Midterm - Malware Case Study

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:

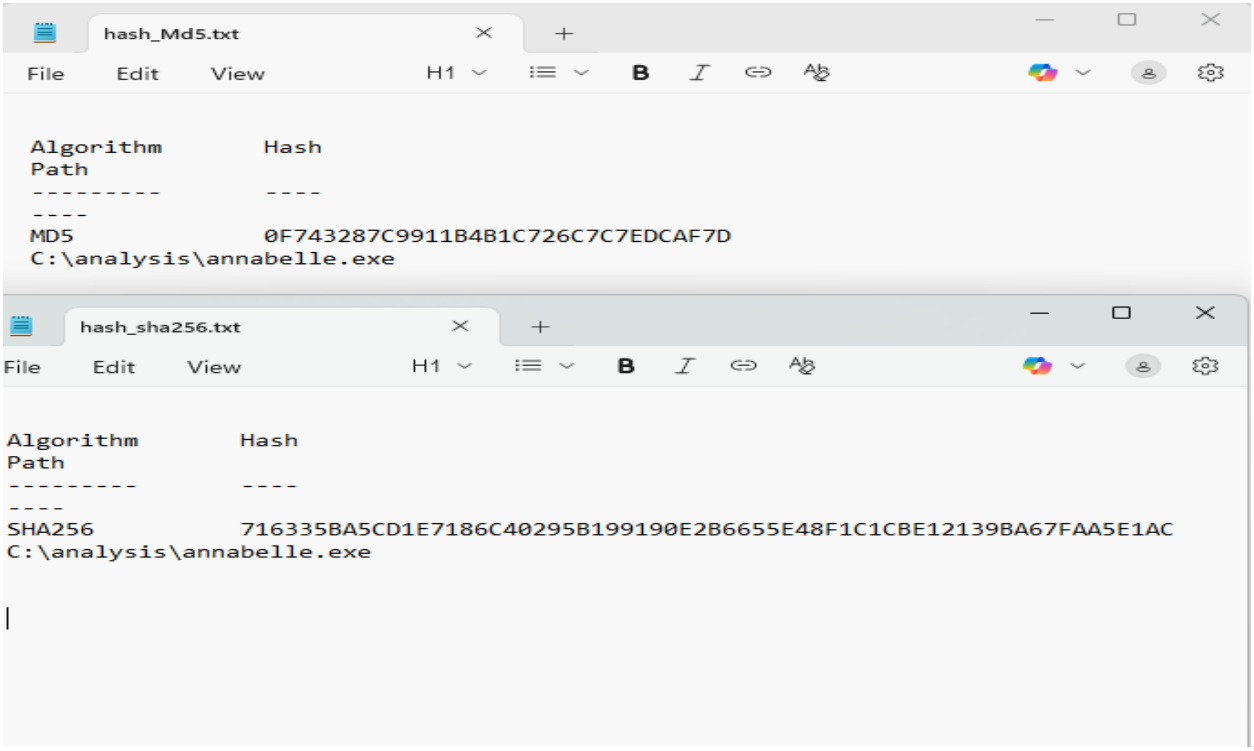
1. Original malware file copied to C:\analysis\annabelle.exe.
2. Compute hashes and record them.
3. For static analysis: PE header inspection PE-bear, CFF Explorer, strings extraction, and code or disassembly inspection in Ghidra is used.

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. .



