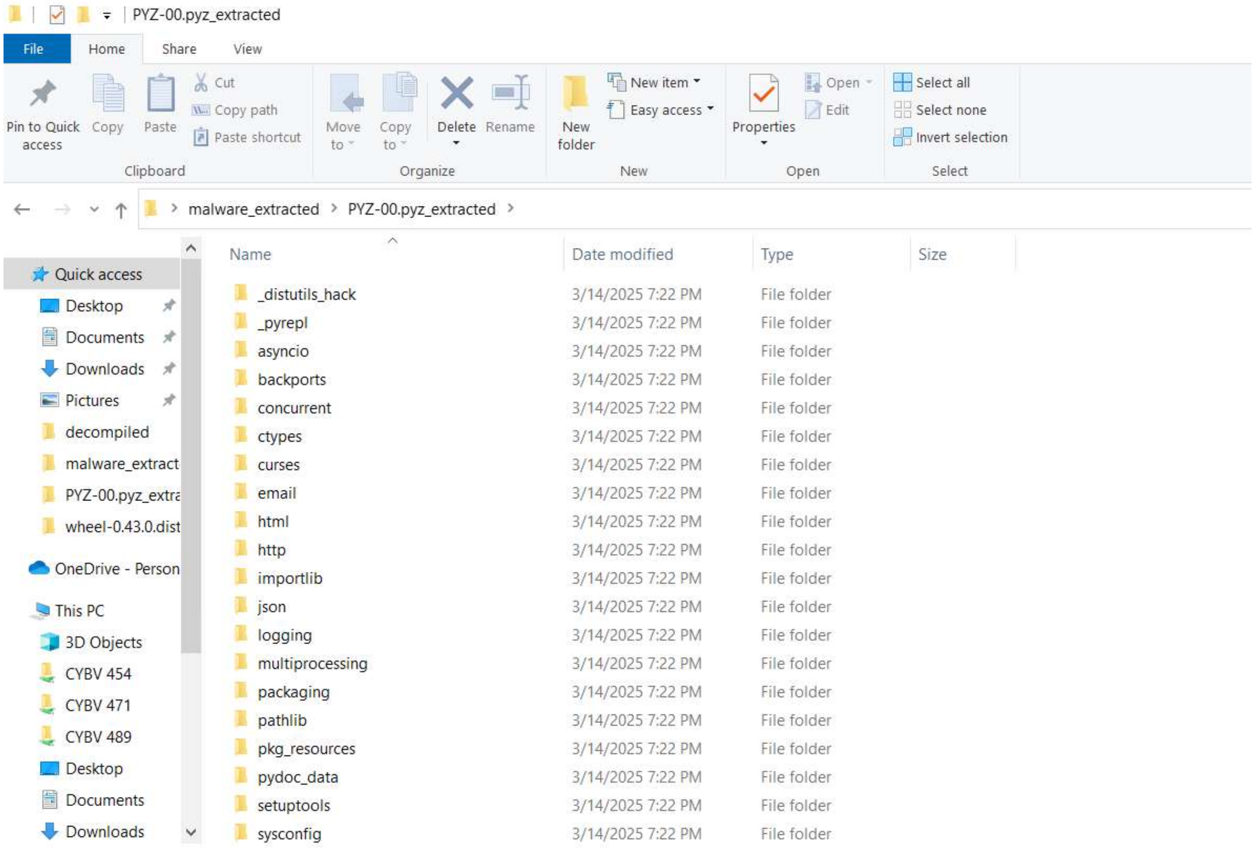


C:\Users\Administrator\Desktop\disassemble_pyc.py - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
abc.pyc
SECRETS
getpass.pyc
disassemble_pyc.py

```python
import os
import marshal
import dis

INPUT_FOLDER = r"C:\Users\Administrator\Desktop\malware_extracted"
OUTPUT_FOLDER = r"C:\Users\Administrator\Desktop\decompiled"

def disassemble_pyc(pyc_file, output_file):
    try:
        with open(pyc_file, "rb") as f:
            f.read(16)  # Skip magic number, timestamp, and other headers
            code_obj = marshal.load(f)  # Load the compiled code object

        with open(output_file, "w", encoding="utf-8") as out_f:
            out_f.write(f"Disassembly of {pyc_file}:\n\n")
            dis.dis(code_obj, file=out_f)

        print(f"✅ Disassembled: {pyc_file} -> {output_file}")

```



Name	Date modified	Type	Size
fastjsonschema_validations.pyc.txt	3/15/2025 5:18 AM	Text Document	1,326 KB
_pydecimal.pyc.txt	3/15/2025 5:17 AM	Text Document	746 KB
pydoc.pyc.txt	3/15/2025 5:17 AM	Text Document	608 KB
_header_value_parser.pyc.txt	3/15/2025 5:17 AM	Text Document	602 KB
entities.pyc.txt	3/15/2025 5:18 AM	Text Document	579 KB
typing.pyc.txt	3/15/2025 5:17 AM	Text Document	558 KB
typing_extensions.pyc.txt	3/15/2025 5:17 AM	Text Document	525 KB
topics.pyc.txt	3/15/2025 5:18 AM	Text Document	525 KB
inspect.pyc.txt	3/15/2025 5:17 AM	Text Document	524 KB
more.pyc.txt	3/15/2025 5:18 AM	Text Document	521 KB
mock.pyc.txt	3/15/2025 5:18 AM	Text Document	516 KB
tarfile.pyc.txt	3/15/2025 5:17 AM	Text Document	511 KB
request.pyc.txt	3/15/2025 5:18 AM	Text Document	493 KB
argparse.pyc.txt	3/15/2025 5:17 AM	Text Document	458 KB
ast.pyc.txt	3/15/2025 5:17 AM	Text Document	436 KB
_pydatetime.pyc.txt	3/15/2025 5:17 AM	Text Document	409 KB
enum.pyc.txt	3/16/2025 3:43 AM	Text Document	390 KB
base_events.pyc.txt	3/15/2025 5:17 AM	Text Document	367 KB
pickle.pyc.txt	3/15/2025 5:17 AM	Text Document	338 KB
ipaddress.pyc.txt	3/15/2025 5:17 AM	Text Document	313 KB



Name	Date modified	Type	Size
_distutils_hack	3/14/2025 7:22 PM	File folder	
_pyrepl	3/14/2025 7:22 PM	File folder	
asyncio	3/14/2025 7:22 PM	File folder	
backports	3/14/2025 7:22 PM	File folder	
concurrent	3/14/2025 7:22 PM	File folder	
ctypes	3/14/2025 7:22 PM	File folder	
curses	3/14/2025 7:22 PM	File folder	
email	3/14/2025 7:22 PM	File folder	
html	3/14/2025 7:22 PM	File folder	
http	3/14/2025 7:22 PM	File folder	
importlib	3/14/2025 7:22 PM	File folder	
json	3/14/2025 7:22 PM	File folder	
logging	3/14/2025 7:22 PM	File folder	
multiprocessing	3/14/2025 7:22 PM	File folder	
packaging	3/14/2025 7:22 PM	File folder	
pathlib	3/14/2025 7:22 PM	File folder	
pkg_resources	3/14/2025 7:22 PM	File folder	
pydoc_data	3/14/2025 7:22 PM	File folder	
setuptools	3/14/2025 7:22 PM	File folder	
sysconfig	3/14/2025 7:22 PM	File folder	

