

# Malware Analysis – Annabelle Ransomware (.NET)

---

All analysis was performed inside an isolated FLARE VM. Annabelle.exe was used to perform analysis from given github link 4. [Malware-Samples Repository](#).

**Summary :** I analyzed annabelle.exe which is a windows executable.

Static analysis shows it is a .NET application that includes references to common .NET libraries and crypto APIs .

Dynamic logs in Procmon show the binary reads system DLLs and attempts to interact with the local file system and .NET runtime components.

Network capture in Wireshark shows no external C2 communications during the run only normal local network announcements.

Regshot comparison indicates the sample **modified system policy settings** and **added persistence via a Run key** . It also set multiple policy values that disable security tools . These registry changes, together with the encryption related code, strongly indicate malicious intent .

The sample should be considered potentially privacy invasive and capable of performing file operations and cryptographic routines.

## 1. Environment & methodology

All work of analysis was performed inside a dedicated FLARE VM with networking disabled from the host and FakeNet-NG available for controlled network simulation. Analysis workflow:

1. Original malware file copied to C:\analysis\annabelle.exe.
2. Compute hashes and record them.

3. For static analysis: PE header inspection PE-bear, CFF Explorer, strings extraction, and code or disassembly inspection in Ghidra is used.
4. For dynamic analysis: Procmon capture during an execution in the isolated VM, Regshot for registry changes, Network capture using Wireshark on the VM interface with host only network.
5. Document findings and extract IOCs.

## 2. Sample identification & metadata

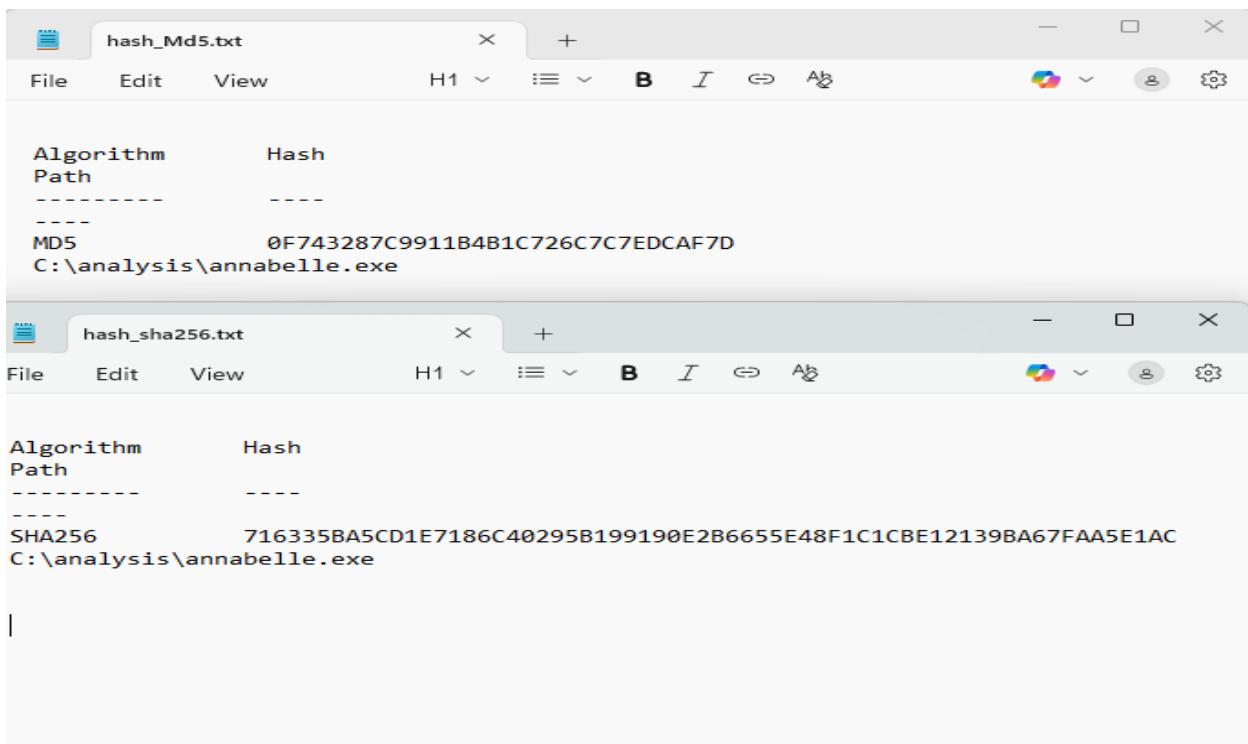
**Filename:** C:\analysis\annabelle.exe

**MD5:** 0F743287C9911B4B1C726C7C7EDCAF7D

**SHA256:**

716335BA5CD1E7186C40295B199190E2B6655E48F1C1CBE12139BA67FAA5E1AC

These hashes uniquely identify the sample and should be used when searching external intel sources or submitting to a sandbox. .



```
hash_Md5.txt
Algorithm      Hash
Path
-----
MD5           0F743287C9911B4B1C726C7C7EDCAF7D
C:\analysis\annabelle.exe

hash_sha256.txt
Algorithm      Hash
Path
-----
SHA256        716335BA5CD1E7186C40295B199190E2B6655E48F1C1CBE12139BA67FAA5E1AC
C:\analysis\annabelle.exe
```

## 3. Static analysis

### 3.1 PE header & imports (PE-bear / CFF Explorer)

Observations from PE tools PE-bear and CFF Explorer : The binary contains the MZ and PE signatures and standard section layout (.text, .rsrc, etc.). Ghidra strings also show MZ and PE present at expected offsets.