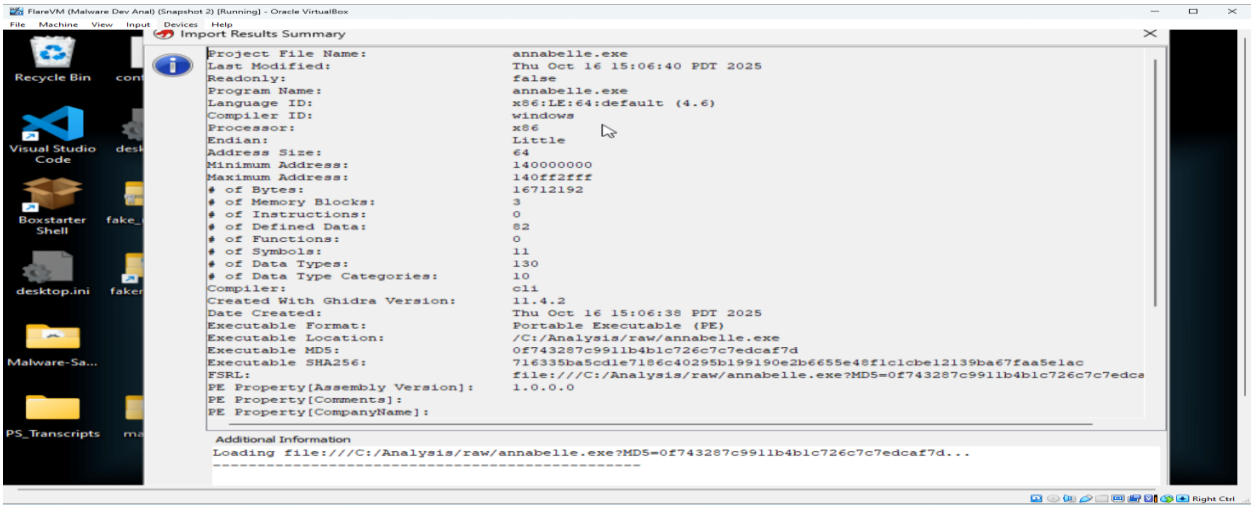
3. Static analysis

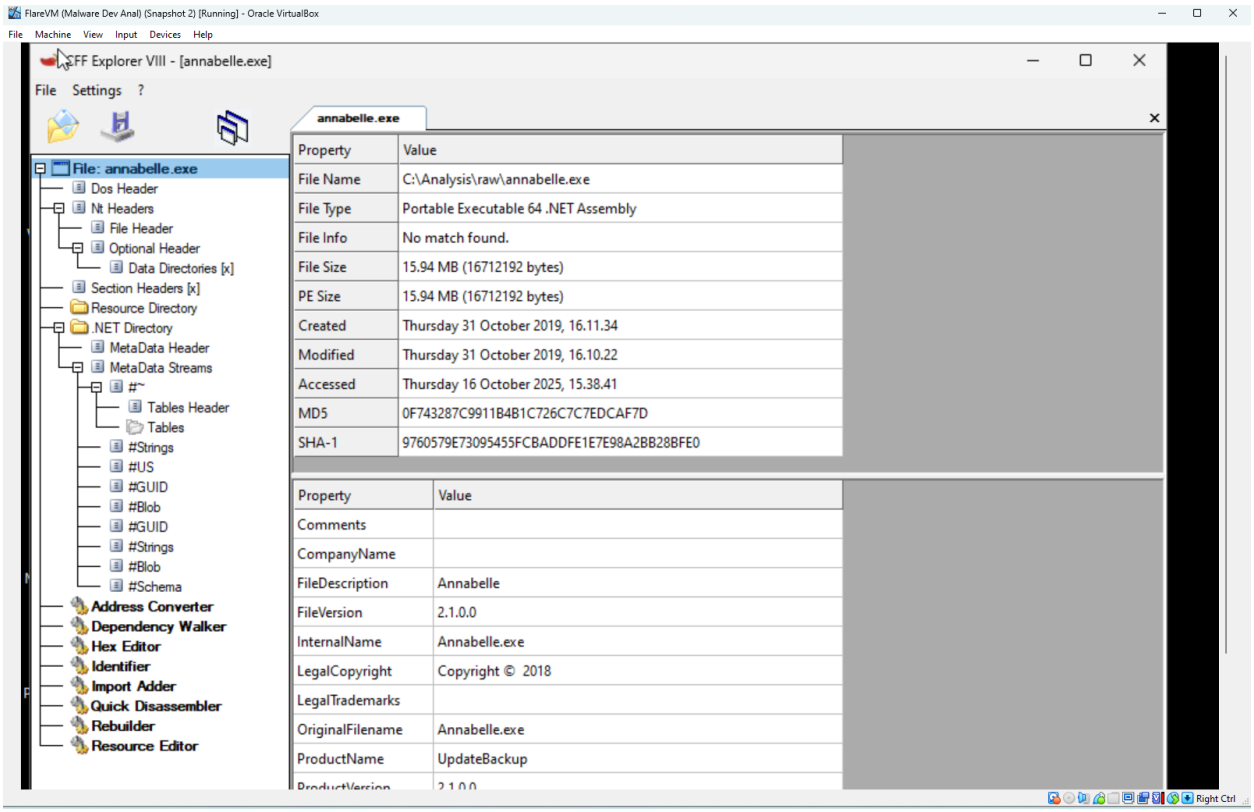
3.1 PE header & imports (PE-bear / CFF Explorer)

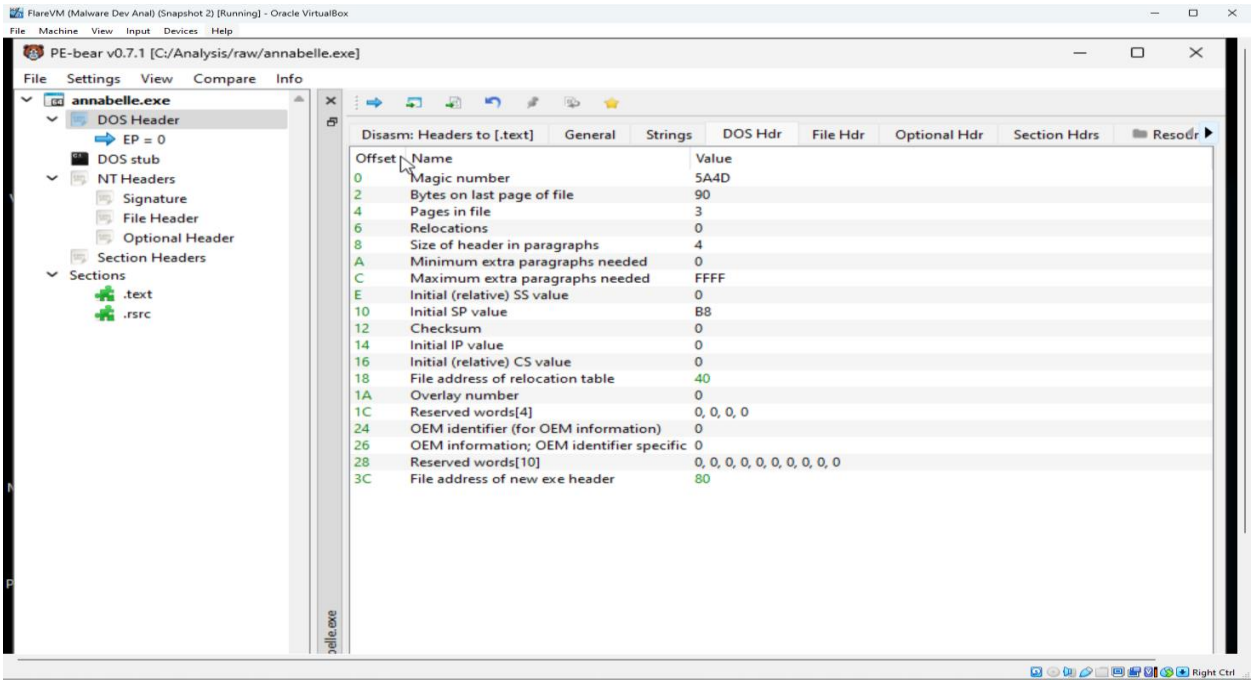
Observations from PE tools PE-bear and CFF Explorer : The binary contains the MZ and PE signatures and standard section layout (.text, .rsrc, etc.). Ghidra strings also show MZ and PE present at expected offsets.