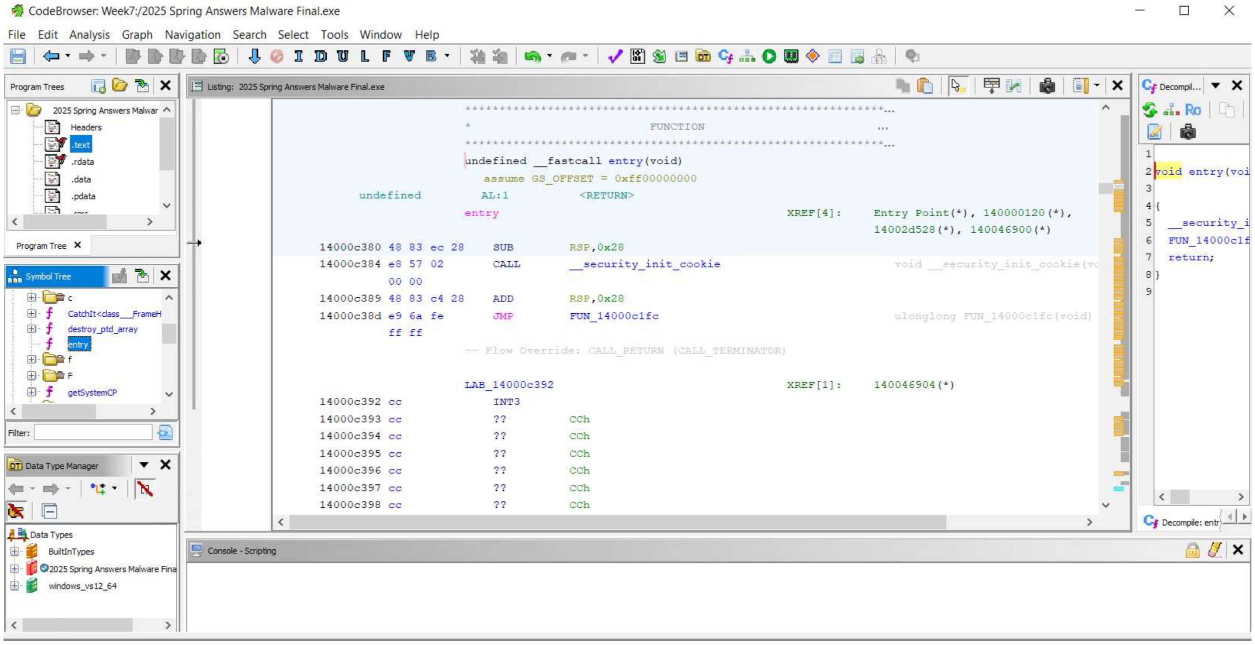
4. Disassembly Analysis using Ghidra

- ENTRY POINT: 14000c380
- Here is an example of a function (screenshot of strcmp function)

strcmp takes two string pointers (_Str1 and _Str2) as arguments.

It compares the characters of the two strings byte-by-byte until it finds a mismatch or reaches a null terminator (\0).

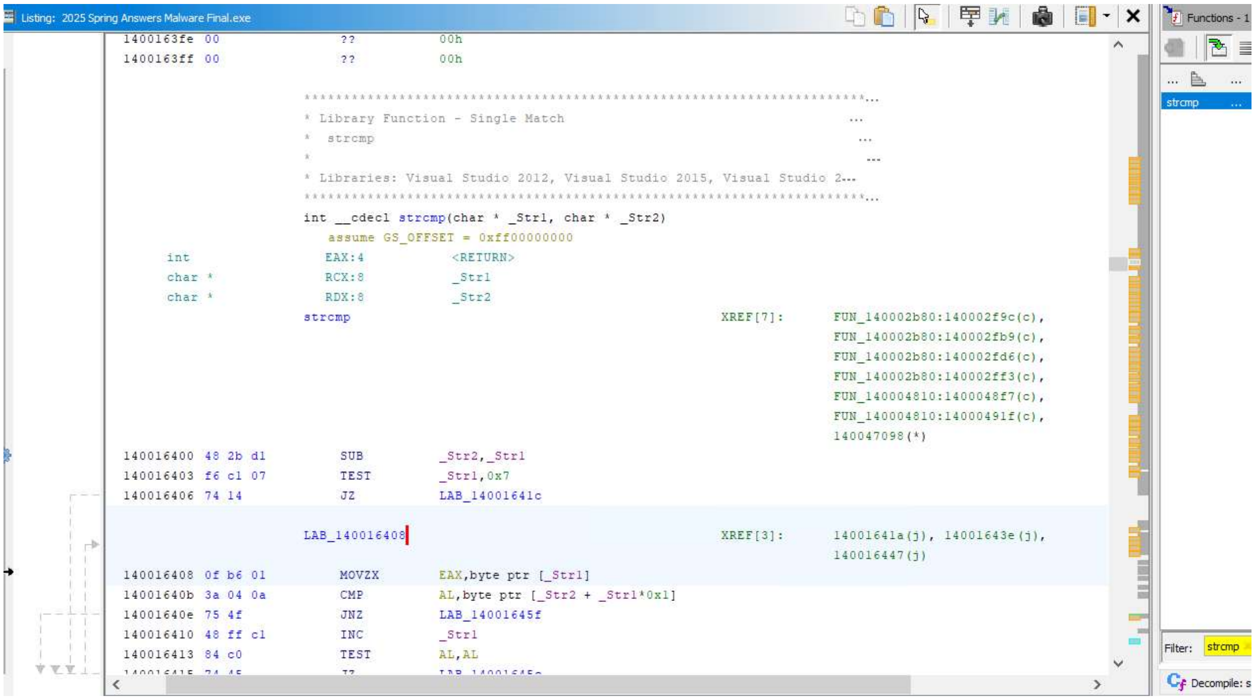
The function returns: 0 if the strings are equal. A negative value if _Str1 is less than _Str2. A positive value if _Str1 is greater than _Str2.