- Import analysis indicates strong .NET dependencies — presence of mscorelib, System.\* namespaces — consistent with a .NET application rather than a native C/C++ binary.
- CFF Explorer and PE-bear confirm references to .NET runtime components.
- The binary references to cryptographic classes such as RijndaelManaged, SHA512Managed, CryptoStream, and ICryptoTransform - observed in Ghidra strings.
- These are typical .NET classes for symmetric encryption and hashing, indicating the sample likely performs encryption/decryption or hashing operations.

**Conclusion from PE analysis:** The file is a managed .NET executable containing references to IO, networking, and cryptography libraries which is likely an application that can read/write files and perform cryptographic processing.



FlareVM (Malware Dev Anal) (Snapshot 2) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

### SFF Explorer VIII - [annabelle.exe]

File Settings ?

**annabelle.exe**

**File: annabelle.exe**

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Resource Directory
- .NET Directory
  - MetaData Header
  - MetaData Streams
    - #~
    - Tables Header
      - #Strings
      - #US
      - #GUID
      - #Blob
      - #GUID
      - #Strings
      - #Blob
      - #Schema
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor

| Property  | Value                                    |
|-----------|--|
| File Name | C:\Analysis\raw\annabelle.exe            |
| File Type | Portable Executable 64 .NET Assembly     |
| File Info | No match found.                          |
| File Size | 15.94 MB (16712192 bytes)                |
| PE Size   | 15.94 MB (16712192 bytes)                |
| Created   | Thursday 31 October 2019, 16.11.34       |
| Modified  | Thursday 31 October 2019, 16.10.22       |
| Accessed  | Thursday 16 October 2025, 15.38.41       |
| MD5       | 0F743287C9911B4B1C726C7C7EDCAF7D         |
| SHA-1     | 9760579E73095455FCBADDDE1E7E98A2BB28BFE0 |

| Property         | Value            |
|------------------|------------------|
| Comments         |                  |
| CompanyName      |                  |
| FileDescription  | Annabelle        |
| FileVersion      | 2.1.0.0          |
| InternalName     | Annabelle.exe    |
| LegalCopyright   | Copyright © 2018 |
| LegalTrademarks  |                  |
| OriginalFilename | Annabelle.exe    |
| ProductName      | UpdateBackup     |
| ProductVersion   | 2.1.0.0          |

Right Ctrl ↵

FlareVM (Malware Dev Anal) (Snapshot 2) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

### PE-bear v0.7.1 [C:/Analysis/raw/annabelle.exe]

File Settings View Compare Info

**annabelle.exe**

- DOS Header
  - DOS stub
- NT Headers
  - Signature
  - File Header
  - Optional Header
- Section Headers
- Sections
  - .text
  - .rsrc

| Offset | Name                                     | Value                        |
|--------|--|------------------------------|
| 0      | Magic number                             | 5A4D                         |
| 2      | Bytes on last page of file               | 90                           |
| 4      | Pages in file                            | 3                            |
| 6      | Relocations                              | 0                            |
| 8      | Size of header in paragraphs             | 4                            |
| A      | Minimum extra paragraphs needed          | 0                            |
| C      | Maximum extra paragraphs needed          | FFFF                         |
| E      | Initial (relative) SS value              | 0                            |
| 10     | Initial SP value                         | B8                           |
| 12     | Checksum                                 | 0                            |
| 14     | Initial IP value                         | 0                            |
| 16     | Initial (relative) CS value              | 0                            |
| 18     | File address of relocation table         | 40                           |
| 1A     | Overlay number                           | 0                            |
| 1C     | Reserved words[4]                        | 0, 0, 0, 0                   |
| 24     | OEM identifier (for OEM information)     | 0                            |
| 26     | OEM information; OEM identifier specific | 0                            |
| 28     | Reserved words[10]                       | 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 |
| 3C     | File address of new exe header           | 80                           |