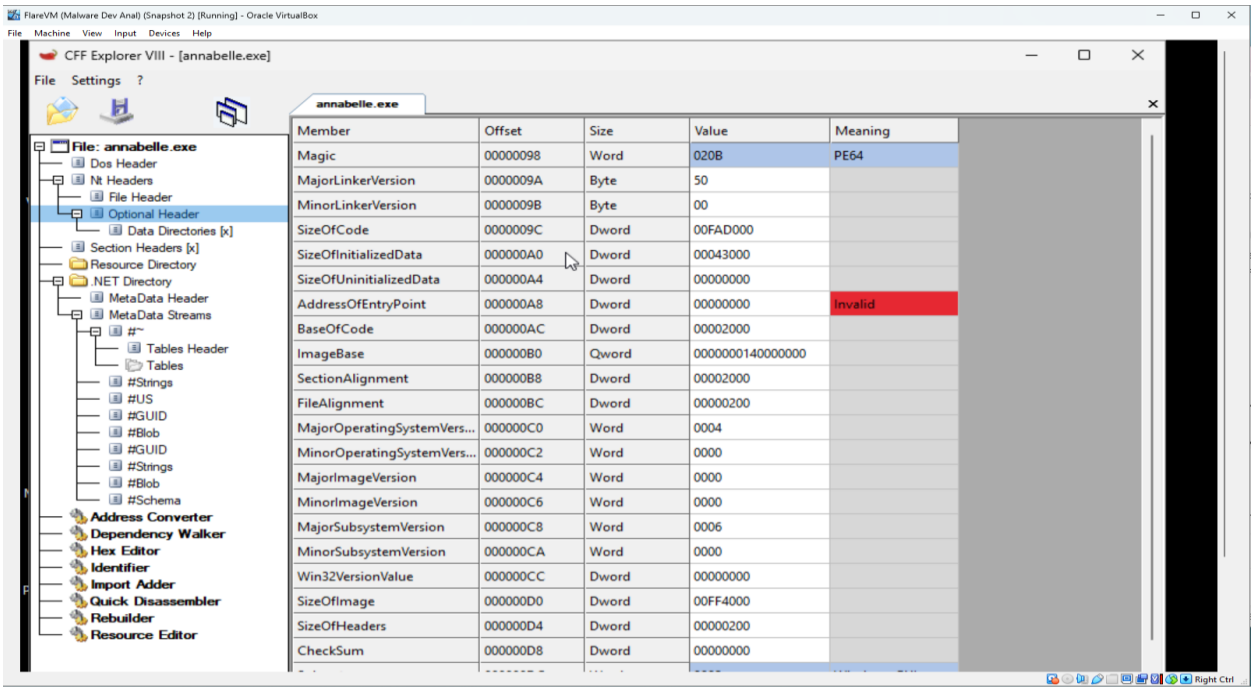
- → Import analysis indicates strong .NET dependencies — presence of mscorlib, System.* namespaces — consistent with a .NET application rather than a native C/C++ binary.
- → CFF Explorer and PE-bear confirm references to .NET runtime components.
- → The binary references to cryptographic classes such 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
FF 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
Tables
#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 9760579E73095455FCBADDFE1E7E98A2BB28BFE0
Property Value
Comments
CompanyName
FileDescription Annabelle
FileVersion 2.1.0.0
InternalName Annabelle.exe
LegalCopyright Copyright © 2018
LegalTrademarks
OriginalFilename Annabelle.exe
ProductName UpdateBackup
Right Ctrl