CodeBrowser: Week7:/2025 Spring Answers Malware Final.exe
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
2025 Spring Answers Malwar
Headers
.text
.rdata
.data
.pdata
Program Tree
Symbol Tree
c
CatchIt<class__FrameH
destroy_ptd_array
entry
f
F
getSystemCP
Filter:
Data Type Manager
Data Types
BuiltInTypes
2025 Spring Answers Malware Fina
windows_vs12_64
Listing: 2025 Spring Answers Malware Final.exe
Console - Scripting
Decompil...
Decompile: entr

```
                         ****************************************************************...
                         *                          FUNCTION                              ...
                         ****************************************************************...
                         undefined __fastcall entry(void)
                           assume GS_OFFSET = 0xff00000000
         undefined         AL:1          <RETURN>
                         entry                                   XREF[4]:     Entry Point(*), 140000120(*),
                                                                              14002d528(*), 140046900(*)
    14000c380 48 83 ec 28     SUB        RSP,0x28
    14000c384 e8 57 02        CALL       __security_init_cookie                          void __security_init_cookie(vo
              00 00
    14000c389 48 83 c4 28     ADD        RSP,0x28
    14000c38d e9 6a fe        JMP        FUN_14000c1fc                                   ulonglong FUN_14000c1fc(void)
              ff ff
                         -- Flow Override: CALL_RETURN (CALL_TERMINATOR)

                         LAB_14000c392                           XREF[1]:     140046904(*)
    14000c392 cc              INT3
    14000c393 cc              ??         CCh
    14000c394 cc              ??         CCh
    14000c395 cc              ??         CCh
    14000c396 cc              ??         CCh
    14000c397 cc              ??         CCh
    14000c398 cc              ??         CCh
```

```
void entry(voi
{
  __security_i
  FUN_14000c1f
  return;
}
```



```
    1400163fe 00              ??         00h
    1400163ff 00              ??         00h

                         ****************************************************************...
                         * Library Function - Single Match                               ...
                         *  strcmp                                                       ...
                         *                                                               ...
                         * Libraries: Visual Studio 2012, Visual Studio 2015, Visual Studio 2...
                         ****************************************************************...
                         int __cdecl strcmp(char * _Str1, char * _Str2)
                           assume GS_OFFSET = 0xff00000000
         int               EAX:4          <RETURN>
         char *            RCX:8          _Str1
         char *            RDX:8          _Str2
                         strcmp                                  XREF[7]:     FUN_140002b80:140002f9c(c),
                                                                              FUN_140002b80:140002fb9(c),
                                                                              FUN_140002b80:140002fd6(c),
                                                                              FUN_140002b80:140002ff3(c),
                                                                              FUN_140004810:1400048f7(c),
                                                                              FUN_140004810:14000491f(c),
                                                                              140047098(*)
    140016400 48 2b d1        SUB        _Str2,_Str1
    140016403 f6 c1 07        TEST       _Str1,0x7
    140016406 74 14           JZ         LAB_14001641c

                         LAB_140016408                           XREF[3]:     14001641a(j), 14001643e(j),
                                                                              140016447(j)
    140016408 0f b6 01        MOVZX      EAX,byte ptr [_Str1]
    14001640b 3a 04 0a        CMP        AL,byte ptr [_Str2 + _Str1*0x1]
    14001640e 75 4f           JNZ        LAB_14001645f
    140016410 48 ff c1        INC        _Str1
    140016413 84 c0           TEST       AL,AL
```

4. Static Analysis Summary

Key findings from static analysis:

- packed with pyinstaller (python 3.13): the executable was identified as a pyinstaller-packed file, requiring manual unpacking and disassembly.
- right-to-left override (RLO) trick: the filename contained an invalid character using U+202E, a technique often used to disguise malicious files by reversing the displayed name.
- virustotal detection: initially undetected, but after proper extraction and recompression, flagged as malicious by 2 out of 61 vendors.

Potential anti-analysis techniques:

- QueryPerformanceCounter & QueryPerformanceFrequency: likely used for anti-debugging by measuring execution delays.
- IsDebuggerPresent: direct debugger detection API call.
- RaiseException: potential debugger disruption technique.

File system & process manipulation:

- CreateFileW, DeleteFileW, FindFirstFileW, FindNextFileW: suggests file interaction capabilities.
- OpenProcessToken, GetTokenInformation: could indicate privilege escalation or security token access.
- LoadLibraryExW, GetProcAddress: common indicators of dynamic code execution and possible process injection.

Network-related strings: presence of strings such as "network unreachable" and "connection reset" suggests network communication capabilities.

Potential functionality:

- evasion & anti-analysis: uses pyinstaller packing, RLO trick, and anti-debugging techniques to avoid detection.
- persistence & privilege escalation: access token manipulation and potential registry modifications.
- file system & process interaction: ability to create, delete, and manipulate files, possibly for data exfiltration or self-propagation.
- network communication: could establish remote connections, possibly for command-and-control (C2) communication.

Risk indicators:

- obfuscation & packing: presence of pyinstaller packing and right-to-left override suggests intentional concealment.
- anti-analysis techniques: includes debugger detection and execution timing checks.
- potential for code injection & execution: use of LoadLibraryExW, and GetProcAddress is common in malware used for injecting malicious payloads.
- file & network manipulation: includes API calls for file deletion, process manipulation, and network interactions, suggesting possible data theft or malware propagation.

Dynamic Analysis

1. Analysis Environment

Environment Setup

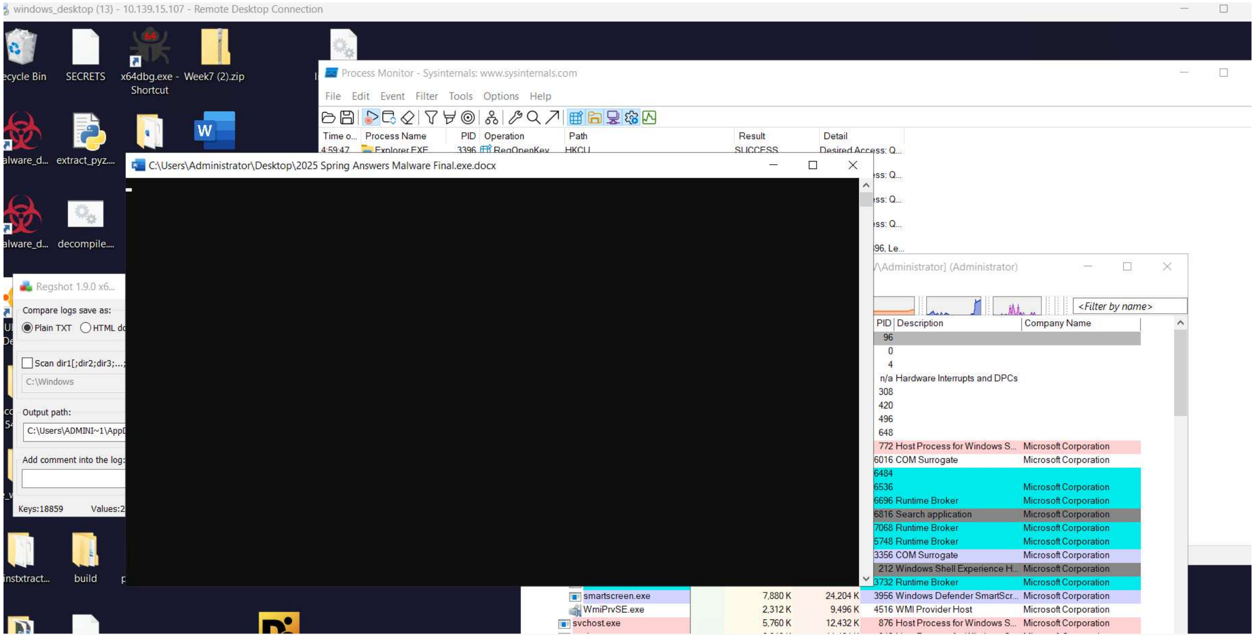
- Virtual Machine specifications:

  - [OS version] Microsoft Windows 2022 Datacenter
  - [Memory allocation] 8GB
  - [Network configuration] Connected to UA network
- Monitoring tools deployed:
  - [Process monitoring]
    - Ensure you use RegShot, Process Monitor, Process Explorer
    - I used RegShot
    - I used Process Monitor
    - I used Process Explorer
  - [Network monitoring]
    - Ensure you use Wireshark
    - I used Wireshark
  - [File system monitoring]
- Safety measures implemented:
  - [Network isolation]
    - Try the analysis with and without Fakenet
    - Used Cyberapolis virtual machine
  - [Snapshot configuration]
    - Reset VM after using
  - [Additional protections]

2. Runtime Observations

Initial Execution

- [Immediate system changes]
  - Cmd shell window opened
- [Process creation]
  - ReadFile
  - WriteFile
  - Loads Python Modules
  - slui.exe
  - 2025 Spring Answers Malware Final.xcod.exe
- [Registry creation]
  - Keys deleted: 1
  - Keys added: 7
  - Values deleted: 2
  - Values added: 122
  - Values modified: 452
  - Total changes: 584
- [Network activity]
  - 20.103.156.88
  - 192.168.100.93
  - 20.190.160.4
  - 40.113.103.199
  - 184.30.131.245
  - HTTP/1.1
    ```
    Connection: Keep-Alive
    Accept: */*
    User-Agent: Microsoft-CryptoAPI/10.0
    Host: ocsp.digicert.com
    ```
- [File system changes]
  - CreateFile
  - CloseFile
  - QueryDirectory
  - ThreadExit
  - ProcessExit



windows_desktop (13) - 10.139.15.107 - Remote Desktop Connection

Process Monitor - Sysinternals: www.sysinternals.com

```
Time o...  Process Name   PID   Operation    Path    Result    Detail
4:59:47    Explorer.EXE   3396  RegOpenKey   HKCU    SUCCESS   Desired Access: Q...
                                                               ss: Q...
                                                               ss: Q...
                                                               ss: Q...
                                                               96, Le...
```

C:\Users\Administrator\Desktop\2025 Spring Answers Malware Final.exe.docx

Regshot 1.9.0 x6...

Compare logs save as:
● Plain TXT ○ HTML do

□ Scan dir1[;dir2;dir3;...;

C:\Windows

Output path:
C:\Users\ADMINI~1\AppD

Add comment into the log:

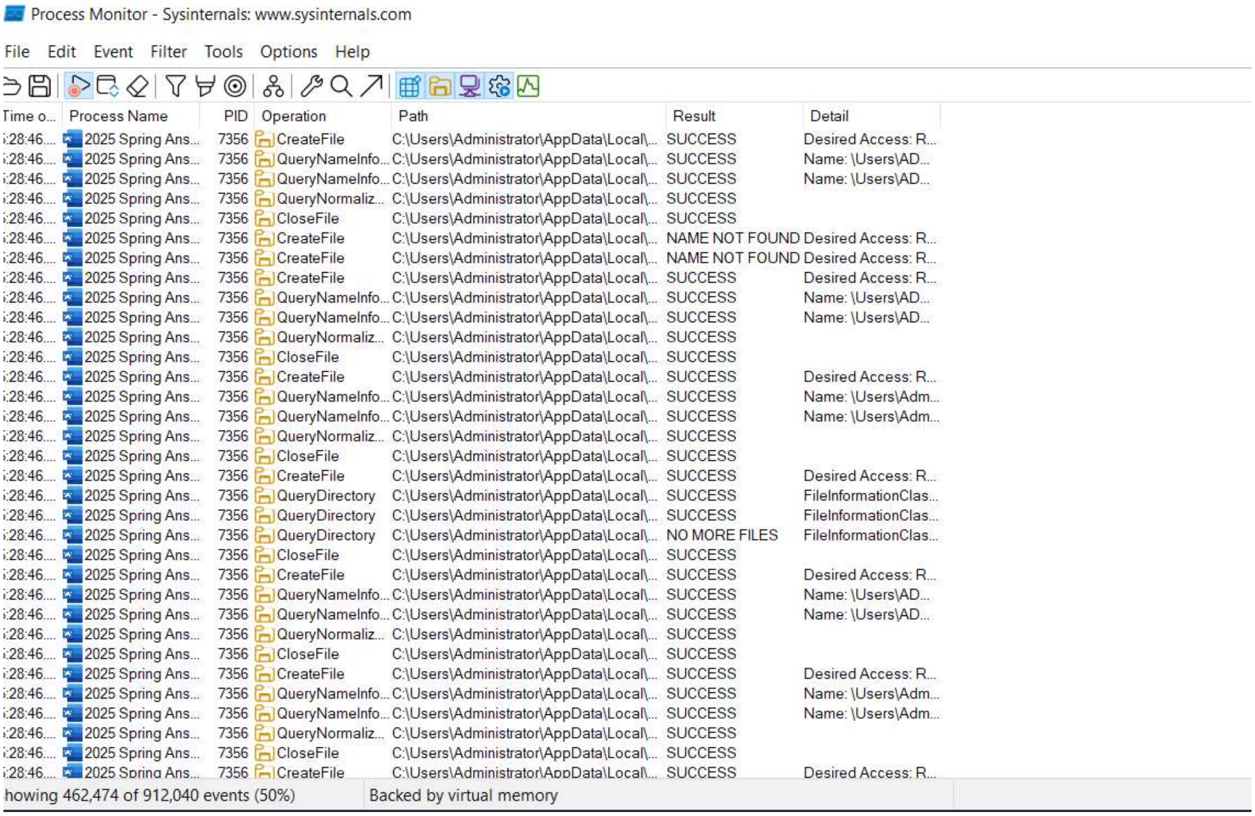
Keys:18859   Values:2

\Administrator] (Administrator)