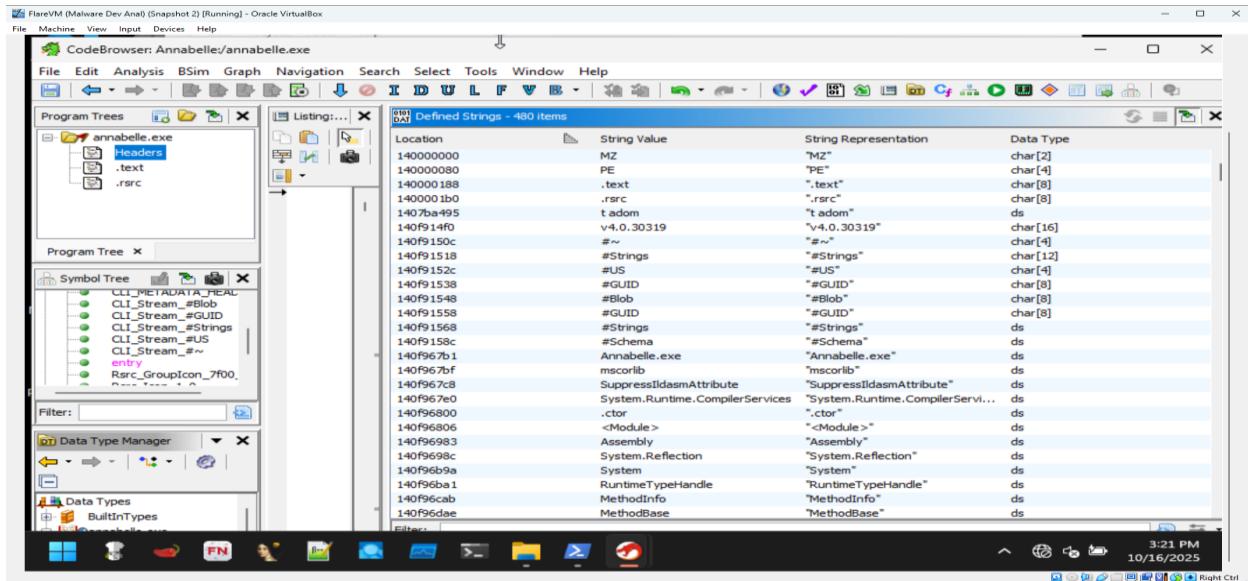
Right Ctrl ↵

| Member                      | Offset   | Size  | Value            | Meaning |
|-----------------------------|----------|-------|------------------|---------|
| Magic                       | 00000098 | Word  | 020B             | PE64    |
| MajorLinkerVersion          | 0000009A | Byte  | 50               |         |
| MinorLinkerVersion          | 0000009B | Byte  | 00               |         |
| SizeOfCode                  | 0000009C | Dword | 00FAD000         |         |
| SizeOfInitializedData       | 000000A0 | Dword | 00043000         |         |
| SizeOfUninitializedData     | 000000A4 | Dword | 00000000         |         |
| AddressOfEntryPoint         | 000000A8 | Dword | 00000000         | Invalid |
| BaseOfCode                  | 000000AC | Dword | 00002000         |         |
| ImageBase                   | 000000B0 | Qword | 0000000014000000 |         |
| SectionAlignment            | 000000B8 | Dword | 00002000         |         |
| FileAlignment               | 000000BC | Dword | 00000200         |         |
| MajorOperatingSystemVers... | 000000C0 | Word  | 0004             |         |
| MinorOperatingSystemVers... | 000000C2 | Word  | 0000             |         |
| MajorImageVersion           | 000000C4 | Word  | 0000             |         |
| MinorImageVersion           | 000000C6 | Word  | 0000             |         |
| MajorSubsystemVersion       | 000000C8 | Word  | 0006             |         |
| MinorSubsystemVersion       | 000000CA | Word  | 0000             |         |
| Win32VersionValue           | 000000CC | Dword | 00000000         |         |
| SizeOfImage                 | 000000D0 | Dword | 00FF4000         |         |
| SizeOfHeaders               | 000000D4 | Dword | 00000200         |         |
| CheckSum                    | 000000D8 | Dword | 00000000         |         |

### 3.2 Strings analysis :

Key strings extracted and relevant observations from ghidra\_strings.txt :

- Annabelle.exe, Annabelle.Resources.resources confirms consistent self identity.
- mscorel, System.\* namespaces confirms .NET runtime usage.
- RijndaelManaged, CryptoStream, ICryptoTransform, SHA512 Managed indicates cryptographic operations that is symmetric encryption + hashing.
- UI and application related strings: WindowsFormsApplicationBase, OnCreate MainForm, MessageBoxButtons, ProgressBar, ListBox suggests a GUI application built with Visual Basic / Windows Forms.
- WebClient, System.Net — indicates potential network capability (HTTP client).



Several obfuscated looking resource names which may correspond to embedded possibly encrypted data or resource streams.

**Interpretation:** The strings show the program is a .NET Windows Forms app with cryptographic and networking capabilities — likely intended to present a GUI and perform file/crypto operations, and possibly network callbacks via WebClient (if enabled).

