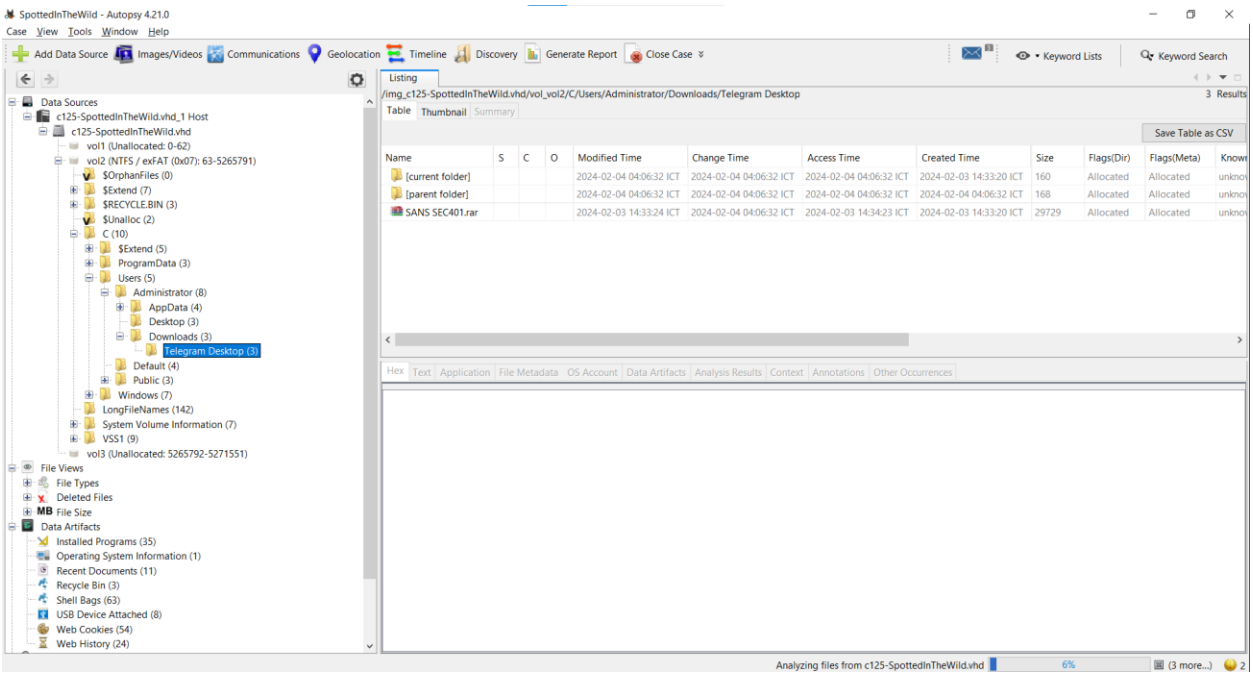
SpottedInTheWild Blue Team Lab

Q1. In your investigation into the FinTrust Bank breach, you found an application that was the entry point for the attack. Which application was used to download the malicious file?



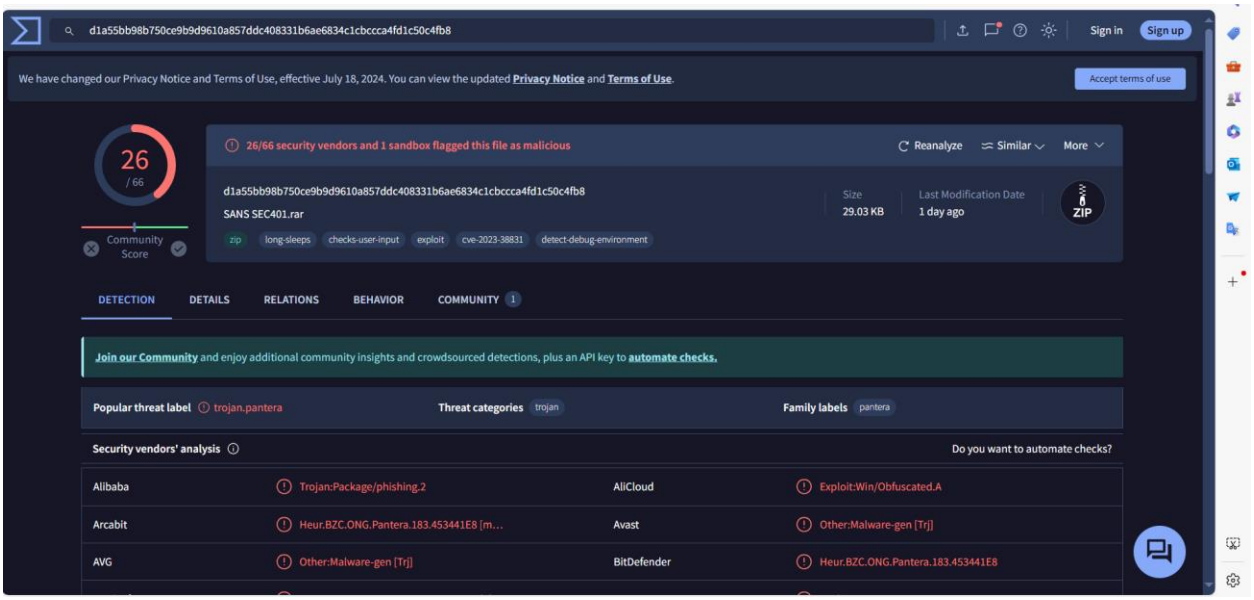
Ở đây em thấy có 1 file được tải về từ **telegram.** Vậy đích thị telegram là công cụ mà các kẻ tấn công đã sử dụng để tải xuống file độc hại

