DLL Stealer

Scenario

You work as a cybersecurity analyst for a major corporation. Recently, your company's security team detected some suspicious activity on the network. It appears that a new DLL Stealer malware has infiltrated your system, and it's causing concern due to its ability to exfiltrate critical DLL files from your system.

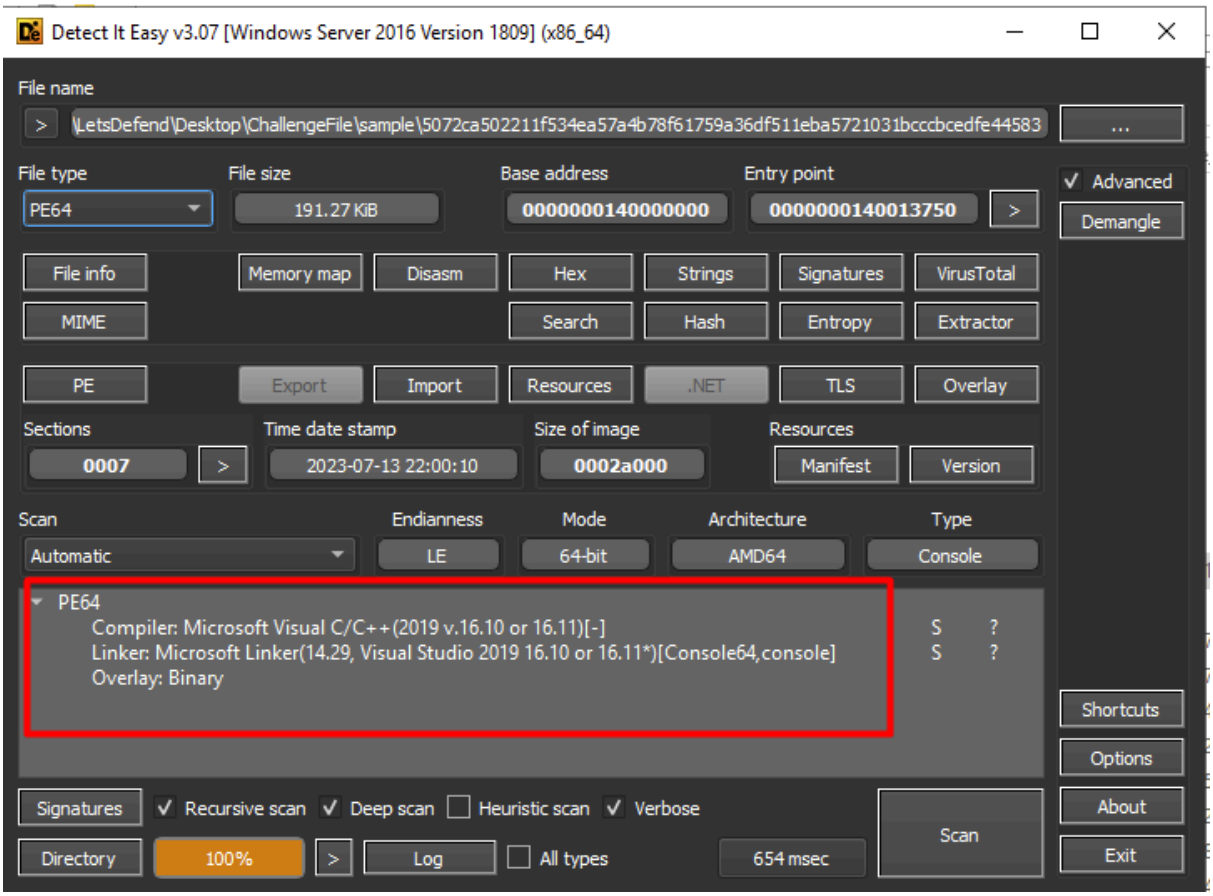
Hello, I’m Mo. Elshaheedy

LinkedIn:https://www.linkedin.com/in/elshaheedy/

This walkthrough analyzes a **DLL Stealer** malware sample using **JetBrains dotPeek**, a .NET decompiler. The goal is to understand the malware's capabilities, identify the stolen data, and determine how it exfiltrates information. The challenge involves answering several questions based on the analysis of the malware.

---

i have file without any ***extensions*** so i will use DIE to get more info about the file which i have:

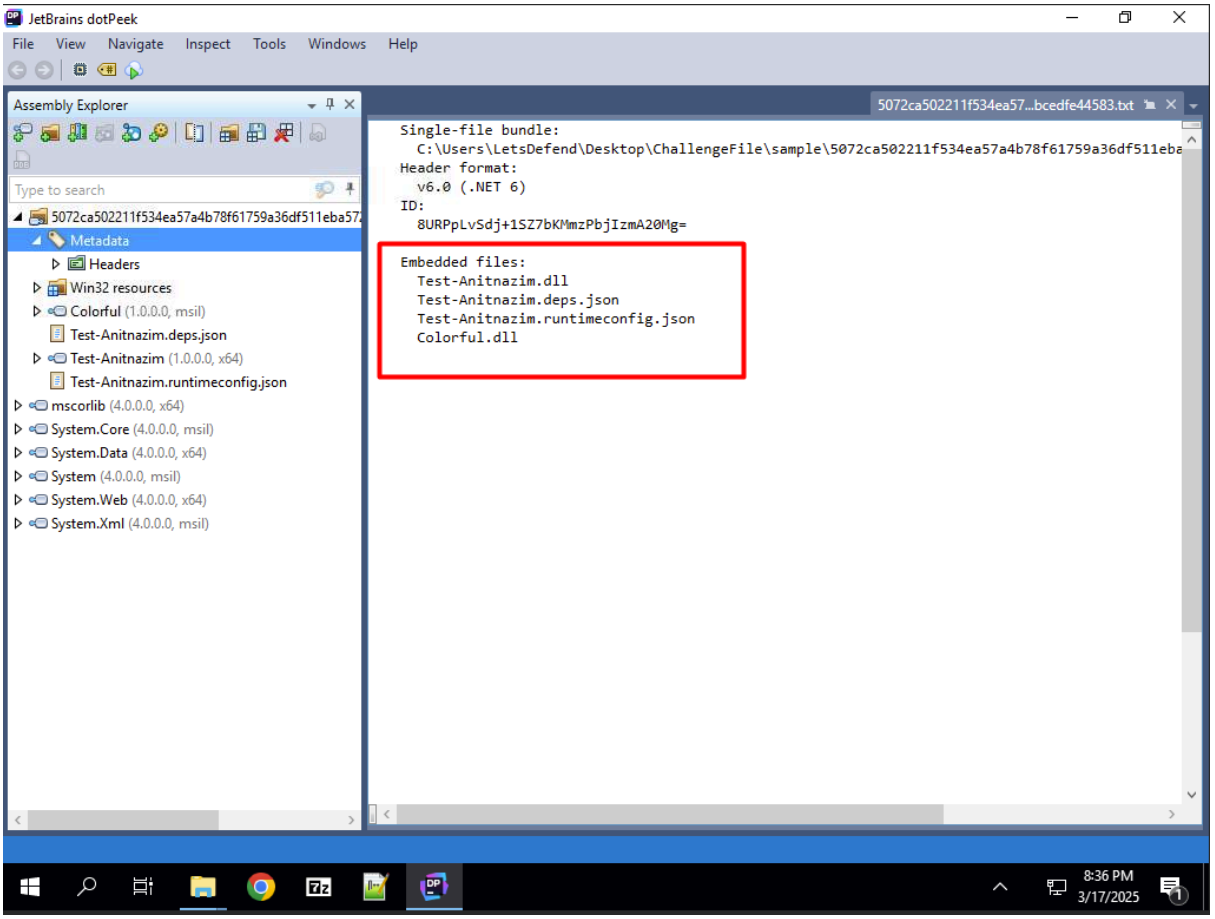


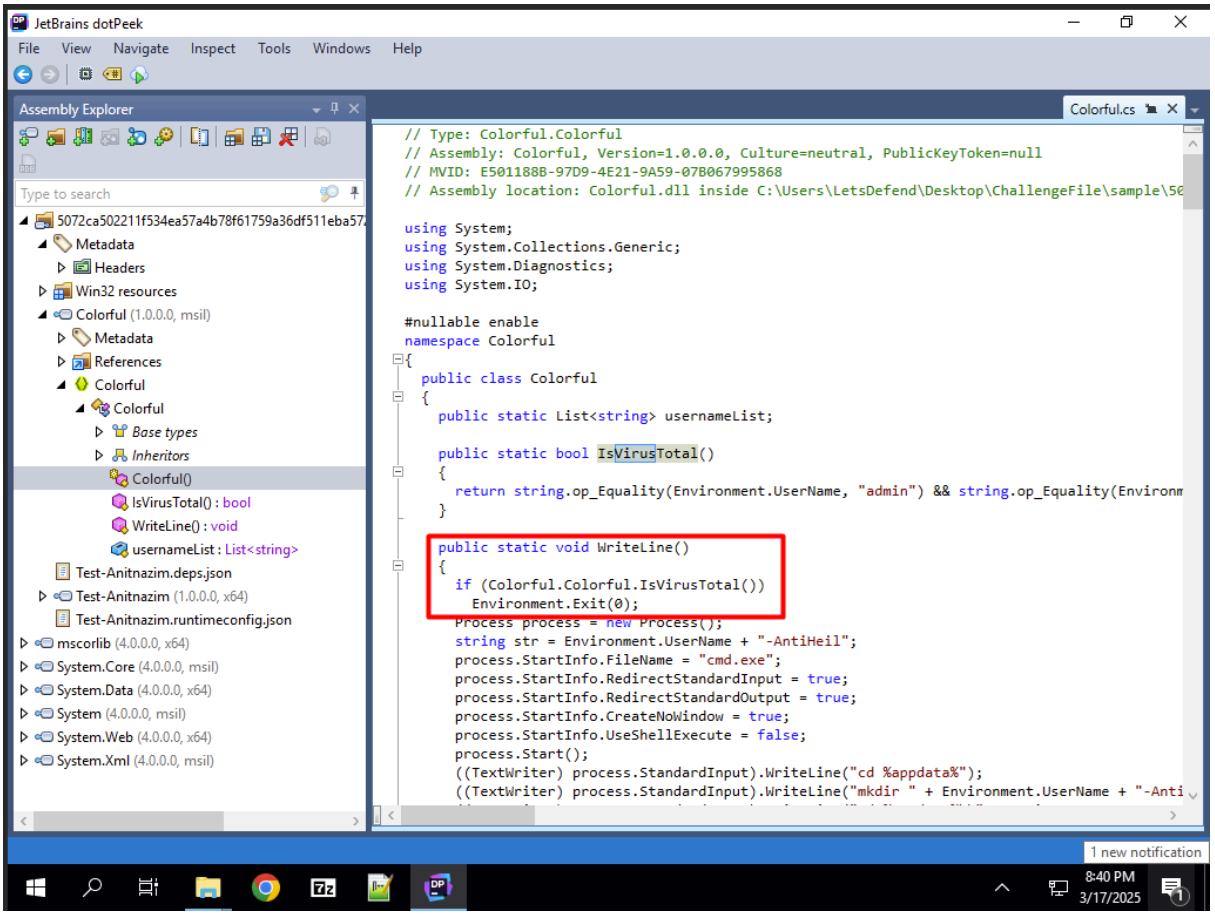
So we will use Jetbrains dotPeek ??