### 3.3 Assembly / .NET disassembly insights :

Ghidra's decompiler reveals managed function names, class names, and references to ActionEncrypt / ActionDecrypt in the string table and symbol metadata.

This suggests the application contains explicit functionality to encrypt and decrypt data

- Observed methods and classes: Annabelle.My namespace, OnCreateMainForm, ActionEncrypt, ActionDecrypt, SendNotifyMessage, FileSystemProxy, RegistryProxy. These names reveal the developer intent: encryption actions, file system operations, possible registry interaction, and UI wiring for user driven encryption tasks.
- Presence of WebClient and System.Net usage in combination with string constants suggests the code may attempt to upload/download data or contact web endpoints.

FlareVM (Malware Dev Anal) (Snapshot 2) [Running] - Oracle VirtualBox

CodeBrowser: Annabelle:/annabelle.exe

Listing: annabelle.exe

```

// .rsrc
// ram:140fb0000-ram:140ff2fff
//
IMAGE_RESOURCE_DIRECTORY_140fb0000 XREF[2]: 140000118(*),
140fb0000 00 00 00 ddw 0h Characterist...
00 00 00 dw TimeDateStamp
00 00 00 dw MajorVersion
140fb000a 00 00 dw 0h MinorVersion
140fb000c 00 00 dw 0h NumberOfName...
140fb000e 04 00 dw 4h NumberOfIdEn...
140fb0010 03 00 00 ddw 0h ...
00 30 00 dw ...
00 80 IMAGE_RESOURCE_DIRECTORY_140fb0018 0e 00 00 ddw 0h ...
00 60 00 dw ...
00 80 IMAGE_RESOURCE_DIRECTORY_140fb0020 10 00 00 ddw 0h ...
00 90 00 dw ...
00 80 IMAGE_RESOURCE_DIRECTORY_140fb0028 18 00 00 ddw 0h ...
00 c0 00 dw ...
00 80

```

Program Tree X

Symbol Tree X

Imports  
Exports  
entry \_EXT\_140003e08  
Functions  
Labels  
CLI\_METADATA\_HEAD  
CLI\_Stream\_Blob  
CLI\_Stream\_GUID  
CLI\_Stream\_Strings  
CLI\_Stream\_US  
CLI\_Stream\_~  
Filter:

Data Type Manager X

3:15 PM 10/16/2025 Right Ctrl

FlareVM (Malware Dev Anal) (Snapshot 2) [Running] - Oracle VirtualBox

CodeBrowser: Annabelle:/annabelle.exe

Listing: annabelle.exe

```

CLI_METADATA_HEADER
140f914e0 42 53 4a CLI_META...
42 01 00 ...
01 00 00 ...
140f914e0 42 53 4a 42 ddw 424a5342h Signature must be 0x424a5342
140f914e4 01 00 dw lh MajorVersion
140f914e6 01 00 dw lh MinorVersion
140f914e8 00 00 00 ddw 0h Reserved should be 0
140f914ec 10 00 00 ddw 10h VersionLength
140f914f0 76 34 2e 30 2e char[16] "v4.0.30319" Version
33 30 33 31 39 ...
00 00 00 00 ...
140f91500 00 00 dw 0h Flags should be 0
140f91502 09 00 dw 9h StreamsCount number of stream h...
140f91504 b4 00 00 00 1c CLI_Stre...
52 00 00 23 7e ...
00 00 ...
140f91510 d0 52 00 00 ec CLI_Stre...
71 01 00 23 53 ...
74 72 69 ee 67 ...
140f91510 d0 52 00 00 ddw 52D0h offset
140f91514 ec 71 01 00 ddw 171ECh size
140f91518 23 53 74 72 69 char[12] "#Strings" name
6e 67 73 00 00 ...
00 00

```

Program Tree X

Functions  
Labels  
CLI\_METADATA\_HEAD  
CLI\_Stream\_Blob  
CLI\_Stream\_GUID  
CLI\_Stream\_Strings  
CLI\_Stream\_US  
CLI\_Stream\_~  
entry  
Rsrc\_GroupIcon\_7f00  
Rsrc\_Icon\_1\_0  
Rsrc\_Manifest\_1\_0  
Rsrc\_VerIcon\_1\_n  
Filter:

Data Type Manager X

3:17 PM 10/16/2025 Right Ctrl

## 4. Dynamic analysis

### 4.1 Procmon timeline & interpretation

Selected Procmon events :

→ 47:48.0 annabelle.exe (PID 4464) CreateFile

C:\Windows\Prefetch\ANNABELLE.EXE-ADD98F06(pf NAME NOT FOUND

Attempt to read prefetch — typical on first run or when prefetch not yet generated.

→ 56:39.4 annabelle.exe (PID 5860) CreateFile C:\Analysis SUCCESS

Process accessed analysis directory.