Q2. Finding out when the attack started is critical. What is the UTC timestamp for when the suspicious file was first downloaded?

Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
2024-02-04 04:06:32 ICT	2024-02-04 04:06:32 ICT	2024-02-03 14:33:20 ICT	160	Allocated	Allocated	unknown	/img_c125-SpottedInTheWild.vhd/vol_vol2/C/Users/
2024-02-04 04:06:32 ICT	2024-02-04 04:06:32 ICT	2024-02-04 04:06:32 ICT	168	Allocated	Allocated	unknown	/img_c125-SpottedInTheWild.vhd/vol_vol2/C/Users/
2024-02-04 04:06:32 ICT	2024-02-03 14:34:23 ICT	2024-02-03 14:33:20 ICT	29729	Allocated	Allocated	unknown	/img_c125-SpottedInTheWild.vhd/vol_vol2/C/Users/

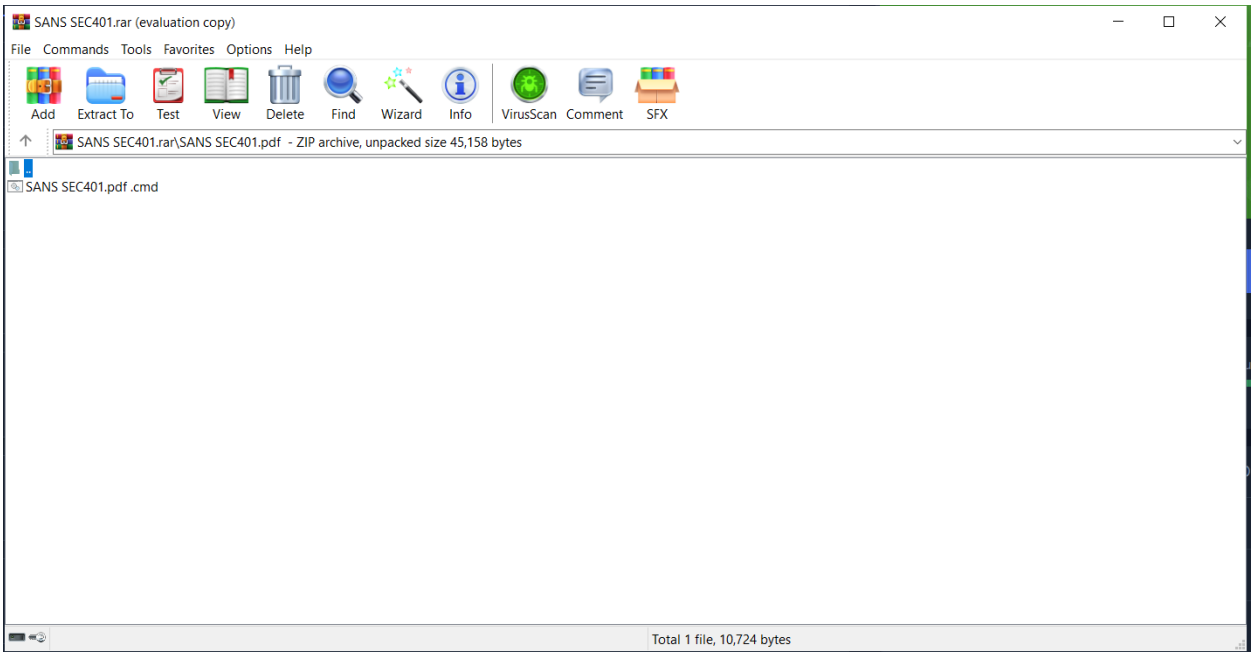
Ở đây em thấy tệp **SANS SEC401.rar** được tải xuống vào ngày **03-02-2024** vào lúc **14:34:23** theo giờ ICT. Và nếu đổi qua giờ UTC là **2024-02-03 07:33:20**