<Filter by name>

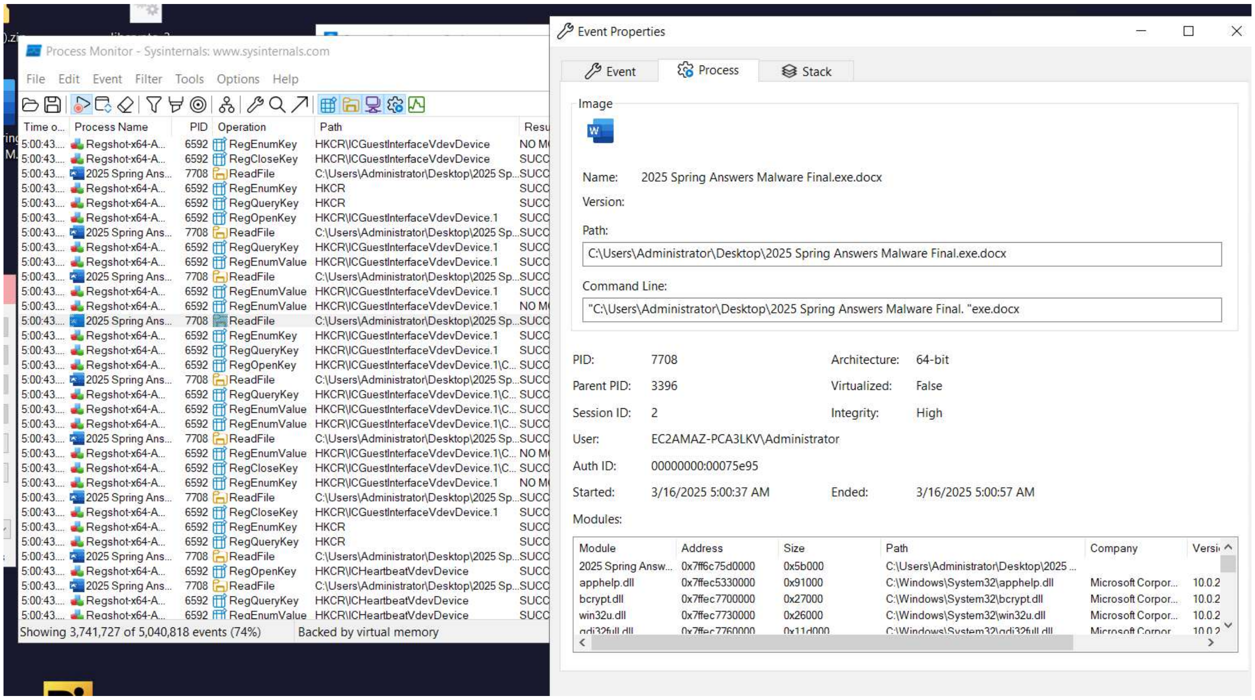
```
PID  Description                      Company Name
  96
   0
   4
 n/a Hardware Interrupts and DPCs
 308
 420
 496
 648
 772 Host Process for Windows S...    Microsoft Corporation
6016 COM Surrogate                    Microsoft Corporation
6484
6536                                  Microsoft Corporation
6696 Runtime Broker                   Microsoft Corporation
6816 Search application               Microsoft Corporation
7068 Runtime Broker                   Microsoft Corporation
5748 Runtime Broker                   Microsoft Corporation
3356 COM Surrogate                    Microsoft Corporation
 212 Windows Shell Experience H...    Microsoft Corporation
3732 Runtime Broker                   Microsoft Corporation
```

```
smartscreen.exe   7,880 K   24,204 K   3956 Windows Defender SmartScr...   Microsoft Corporation
WmiPrvSE.exe      2,312 K    9,496 K   4516 WMI Provider Host              Microsoft Corporation
svchost.exe       5,760 K   12,432 K    876 Host Process for Windows S...  Microsoft Corporation
```



Process Monitor - Sysinternals: www.sysinternals.com

```
Time o...  Process Name      PID   Operation         Path                                      Result           Detail
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\AD...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\AD...
:28:46...  2025 Spring Ans...  7356  QueryNormaliz...  C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CloseFile         C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  NAME NOT FOUND   Desired Access: R...
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  NAME NOT FOUND   Desired Access: R...
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\AD...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\AD...
:28:46...  2025 Spring Ans...  7356  QueryNormaliz...  C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CloseFile         C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\Adm...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\Adm...
:28:46...  2025 Spring Ans...  7356  QueryNormaliz...  C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CloseFile         C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
:28:46...  2025 Spring Ans...  7356  QueryDirectory    C:\Users\Administrator\AppData\Local\...  SUCCESS          FileInformationClas...
:28:46...  2025 Spring Ans...  7356  QueryDirectory    C:\Users\Administrator\AppData\Local\...  SUCCESS          FileInformationClas...
:28:46...  2025 Spring Ans...  7356  QueryDirectory    C:\Users\Administrator\AppData\Local\...  NO MORE FILES    FileInformationClas...
:28:46...  2025 Spring Ans...  7356  CloseFile         C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\AD...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\AD...
:28:46...  2025 Spring Ans...  7356  QueryNormaliz...  C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CloseFile         C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\Adm...
:28:46...  2025 Spring Ans...  7356  QueryNameInfo...  C:\Users\Administrator\AppData\Local\...  SUCCESS          Name: \Users\Adm...
:28:46...  2025 Spring Ans...  7356  QueryNormaliz...  C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CloseFile         C:\Users\Administrator\AppData\Local\...  SUCCESS
:28:46...  2025 Spring Ans...  7356  CreateFile        C:\Users\Administrator\AppData\Local\...  SUCCESS          Desired Access: R...
howing 462,474 of 912,040 events (50%)      Backed by virtual memory
```



Process Monitor - Sysinternals: www.sysinternals.com

Time o...	Process Name	PID	Operation	Path	Resu
5:00:43....	Regshot-x64-A...	6592	RegEnumKey	HKCR\ICGuestInterfaceVdevDevice	NO M
5:00:43....	Regshot-x64-A...	6592	RegCloseKey	HKCR\ICGuestInterfaceVdevDevice	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumKey	HKCR	SUCC
5:00:43....	Regshot-x64-A...	6592	RegQueryKey	HKCR	SUCC
5:00:43....	Regshot-x64-A...	6592	RegOpenKey	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegQueryKey	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICGuestInterfaceVdevDevice.1	NO M
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumKey	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	Regshot-x64-A...	6592	RegQueryKey	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	Regshot-x64-A...	6592	RegOpenKey	HKCR\ICGuestInterfaceVdevDevice.1\C...	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegQueryKey	HKCR\ICGuestInterfaceVdevDevice.1\C...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICGuestInterfaceVdevDevice.1\C...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICGuestInterfaceVdevDevice.1\C...	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICGuestInterfaceVdevDevice.1\C...	NO M
5:00:43....	Regshot-x64-A...	6592	RegCloseKey	HKCR\ICGuestInterfaceVdevDevice.1\C...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumKey	HKCR\ICGuestInterfaceVdevDevice.1	NO M
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegCloseKey	HKCR\ICGuestInterfaceVdevDevice.1	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumKey	HKCR	SUCC
5:00:43....	Regshot-x64-A...	6592	RegQueryKey	HKCR	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegOpenKey	HKCR\ICHeartbeatVdevDevice	SUCC
5:00:43....	2025 Spring Ans...	7708	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCC
5:00:43....	Regshot-x64-A...	6592	RegQueryKey	HKCR\ICHeartbeatVdevDevice	SUCC
5:00:43....	Regshot-x64-A...	6592	RegEnumValue	HKCR\ICHeartbeatVdevDevice	SUCC