→ 56:39.4 many CreateFile events on system DLLs: mscoree.dll, apphelp.dll, ntdll.dll, kernel32.dll, KernelBase.dll, msrvct.dll, bcrypt.dll, advapi32.dll, shlwapi.dll, etc.

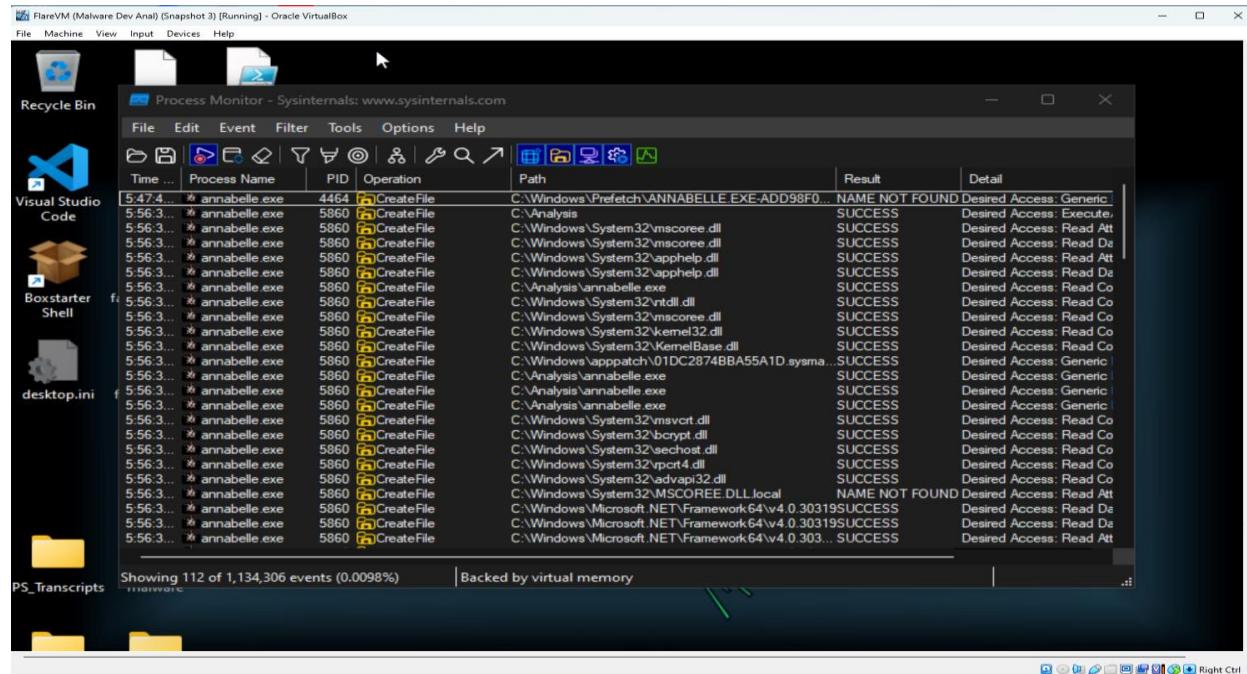
These indicate the loader resolving runtime dependencies (expected for .NET process startup).

→ 56:39.4 repeated CreateFile on C:\Analysis\annabelle.exe (SUCCESS)

Process reads its own binary (self-checks/resources). No immediate WriteFile events to user data observed in the provided snippet.

**Interpretation:** The Procmon trace confirms process startup and .NET runtime loading. No mass file writes or obvious file renaming/deletion events appear in the excerpt.

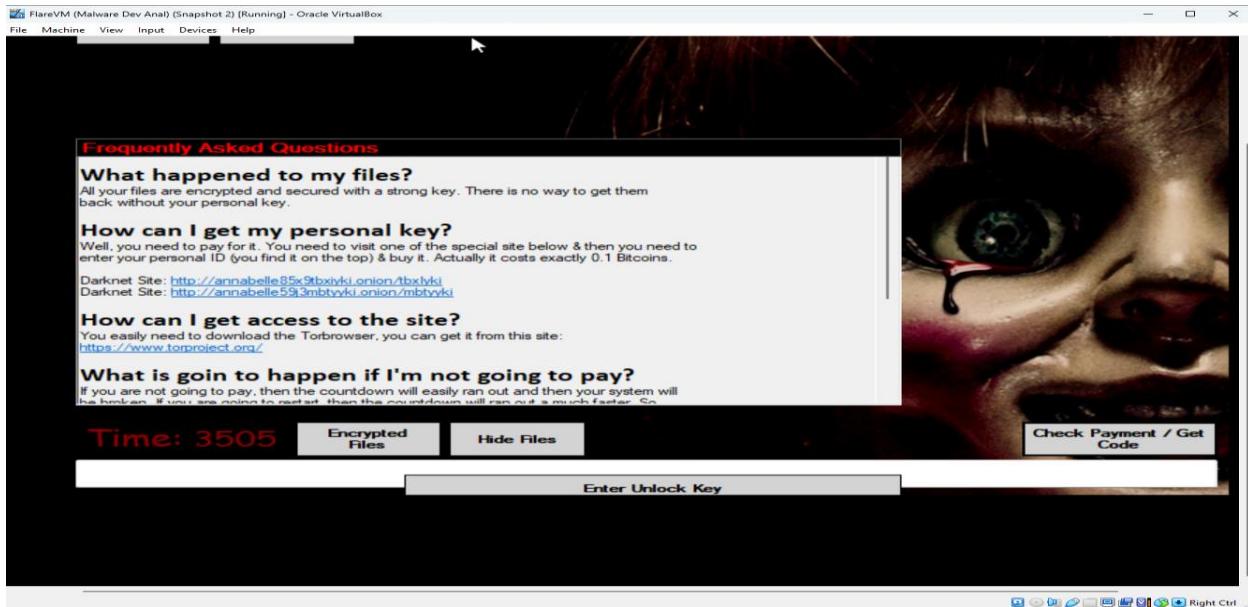
However, absence of writes in this snippet does not rule out encryption — the sample may require arguments or a user action to trigger encryption, or the test run was short.