Q3. Knowing which vulnerability was exploited is key to improving security. What is the CVE identifier of the vulnerability used in this attack?



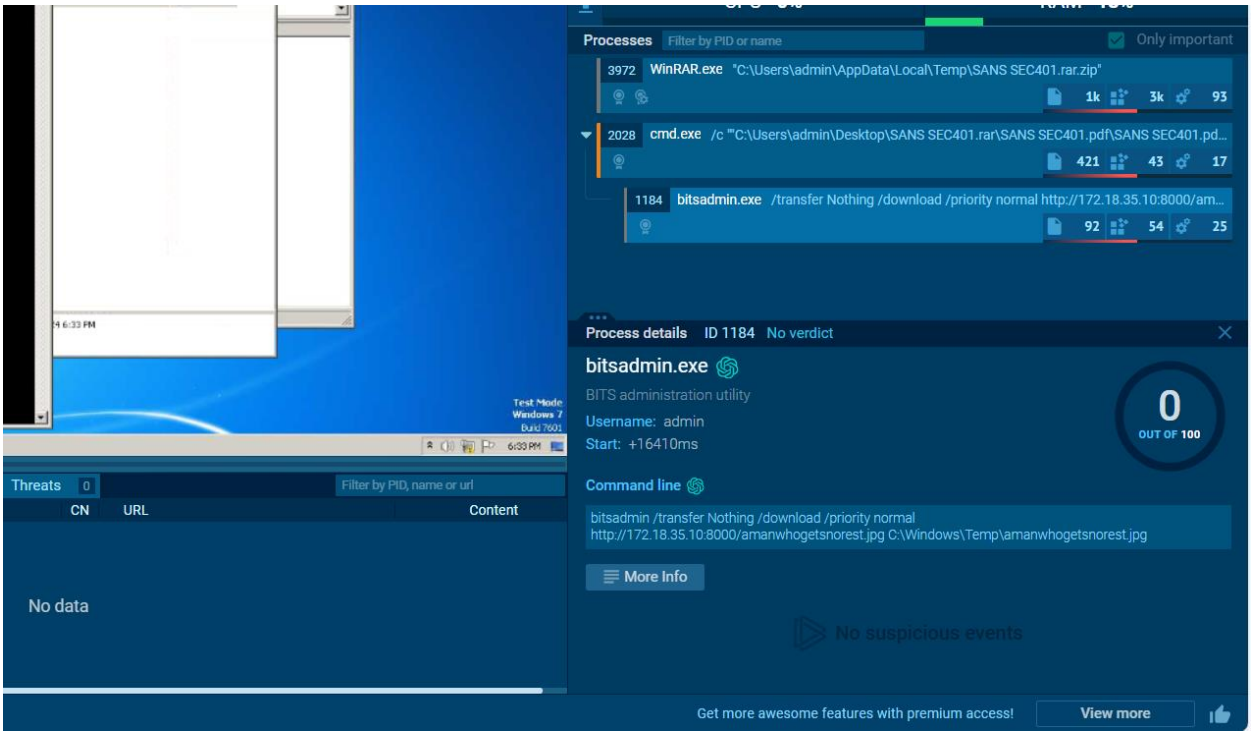
Em đã upload file lên virustotal để biết được CVE và đó là **CVE-2023-38831**

Q4. In examining the downloaded archive, you noticed a file in with an odd extension indicating it might be malicious. What is the name of this file?