Showing 3,741,727 of 5,040,818 events (74%)   Backed by virtual memory

Event Properties

Image

Name: 2025 Spring Answers Malware Final.exe.docx

Version:

Path:

C:\Users\Administrator\Desktop\2025 Spring Answers Malware Final.exe.docx

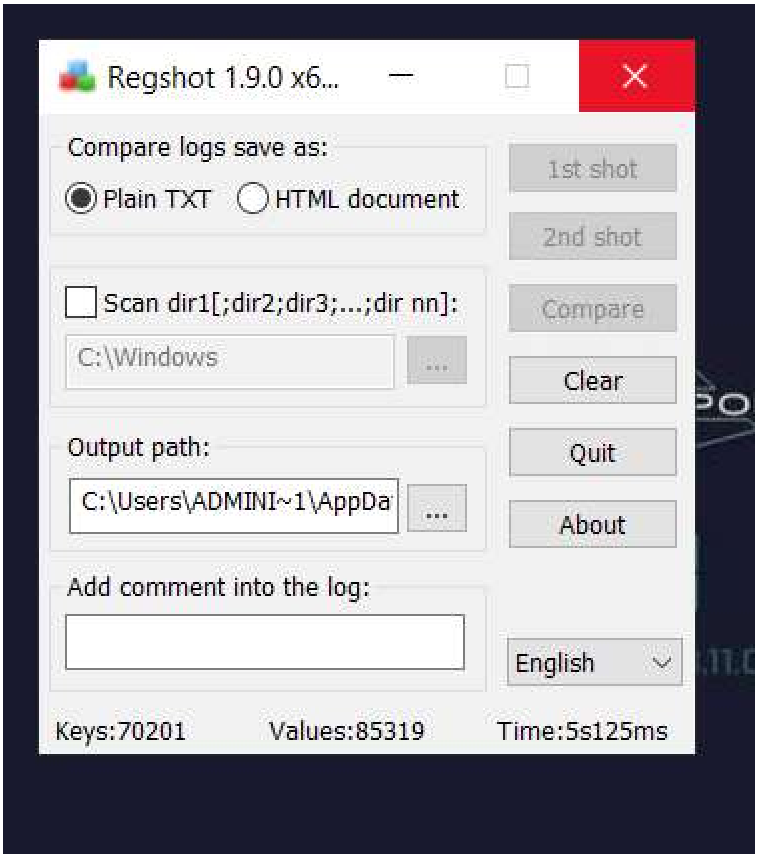
Command Line:

"C:\Users\Administrator\Desktop\2025 Spring Answers Malware Final. "exe.docx

PID:	7708	Architecture:	64-bit
Parent PID:	3396	Virtualized:	False
Session ID:	2	Integrity:	High
User:	EC2AMAZ-PCA3LKV\Administrator		
Auth ID:	00000000:00075e95		
Started:	3/16/2025 5:00:37 AM	Ended:	3/16/2025 5:00:57 AM

Modules:

Module	Address	Size	Path	Company	Versi
2025 Spring Answ...	0x7ff6c75d0000	0x5b000	C:\Users\Administrator\Desktop\2025 ...		
apphelp.dll	0x7ffec5330000	0x91000	C:\Windows\System32\apphelp.dll	Microsoft Corpor...	10.0.2
bcrypt.dll	0x7ffec7700000	0x27000	C:\Windows\System32\bcrypt.dll	Microsoft Corpor...	10.0.2
win32u.dll	0x7ffec7730000	0x26000	C:\Windows\System32\win32u.dll	Microsoft Corpor...	10.0.2
gdi32full.dll	0x7ffec7760000	0x11d000	C:\Windows\System32\gdi32full.dll	Microsoft Corpor...	10.0.2



Regshot 1.9.0 x6...

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

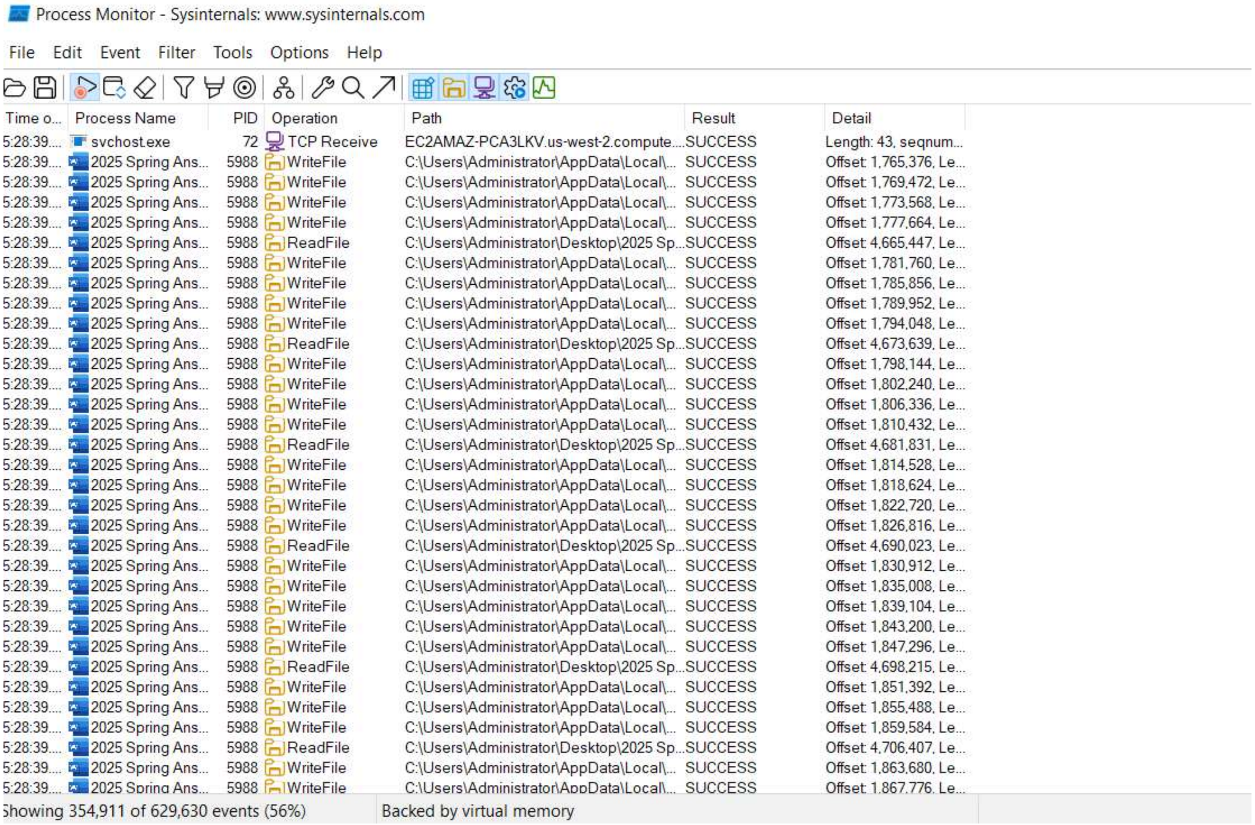
C:\Windows

Output path:

C:\Users\ADMINI~1\AppDa

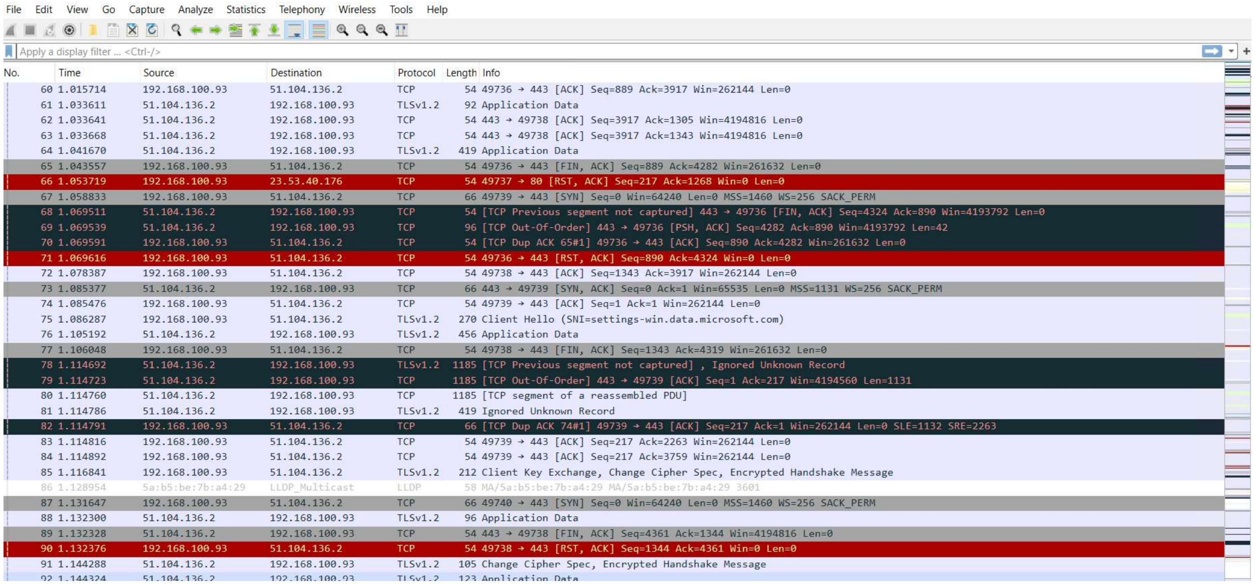
Add comment into the log:

Keys:70201 Values:85319 Time:5s125ms


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
5:28:39....	svchost.exe	72	TCP Receive	EC2AMAZ-PCA3LKV.us-west-2.compute....	SUCCESS	Length: 43, seqnum...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,765,376, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,769,472, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,773,568, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,777,664, Le...
5:28:39....	2025 Spring Ans...	5988	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCCESS	Offset: 4,665,447, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,781,760, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,785,856, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,789,952, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,794,048, Le...
5:28:39....	2025 Spring Ans...	5988	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCCESS	Offset: 4,673,639, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,798,144, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,802,240, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,806,336, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,810,432, Le...
5:28:39....	2025 Spring Ans...	5988	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCCESS	Offset: 4,681,831, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,814,528, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,818,624, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,822,720, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,826,816, Le...
5:28:39....	2025 Spring Ans...	5988	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCCESS	Offset: 4,690,023, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,830,912, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,835,008, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,839,104, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,843,200, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,847,296, Le...
5:28:39....	2025 Spring Ans...	5988	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCCESS	Offset: 4,698,215, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,851,392, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,855,488, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,859,584, Le...
5:28:39....	2025 Spring Ans...	5988	ReadFile	C:\Users\Administrator\Desktop\2025 Sp...	SUCCESS	Offset: 4,706,407, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,863,680, Le...
5:28:39....	2025 Spring Ans...	5988	WriteFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Offset: 1,867,776, Le...

Showing 354,911 of 629,630 events (56%) Backed by virtual memory


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
60	1.015714	192.168.100.93	51.104.136.2	TCP	54	49736 → 443 [ACK] Seq=889 Ack=3917 Win=262144 Len=0
61	1.033611	51.104.136.2	192.168.100.93	TLSv1.2	92	Application Data
62	1.033641	51.104.136.2	192.168.100.93	TCP	54	443 → 49738 [ACK] Seq=3917 Ack=1305 Win=4194816 Len=0
63	1.033668	51.104.136.2	192.168.100.93	TCP	54	443 → 49738 [ACK] Seq=3917 Ack=1343 Win=4194816 Len=0
64	1.041670	51.104.136.2	192.168.100.93	TLSv1.2	419	Application Data
65	1.043557	192.168.100.93	51.104.136.2	TCP	54	49736 → 443 [FIN, ACK] Seq=889 Ack=4282 Win=261632 Len=0
66	1.053719	192.168.100.93	23.53.40.176	TCP	54	49737 → 80 [RST, ACK] Seq=217 Ack=1268 Win=0 Len=0
67	1.058833	192.168.100.93	51.104.136.2	TCP	66	49739 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
68	1.069511	51.104.136.2	192.168.100.93	TCP	54	[TCP Previous segment not captured] 443 → 49736 [FIN, ACK] Seq=4324 Ack=890 Win=4193792 Len=0
69	1.069539	51.104.136.2	192.168.100.93	TCP	96	[TCP Out-Of-Order] 443 → 49736 [PSH, ACK] Seq=4282 Ack=890 Win=4193792 Len=42
70	1.069591	192.168.100.93	51.104.136.2	TCP	54	[TCP Dup ACK 65#1] 49736 → 443 [ACK] Seq=890 Ack=4282 Win=261632 Len=0
71	1.069616	192.168.100.93	51.104.136.2	TCP	54	49736 → 443 [RST, ACK] Seq=890 Ack=4324 Win=0 Len=0
72	1.078387	192.168.100.93	51.104.136.2	TCP	54	49738 → 443 [ACK] Seq=1343 Ack=3917 Win=262144 Len=0
73	1.085377	51.104.136.2	192.168.100.93	TCP	66	443 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1131 WS=256 SACK_PERM
74	1.085476	192.168.100.93	51.104.136.2	TCP	54	49739 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
75	1.086287	192.168.100.93	51.104.136.2	TLSv1.2	270	Client Hello (SNI=settings-win.data.microsoft.com)
76	1.105192	51.104.136.2	192.168.100.93	TLSv1.2	456	Application Data
77	1.106048	192.168.100.93	51.104.136.2	TCP	54	49738 → 443 [FIN, ACK] Seq=1343 Ack=4319 Win=261632 Len=0
78	1.114692	51.104.136.2	192.168.100.93	TLSv1.2	1185	[TCP Previous segment not captured] , Ignored Unknown Record
79	1.114723	51.104.136.2	192.168.100.93	TCP	1185	[TCP Out-Of-Order] 443 → 49739 [ACK] Seq=1 Ack=217 Win=4194560 Len=1131
80	1.114760	51.104.136.2	192.168.100.93	TCP	1185	[TCP segment of a reassembled PDU]
81	1.114786	51.104.136.2	192.168.100.93	TLSv1.2	419	Ignored Unknown Record
82	1.114791	192.168.100.93	51.104.136.2	TCP	66	[TCP Dup ACK 74#1] 49739 → 443 [ACK] Seq=217 Ack=1 Win=262144 Len=0 SLE=1132 SRE=2263
83	1.114816	192.168.100.93	51.104.136.2	TCP	54	49739 → 443 [ACK] Seq=217 Ack=2263 Win=262144 Len=0
84	1.114892	192.168.100.93	51.104.136.2	TCP	54	49739 → 443 [ACK] Seq=217 Ack=3759 Win=262144 Len=0
85	1.116841	192.168.100.93	51.104.136.2	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
86	1.128954	5a:b5:be:7b:a4:29	LLDP_Multicast	LLDP	58	MA/5a:b5:be:7b:a4:29 MA/5a:b5:be:7b:a4:29 3601
87	1.131647	192.168.100.93	51.104.136.2	TCP	66	49740 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
88	1.132300	51.104.136.2	192.168.100.93	TLSv1.2	96	Application Data
89	1.132328	51.104.136.2	192.168.100.93	TCP	54	443 → 49738 [FIN, ACK] Seq=4361 Ack=1344 Win=4194816 Len=0
90	1.132376	192.168.100.93	51.104.136.2	TCP	54	49738 → 443 [RST, ACK] Seq=1344 Ack=4361 Win=0 Len=0
91	1.144288	51.104.136.2	192.168.100.93	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
92	1.144324	51.104.136.2	192.168.100.93	TLSv1.2	123	Application Data

