Days 2 :

HTB/Sherlock

Challenge : BFT

Level : Very Easy

Link: [Hack The Box :: Hack The Box](https://app.hackthebox.com/sherlocks/BFT)

Scenario :

In this Sherlock, you will become acquainted with MFT (Master File Table) forensics. You will be introduced to well-known tools and methodologies for analyzing MFT artifacts to identify malicious activity. During our analysis, you will utilize the MFTECmd tool to parse the provided MFT file, TimeLine Explorer to open and analyze the results from the parsed MFT, and a Hex editor to recover file contents from the MFT.

Tools use : MFTECmd,TimeLine Explorer, Bless or Hexedit,MFTE Explorer

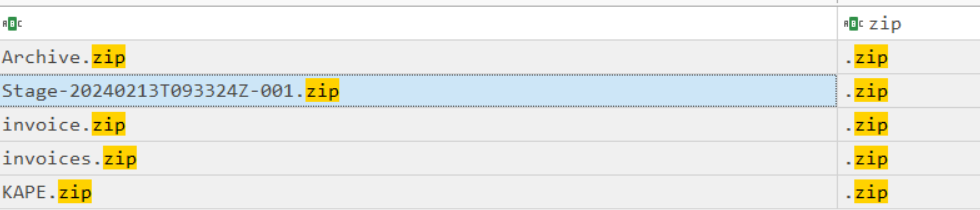
Nhận diện ban đầu :



Hex của nó gần như chẳng có gì.

Q1 : Simon Stark was targeted by attackers on February 13. He downloaded a ZIP file from a link received in an email. What was the name of the ZIP file he downloaded from the link?

- Filter “zip” trong phần Extension, ta có 5 file trong phần kết quả.

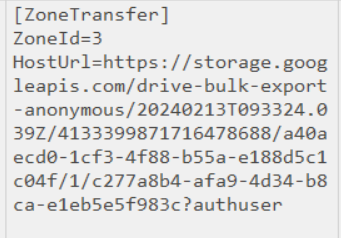


- File đầu tiên có ModifiedTime và CreateTime quá chênh lệch so với trong câu hỏi, nên mình đã loại nó ( hay chính xác hơn là nó sai khi subm ). Thử với file thứ 2 và chính xác.

-> Answer : Stage-20240213T093324Z-001.zip

Q2 : Examine the Zone Identifier contents for the initially downloaded ZIP file. This field reveals the HostUrl from where the file was downloaded, serving as a valuable Indicator of Compromise (IOC) in our investigation/analysis. What is the full Host URL from where this ZIP file was downloaded?

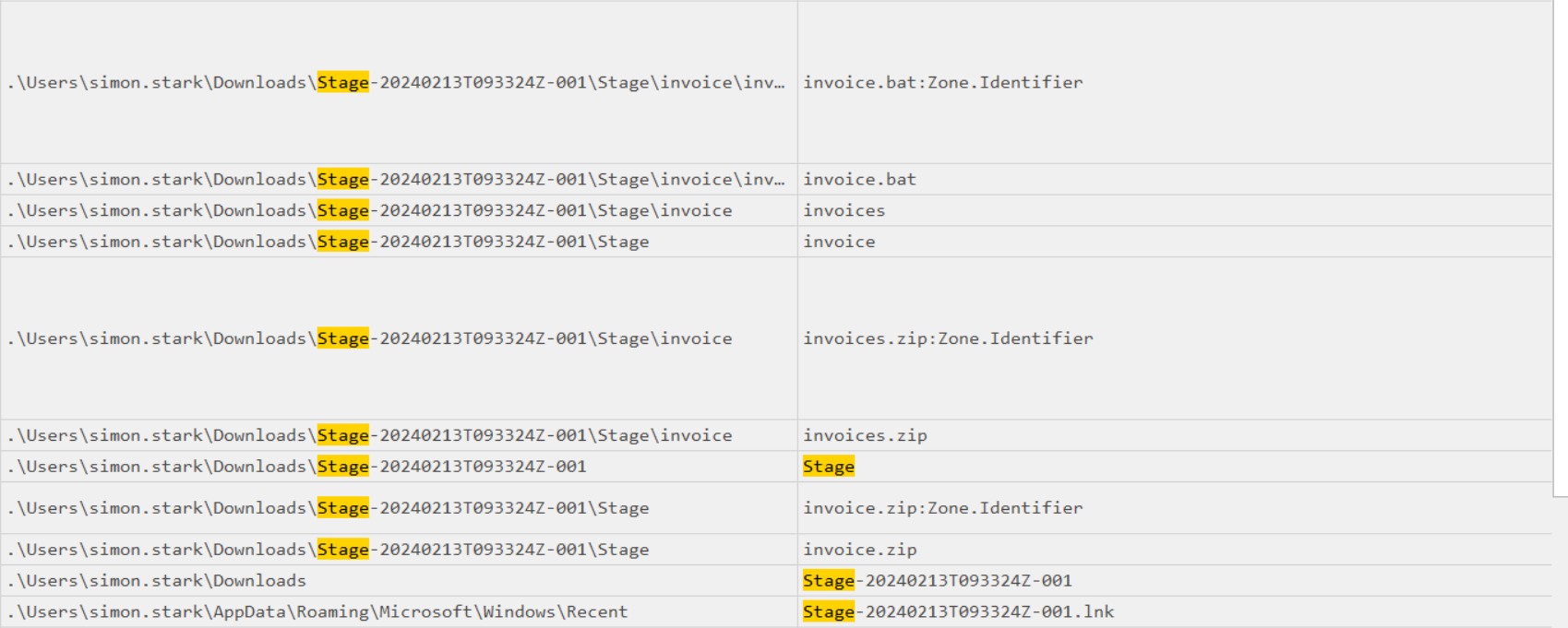
- Mình lọc theo 2 trường : Last Modified 0x10 hoặc Last Modified 0x30 đều được, và File Name = Stage + “ Identi “. Theo đó ta lọc ra được dòng duy nhất với thông tin cần tìm :