decompiling

The main idea behind dotPeek is **to make high-quality decompiling available to everyone in the . NET community**, free of charge. dotPeek decompiles any . NET assemblies and presents them as C# or IL code.

Exploring the file in dotPeek:


JetBrains dotPeek
File View Navigate Inspect Tools Windows Help
Assembly Explorer
Type to search
5072ca502211f534ea57a4b78f61759a36df511eba57
Metadata
Headers
Win32 resources
Colorful (1.0.0.0, msil)
Test-Anitnazim.deps.json
Test-Anitnazim (1.0.0.0, x64)
Test-Anitnazim.runtimeconfig.json
mscorlib (4.0.0.0, x64)
System.Core (4.0.0.0, msil)
System.Data (4.0.0.0, x64)
System (4.0.0.0, msil)
System.Web (4.0.0.0, x64)
System.Xml (4.0.0.0, msil)
5072ca502211f534ea57...bcedfe44583.txt
Single-file bundle:
C:\Users\LetsDefend\Desktop\ChallengeFile\sample\5072ca502211f534ea57a4b78f61759a36df511eba
Header format:
v6.0 (.NET 6)
ID:
8URPpLvSdj+1SZ7bKMmzPbjIzmA20Mg=
Embedded files:
Test-Anitnazim.dll
Test-Anitnazim.deps.json
Test-Anitnazim.runtimeconfig.json
Colorful.dll
8:36 PM
3/17/2025



Key Functionality:

1. **Anti-Analysis Mechanism**:
   - The malware checks for specific usernames, machine names, and command-line arguments to determine if it is being analyzed in a sandbox or by **VirusTotal**.
   - If it detects analysis, it terminates to avoid detection.
2. **Data Collection**:
   - The malware collects data from various sources, including:
     - **Browsers**: Chrome, Opera, Opera GX, Microsoft Edge.
     - **Messengers**: WhatsApp, Telegram, Skype, Discord.
     - **Gaming Platforms**: Riot Games, Epic Games, Minecraft, Steam, GrowTopia.
     - **Cryptocurrency Wallets**: Armory, ByteCoin, Liberty, Ethereum, Electrum, Atomic, Guarda, Coinomi, Exodus.

- **System Information**: Product keys, IP addresses, task lists, antivirus information.

3. **Data Exfiltration**:

   The stolen data is compressed into a ZIP file and exfiltrated using a **Discord webhook**.

   The webhook URL used is:

   ```
   https://discord.com/api/webhooks/1165744386949271723/kFr6Cc0DSTK1jB8aV3820mBxji06gF2KorUuO2Rd2ckLkhUEHxdi6kv6UHwgJ_W82fgZ
   ```

4. **Cleanup**:

   - After exfiltration, the malware deletes the collected data and the ZIP file to cover its tracks.

Questions and Answers:

Question 1: What is the DLL that has the stealer code?

```
Colorful.dll
```

Question 2: What is the anti-analysis method used by the malware?

```
IsVirusTotal
```

Question 3: What is the full command used to gather information from the system into the “productkey.txt” file?

```
wmic path softwareLicensingService get OA3xOriginalProductKey >> productkey.txt
```

Question 4: What is the full command used to gather information through the “ips.txt” file?

```
ipconfig /all >> ips.txt
```

Question 5: What is the webhook used by the malware?

https://discord.com/api/webhooks/1165744386949271723/kFr6CcdDSTKj9B8vJ3820mb9j06gF2KorUuO2Rd2cLLklUEHxdI6kvGUHwgJ_W