Continued Monitoring

- Persistent changes: Registry modifications and file system changes
- Scheduled tasks: No evidence of scheduled tasks was observed
- Registry modifications:
  - 7 new registry keys added
  - 122 values added, 452 values modified
  - Possible persistence via registry changes

Post-Execution Analysis

System State Changes

- Permanent modifications: Registry and system altered
- Persistence mechanisms: Potential persistence via registry key modifications.
- Data exfiltration evidence:
- Network activity observed
- Potential exfiltration to external IPs

Network Activity Summary

- Connection attempts: Outbound connections to multiple IPs.
- Data transfers: Possible HTTP requests to external servers.
- Command & Control activity: No definitive evidence, however outbound connections suggest potential C2 communication.

Impact Analysis

1. User Impact Assessment

Home Users

- Potential impact: Data theft, compromised system integrity.
- Risk level: Moderate to high.
- Data compromise potential: Risk of credential theft, spyware, or unauthorized access.

Business Users

- Operational impact: damage business operations.
- Data security concerns: covert access to sensitive files and data exfiltration risks.
- Financial implications: data breach costs, and reputational damage.

Government Users

- Security implications: Threat to national security if this malware runs in government networks.
- Data sensitivity concerns: Possible exposure of classified or sensitive government data.
- Operational disruption potential: Could impact essential services.

2. Mitigation Strategy

Immediate Response

- Initial containment steps:
  - Isolate infected systems from the network.
- System isolation procedures:
  - Disable network access
- Data preservation methods:
  - Collect evidence using memory dumps and registry snapshots.

Long-term Prevention

- Security control recommendations:
  - Monitor for unusual network traffic.
- Policy modifications:
  - Save regular backups, snapshots, and system restore points
  - stricter file execution policies.
- Training requirements:
  - Educate employees on phishing risks and malware infection vectors.

Conclusion

1. Analysis Reflection

- Summary of findings:
  - Malware packed with PyInstaller using Python 3.13.
  - Uses RLO trick consistent with malware family from VirusTotal
  - Potentially capable of persistence and privilege escalation.
  - Suspicious network activity, but not confirmed
- Unusual characteristics:
  - Right-to-Left Override (RLO) obfuscation technique.
  - Python-based malware packed by PyInstaller
- Learning outcomes:
  - Importance of unpacking PyInstaller executables correctly.
  - Anti-debugging techniques can slow down analysis.
  - Thinking outside the box, compressing malware instead of unzipping (even though I did both)
- Additional research needed:
  - packet inspection for exfiltration

2. Evidence Documentation

- Screenshot descriptions and relevance:
- Tool output documentation:
  - Ghidra, Detect-It-Easy, pyinstxtractor, 7z, procmon, process explorer, wireshark
- Additional supporting materials:
  - Network packet capture logs from Wireshark.
  - Static analysis breakdown from Detect-It-Easy.

Discussion Post 7

First I changed the name of “2025SpringAnswersMalwareFinal.exe.docx” to “malware”. Then I used pyinstxtractor using Python version 3.13 to extract files from “malware” to a folder on my desktop “malware_extracted”. Originally, I ran into a problem trying to unzip PYZ-00.pyz, but using python version 3.13 fixed the problem and unzipped the .pyz files correctly. I then tried many approaches to convert all of the .pyc files to .py files using decompyle3, decompyle++, uncompyle3, and pycdc. None of these approaches worked, because the files were zipped using Python 3.13, and none of those tools were updated to be able to decompile files compiled with python 3.13. So I did the best I could, and I wrote a python script to disassemble all of the .pyc files and output .txt files with python bytecode. All of this took a really long time but I finally extracted everything and could find useful information from the bytecode! It feels like I succeeded.
As for VirusTotal, I searched for all of the executables in the malware_extracted folder and it showed 0 .exe files and 6 .dll files. I ran all of the .dll files in VirusTotal and one of them showed up as having a bad community score, so I started to do my analysis with that one suspicious .dll file, which is called libcrypto-3.dll.
EDIT: after doing an entire detailed static analysis report on libcrypto-3.dll, I determined libcrypto-3.dll to be an OpenSSL cryptographic library and that it is NOT malicious. So I started over with a different approach.

After determining that libcrypto-3.dll is a OpenSSL cryptographic library, I decided to do the rest of the analysis for the malware: “2025SpringAnswersMalwareFinal.exe.docx” since I spent so much time unpacking it and this does not seem like the correct file after this much static analysis.

Then I thought, maybe I should do something different. I decided to unzip the “2025SpringAnswersMalwareFinal.exe.docx” file with the password: SpringBreakBestBreak2025, and then recompress it without a password, and then upload it to VirusTotal. Now I am going to start the analysis again because after uploading the compressed file to VirusTotal, it is flagged by vendors as malicious! Maybe this is the correct answer! Whew! Time to start over and do this report again!