The screenshot shows the Process Monitor application running on a Windows 10 desktop. The main window displays a list of 112 events out of 1,134,306 total, all occurring at 56:39.3. The events are filtered to show only CreateFile operations. The list includes multiple entries for the process ID 5860, which corresponds to the annabelle.exe process. The operations are performed on various system DLLs such as mscoree.dll, apphelp.dll, ntdll.dll, kernel32.dll, KernelBase.dll, msrvct.dll, bcrypt.dll, advapi32.dll, and shlwapi.dll. Most of these operations result in 'SUCCESS' and involve 'Desired Access: Read' or 'Read & Execute'. There are also several entries for the path 'C:\Windows\Prefetch\ANNABELLE EXE-ADD98F0...', indicating the creation of prefetch files. The bottom status bar indicates the monitor is 'Backed by virtual memory'.

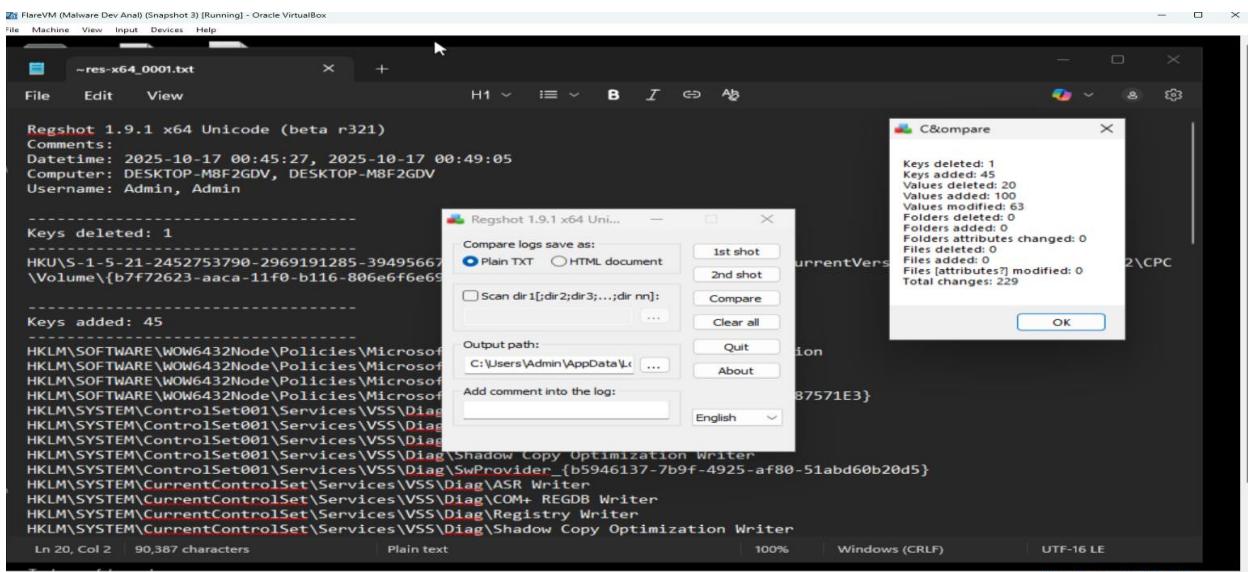
During the controlled execution of annabelle.exe inside the isolated FLARE VM, a **ransom note** appeared on screen shortly after launch.

The note demanded payment in cryptocurrency to restore access to the system.



## 4.2 Regshot comparison (before vs after) — critical findings

Provided a Regshot with 2 snapshots - 4 minutes apart. Key, high value items extracted from the comparison:



### A. Persistence created

- Run key added:  
HKU\<User>

```
SID>\Software\Microsoft\Windows\CurrentVersion\Run\UpdateBackup:  
"C:\Analysis\annabelle.exe"
```

This creates persistence: the binary will be launched at user log on under the name UpdateBackup.