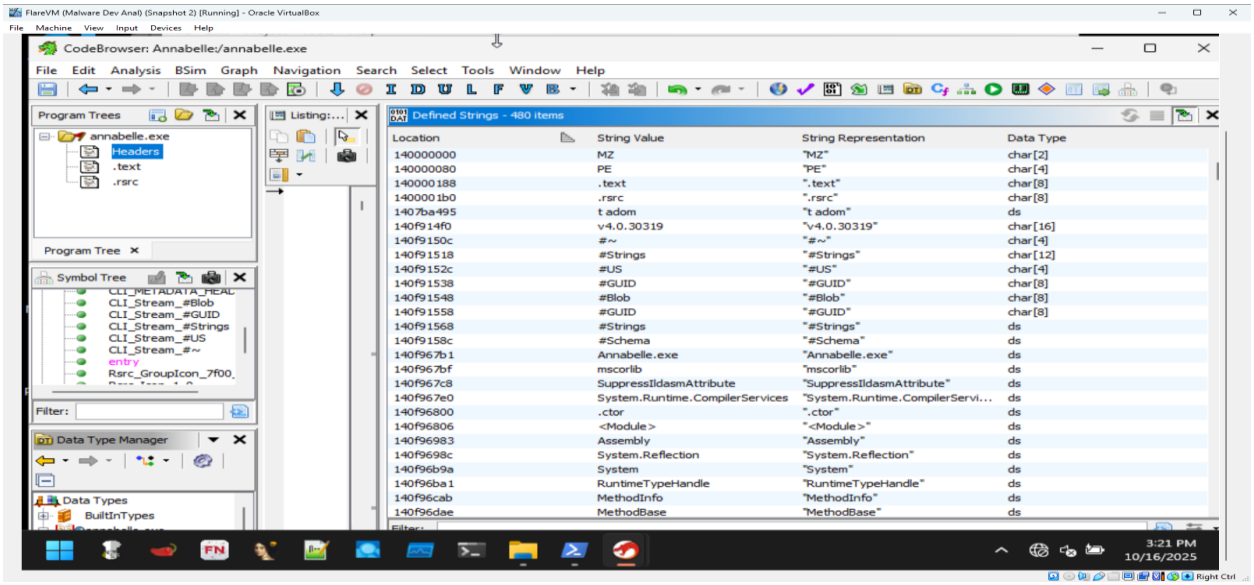

FlareVM (Malware Dev Anal) (Snapshot 2) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
PE-bear v0.7.1 [C:/Analysis/raw/annabelle.exe]
File Settings View Compare Info
annabelle.exe
DOS Header
EP = 0
DOS stub
NT Headers
Signature
File Header
Optional Header
Section Headers
Sections
.text
.rsrc
Disasm: Headers to [.text] General Strings DOS Hdr File Hdr Optional Hdr Section Hdrs
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



3.2 Strings analysis :

Key strings extracted and relevant observations from ghidra_strings.txt :

→ Annabelle.exe, Annabelle.Resources.resources confirms consistent self identity.
→ mscorlib, 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, OnCreateMainForm, 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.

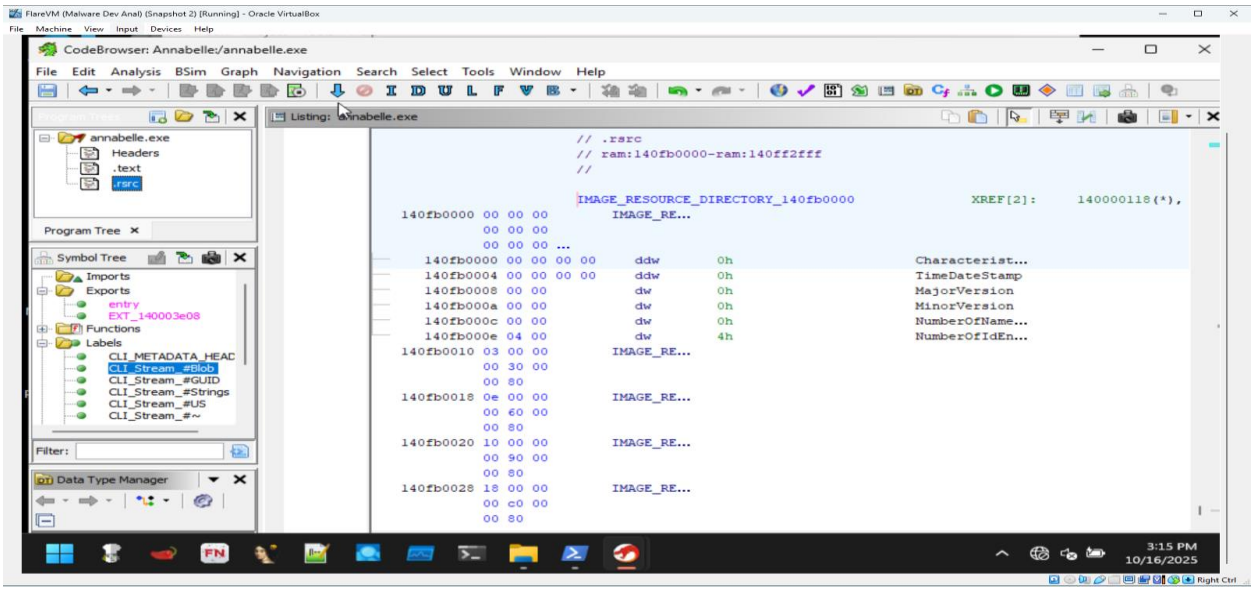
Interpretation: The strings show the program is a .NET Windows Forms app with cryptographic and networking capabilities — likely intended to present a GUI and perform file/crypto operations, and possibly network callbacks via WebClient (if enabled).