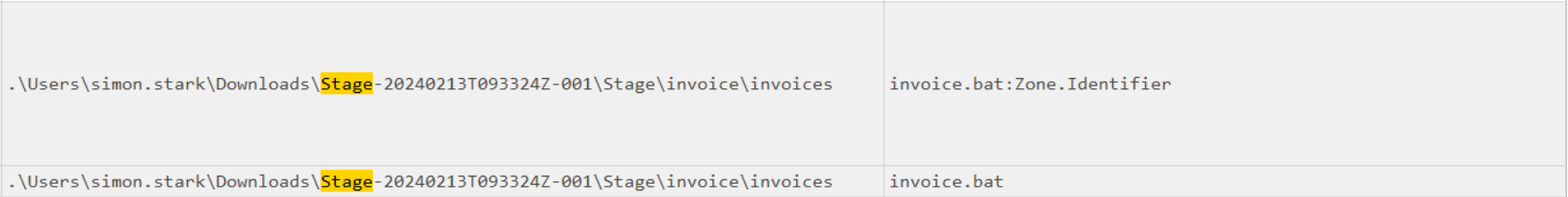
-> Answer : <https://storage.googleapis.com/drive-bulk-export-anonymous/20240213T093324.039Z/4133399871716478688/a40aecd0-1cf3-4f88-b55a-e188d5c1c04f/1/c277a8b4-afa9-4d34-b8ca-e1eb5e5f983c?authuser>

Q3 : What is the full path and name of the malicious file that executed malicious code and connected to a C2 server?

- Để mã độc có thể thực thi, chắc chắn file được tải xuống phải được mở (unzip). Theo đó, ta lọc theo từ khóa “Stage” và LastModified = “13/02/2024”. Nhận được một loạt kết quả :



- Có thể thấy 2 đường dẫn sau là đáng chú ý nhất :



- Trong đó chỉ có 1 file duy nhất có khả năng thực hiện mã thực thi, đó là invoice.bat

->Answer : “C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices\invoice.bat”

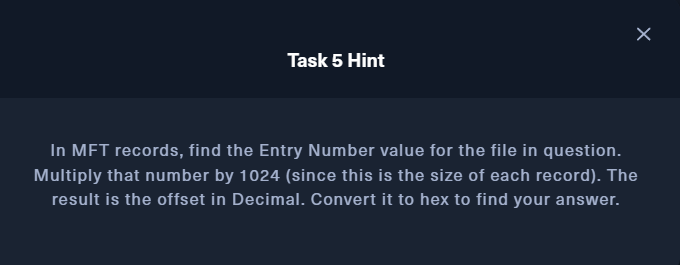
Q4 : Analyze the $Created0x30 timestamp for the previously identified file. When was this file created on disk?

- Từ file tìm thấy, ta có thể lấy thông tin từ trường Created0x30 và nhận được kết quả

-> Answer : 2024-02-13 16:38:39

Q5 : Finding the hex offset of an MFT record is beneficial in many investigative scenarios. Find the hex offset of the stager file from Question 3.

- Từ hint :



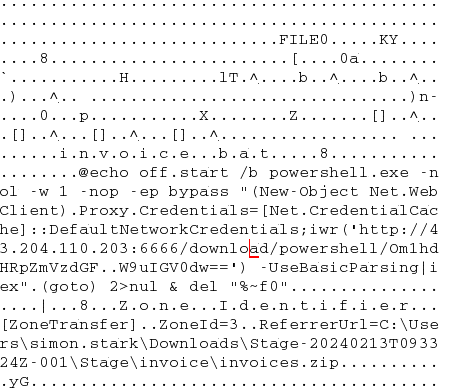
- Nếu bạn thắc mắc tại sao lại là 1024, có thể đây là một phần của đáp án : [windows - Kích thước tối đa của tệp có thể được lưu trữ hoàn toàn trong Bảng tệp chính NTFS (MFT) - Siêu người dùng (superuser.com)](https://superuser.com/questions/1185461/maximum-size-of-file-that-can-be-stored-entirely-in-ntfs-master-file-table-mft)

- Quay lại với câu hỏi, thực hiện tính toán một chút, ta nhận được kết quả.

-> Answer : 16E3000

Q6 : Each MFT record is 1024 bytes in size. If a file on disk has smaller size than 1024 bytes, they can be stored directly on MFT File itself. These are called MFT Resident files. During Windows File system Investigation, its crucial to look for any malicious/suspicious files that may be resident in MFT. This way we can find contents of malicious files/scripts. Find the contents of The malicious stager identified in Question3 and answer with the C2 IP and port.

- Để tìm nội dung, ta dùng kết quả của Q5. Dùng bless và tìm đến offset ở Q5, ta có thể thấy :



-> Answer : 43.204.110.203:6666