Ở đây em thấy rằng trong file **SANS SEC401.rar** có 1 file thực thi chính là file **SANS SEC401.pdf .cmd.**
Vậy kết quả của câu này là **SANS SEC401.pdf .cmd**

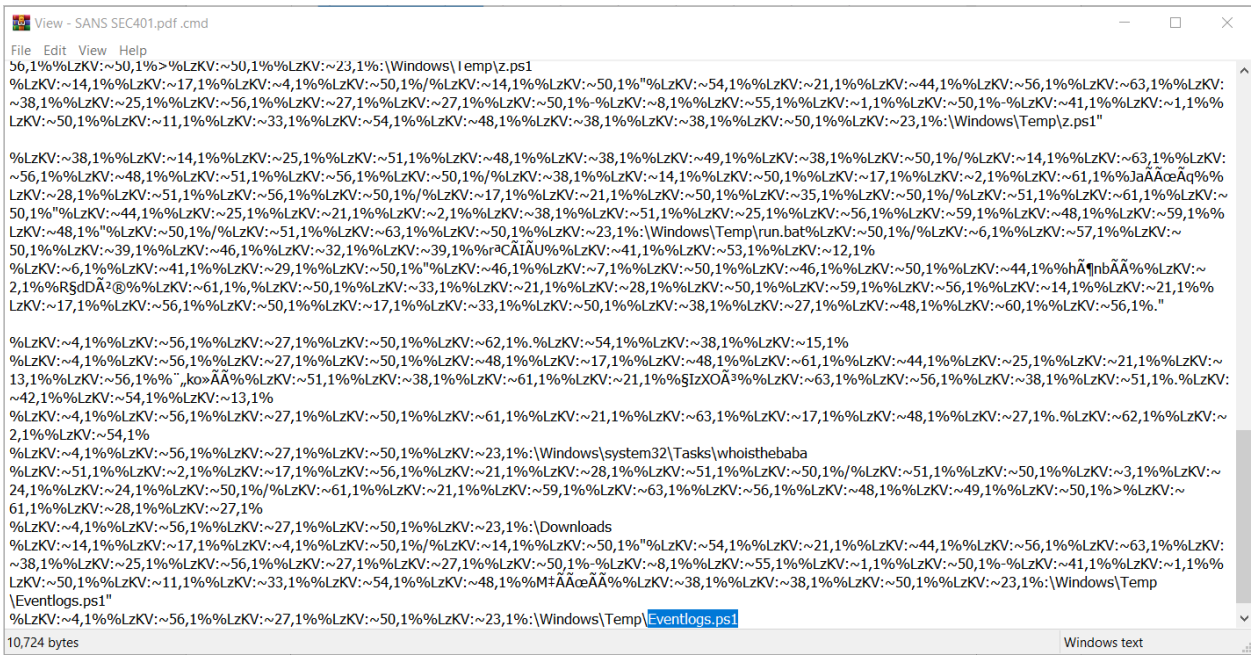
Q5. Uncovering the methods of payload delivery helps in understanding the attack vectors used. What is the URL used by the attacker to download the second stage of the malware?



Ở đây em thấy file đầu tiên nó đang tải xuống từ URL mà kẻ tấn công sử dụng để tải xuống giai đoạn thứ hai của phần mềm độc hại.

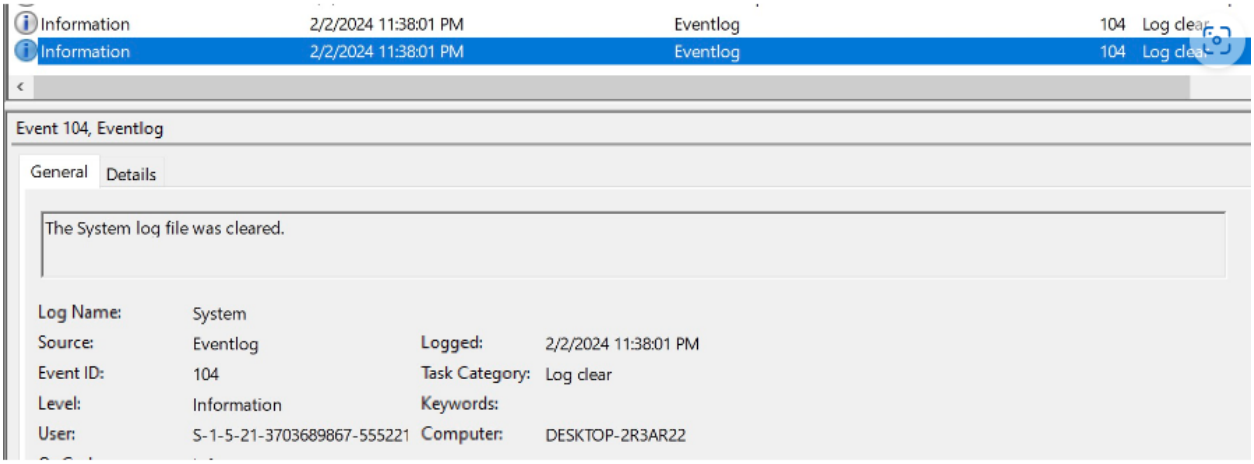
Đáp án là **http://172.18.35.10:8000/amanwhogetsnorest.jpg**