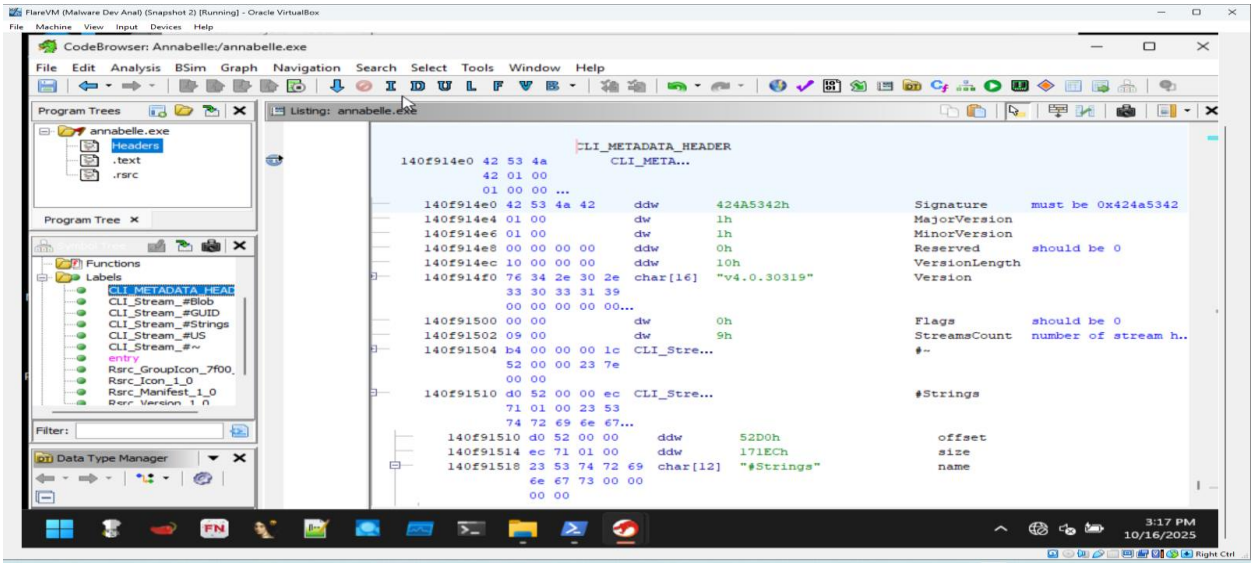
3.3 Assembly / .NET disassembly insights :

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.





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, msvcrt.dll, bcrypt.dll, advapi32.dll, shlwapi.dll, etc.

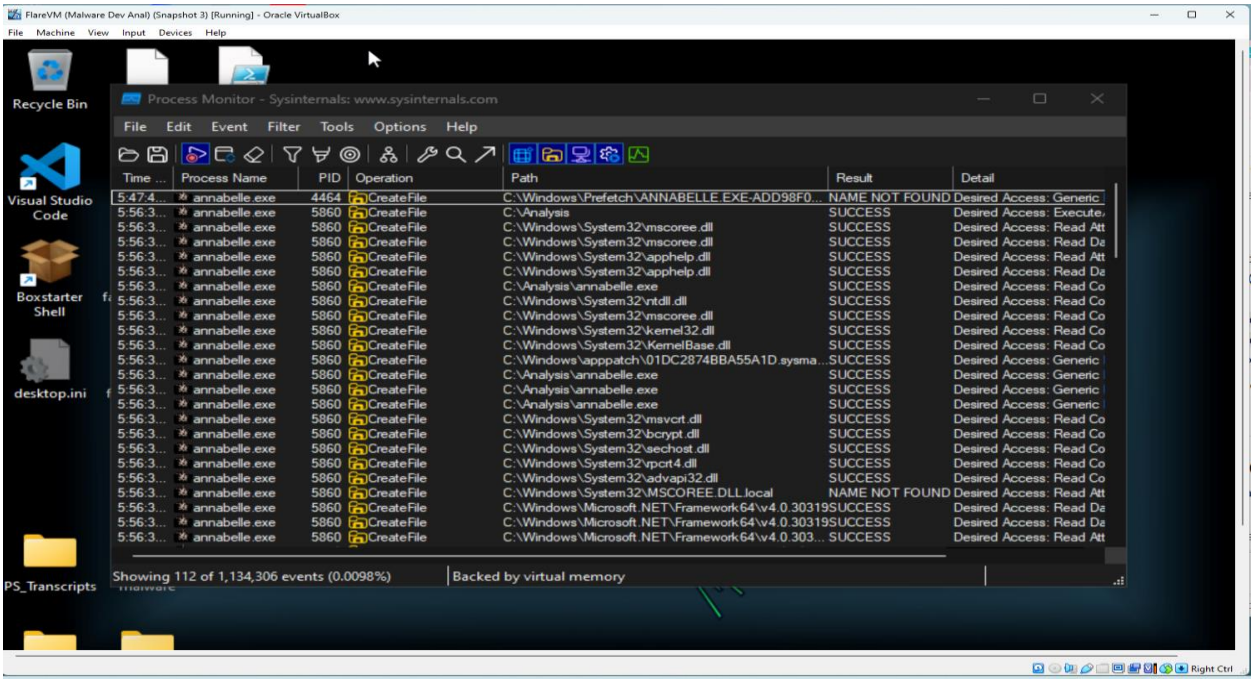
These indicate the loader resolving runtime dependencies (expected for .NET process startup).