### ***B. Security and system protections disabled or altered***

Multiple newly added values indicate policy changes to disable Windows security functionality and system recovery:

- HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows Defender\DisableAntiSpyware: 0x00000001
- HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring: 0x00000001
- HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows NT\SystemRestore\DisableSR: 0x00000001
- HKU\<SID>\Software\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring: 0x00000001
- HKU\<SID>\Software\Policies\Microsoft\Windows\CurrentVersion\Policies\System \DisableTaskMgr: 0x00000001
- HKU\<SID>\Software\Policies\Microsoft\Windows\CurrentVersion\Policies\System \DisableRegistryTools: 0x00000001
- HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\DisableCMD: 0x00000002 and related DisableCMD keys
- HKLM\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows NT\SystemRestore\DisableConfig: 0x00000001

**Interpretation:** These registry additions are strong evidence of a deliberate attempt to reduce the victim's ability to detect, stop, or recover from the malware, turning off Defender real time monitoring, preventing System Restore, disabling Task Manager and Registry Editor, and disabling CMD.

This is classic behavior for ransomware or stealthy malware trying to prevent remediation.

### ***C. SafeBoot changes***

- Keys added under ControlSet001\Control\SafeBoot\Minimal\MinimalX and service flags like HKLM\SYSTEM\ControlSet001\Services\USBSTOR changed to

0x00000004 — suggesting modification of service startup behavior and Safe Boot configuration values.

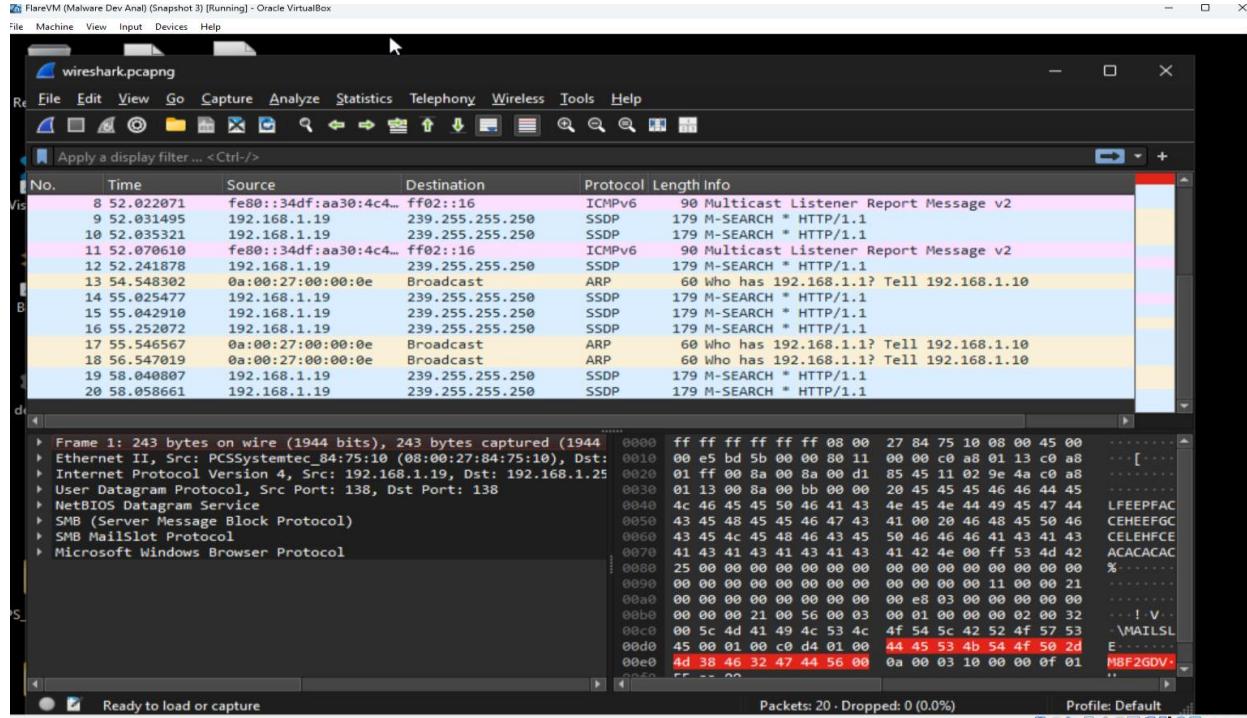
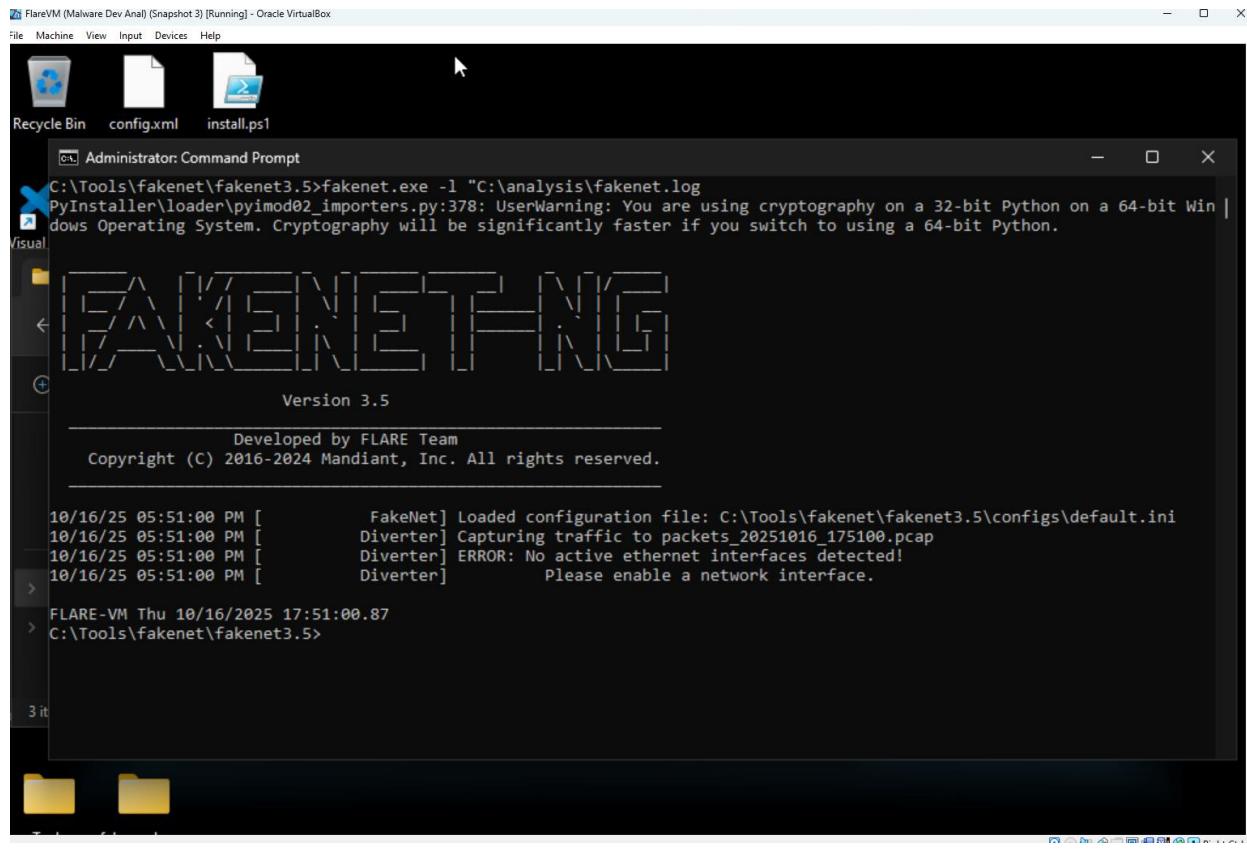
- Values for WinDefend and related services show modifications (e.g., HKLM\SYSTEM\CurrentControlSet\Services\WinDefend: 0x00000003) — may correspond to service start types or states.