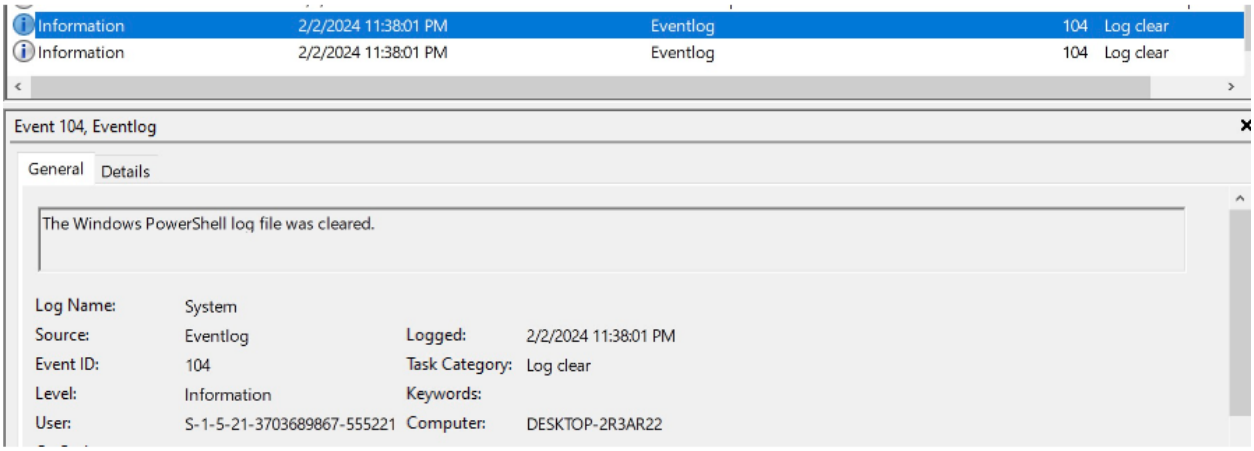
Q6. To further understand how attackers cover their tracks, identify the script they used to tamper with the event logs. What is the script name?



Ở đây em đã xác định tập lệnh mà chúng sử dụng để giả mạo nhật ký sự kiện là **Eventlogs.ps1**

Q7. Knowing when unauthorized actions happened helps in understanding the attack. What is the UTC timestamp for when the script that tampered with event logs was run?