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

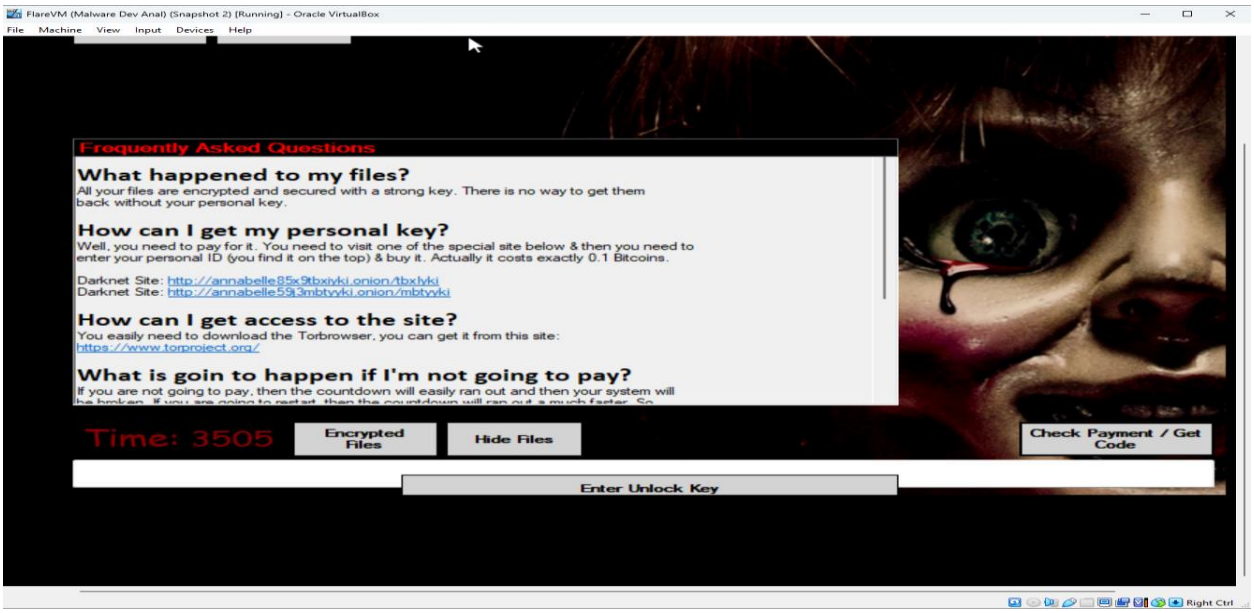
Process reads its own binary (self-checks/resources). No immediate WriteFile events to user data observed in the provided snippet.

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.

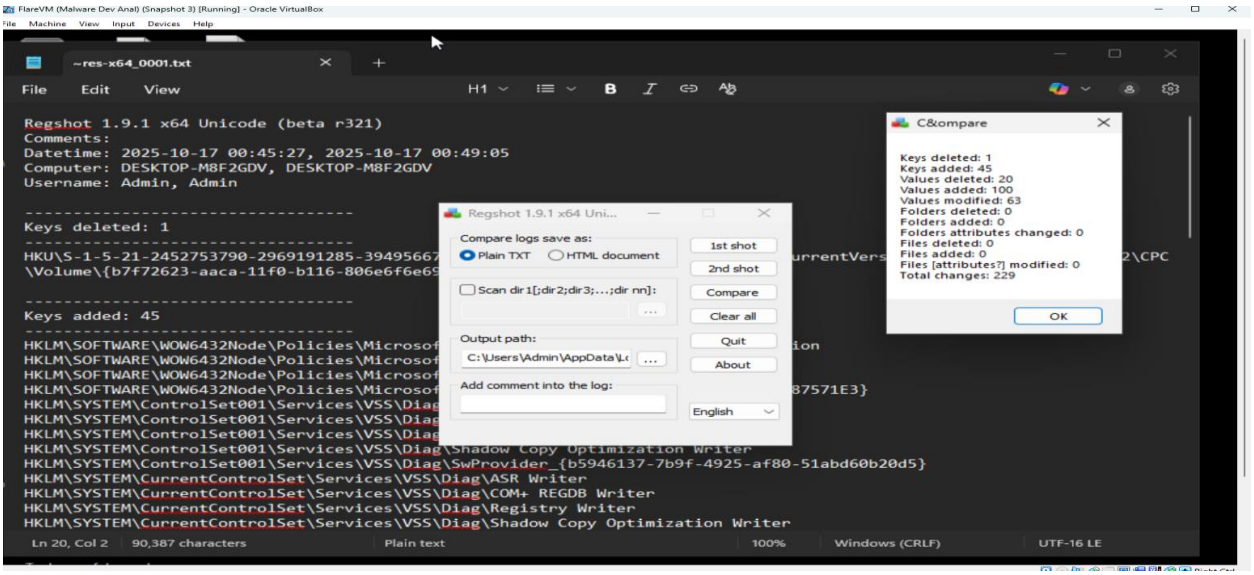


During the controlled execution of annabelle.exe inside the isolated FLARE VM, a **ransom note** appeared on screen shortly after launch.
The note demanded payment in cryptocurrency to restore access to the system.