#### **D. USB enumeration entries deleted**

- Several Enum entries for USB devices and volume snapshots were deleted . This might reflect attempts to disable Volume Shadow Copy (to prevent backup recovery) or to interfere with removable media enumeration.

### **4.3 Network capture (Wireshark & Fakenet)**

- The provided capture shows only local/host discovery traffic (NetBIOS/BROWSER, mDNS, SSDP, ARP). No outbound HTTP, DNS to suspicious domains, or other C2 traffic was observed in the snippet.
- This implies either the sample did not attempt network C2 during this short run, or network attempts were conditional and not triggered.



## 5. Findings & assessment

### 5.1 Confirmed malicious behaviors

- **Persistence:** HKU\<SID>\...\Run\UpdateBackup was added pointing to C:\Analysis\annabelle.exe. This ensures the sample runs at user logon.
- **Defense disabling:** Registry values added to disable Windows Defender real-time monitoring and other recovery options - DisableAntiSpyware, DisableRealtimeMonitoring, DisableSR, etc.
- **System modification:** SafeBoot and service entries modified; USB/volume enumeration entries deleted (suggests attempts to prevent Volume Shadow Copy based recovery).
- **Encryption capability (static):** The binary contains explicit references to encryption libraries and function names (RijndaelManaged, CryptoStream, ActionEncrypt/ActionDecrypt).

**Overall assessment:** The combination of encryption code plus persistence and active disabling of security/recovery mechanisms is highly indicative of ransomware style malware or a malicious encryptor.

Even though no mass file encryption was observed within the short dynamic run, the registry changes demonstrate the sample attempted in modifying the system to facilitate malicious activity and block remediation.