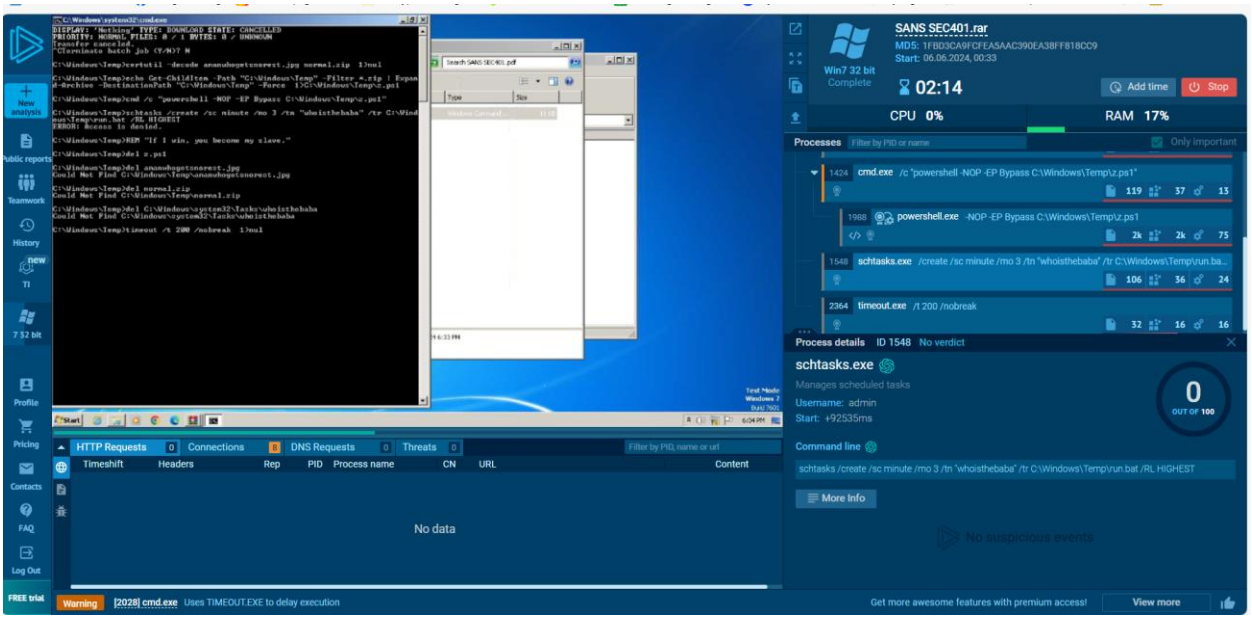




Khi cuộc tấn công đầu tiên xảy ra em thấy file đầu tiên chạy lúc 11:38:01

Vậy thời gian ở đây sẽ là **2024-02-03 07:38:01**

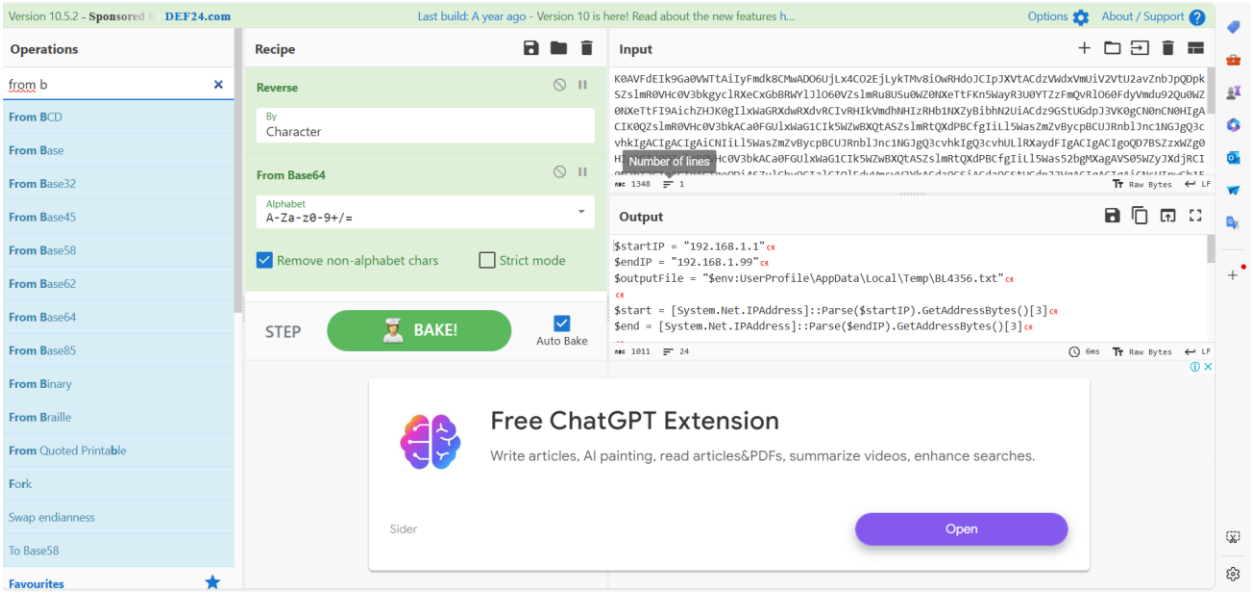
Q8. We need to identify if the attacker maintained access to the machine. What is the command used by the attacker for persistence?



Ở đây em thấy các kẻ tấn công đã chạy câu lệnh **schtasks /create /sc minute /mo 3 /tn "whoisthebaba" /tr C:\Windows\Temp\run.bat /RL HIGHEST**.

- Lệnh này sẽ tạo một tác vụ theo lịch trình có tên là "whoisthebaba" trên hệ thống Windows. Tác vụ này sẽ thực thi tập tin run.bat nằm trong thư mục C:\Windows\Temp mỗi 3 phút một lần. Tác vụ này sẽ được thực thi với mức độ ưu tiên cao nhất (quyền admin).

Q9. To understand the attacker's data exfiltration strategy, we need to locate where they stored their harvested data. What is the full path of the file storing the data collected by one of the attacker's tools in preparation for data exfiltration?



Ở đây em thấy rằng file run.ps đã được chạy. Sau khi reverse khi đó và em có đáp án của câu này là **C:\Users\Administrator\AppData\Local\Temp\BL4356.txt**