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.

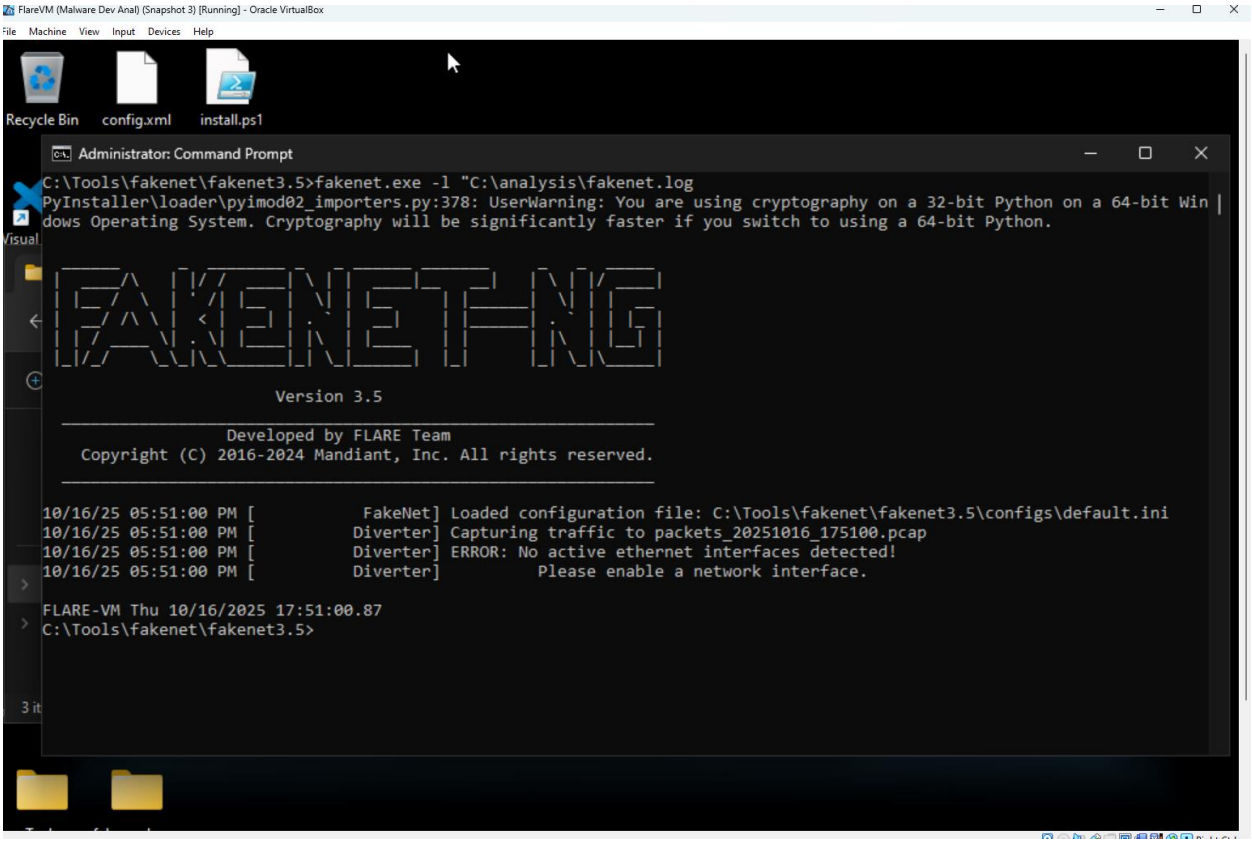
- Values for WinDefend and related services show modifications (e.g., HKLM\SYSTEM\CurrentControlSet\Services\WinDefend: 0x00000003) — may correspond to service start types or states.

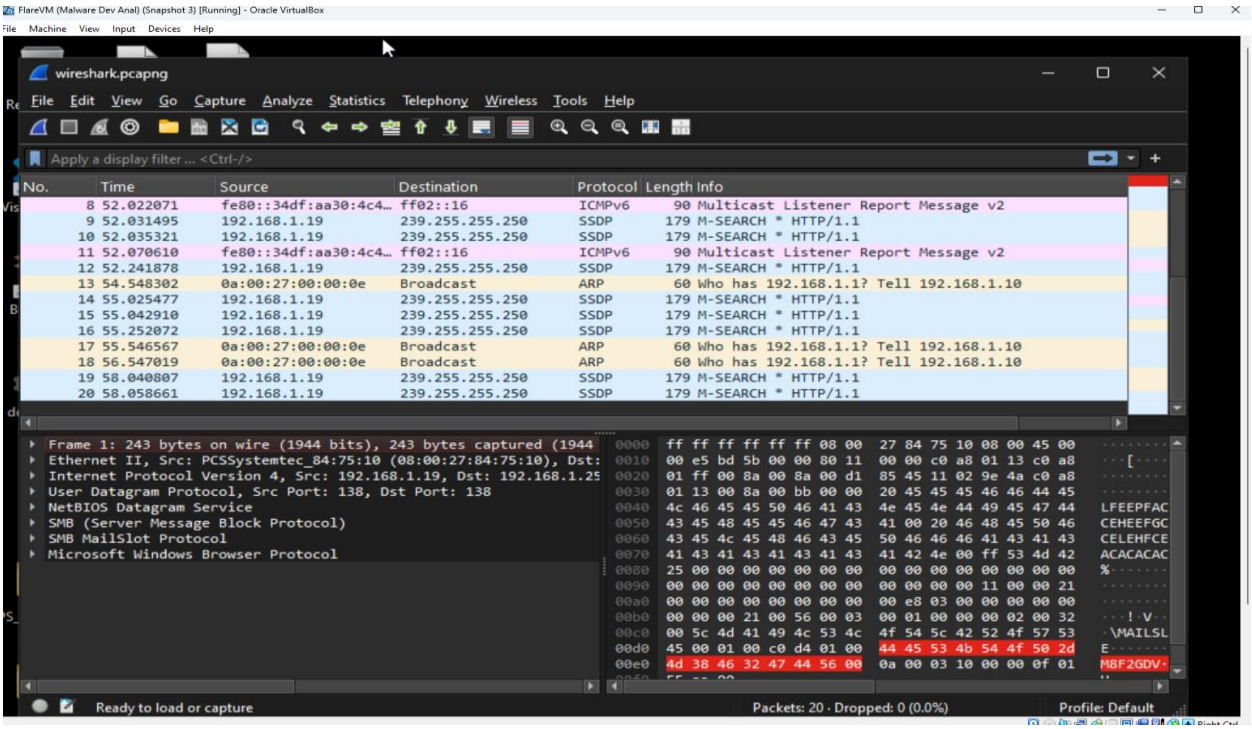
D. USB enumeration entries deleted

- 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.


FlareVM (Malware Dev Anal) (Snapshot 3) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
config.xml
install.ps1
Administrator: Command Prompt
C:\Tools\fakenet\fakenet3.5>fakenet.exe -l "C:\analysis\fakenet.log
PyInstaller\loader\pyimod02_importers.py:378: UserWarning: You are using cryptography on a 32-bit Python on a 64-bit Win
dows Operating System. Cryptography will be significantly faster if you switch to using a 64-bit Python.
Version 3.5
Developed by FLARE Team
Copyright (C) 2016-2024 Mandiant, Inc. All rights reserved.
10/16/25 05:51:00 PM [FakeNet] Loaded configuration file: C:\Tools\fakenet\fakenet3.5\configs\default.ini
10/16/25 05:51:00 PM [Diverter] Capturing traffic to packets_20251016_175100.pcap
10/16/25 05:51:00 PM [Diverter] ERROR: No active ethernet interfaces detected!
10/16/25 05:51:00 PM [Diverter] Please enable a network interface.
FLARE-VM Thu 10/16/2025 17:51:00.87
C:\Tools\fakenet\fakenet3.5>


FlareVM (Malware Dev Anal) (Snapshot 3) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
8 52.022071 fe80::34df:aa30:4c4… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
9 52.031495 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
10 52.035321 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
11 52.070610 fe80::34df:aa30:4c4… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
12 52.241878 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
13 54.548302 0a:00:27:00:00:0e Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.10
14 55.025477 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
15 55.042910 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
16 55.252072 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
17 55.546567 0a:00:27:00:00:0e Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.10
18 56.547019 0a:00:27:00:00:0e Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.10
19 58.040807 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
20 58.058661 192.168.1.19 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944
Ethernet II, Src: PCSSystemtec_84:75:10 (08:00:27:84:75:10), Dst:
Internet Protocol Version 4, Src: 192.168.1.19, Dst: 192.168.1.25
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 08 00 27 84 75 10 08 00 45 00
0010 00 e5 bd 5b 00 00 80 11 00 00 c0 a8 01 13 c0 a8
0020 01 ff 00 8a 00 8a 00 d1 85 45 11 02 9e 4a c0 a8
0030 01 13 00 8a 00 bb 00 00 20 45 45 45 46 46 44 45
0040 4c 46 45 45 50 46 41 43 4e 45 4e 44 49 45 47 44 LFEEPFAC
0050 43 45 48 45 45 46 47 43 41 00 20 46 48 45 50 46 CEHEEFGC
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43 CELEHFCE
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42 ACACACAC
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 21
00a0 00 00 00 00 00 00 00 00 00 e8 03 00 00 00 00 00
00b0 00 00 00 21 00 56 00 03 00 01 00 00 00 02 00 32 ! V
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53 \MAILSL
00d0 45 00 01 00 c0 d4 01 00 44 45 53 4b 54 4f 50 2d E DESKTOP-
00e0 4d 38 46 32 47 44 56 00 0a 00 03 10 00 00 0f 01 M8F2GDV
Ready to load or capture
Packets: 20 · Dropped: 0 (0.0%)
Profile: Default

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.