Kịch bản: Vào ngày 24 tháng 8, Bob Smith (sử dụng máy tính chạy Windows 10 có tên we8105desk) đã quay lại bàn làm việc của mình sau khi tập gym, và thấy loa máy tính phát ra tiếng kêu lạ, hình ảnh nền trên màn hình của anh ấy đã thay đổi và các tệp của anh ấy không thể truy cập được. Alice, đồng nghiệp của anh đã từng thấy điều này trước đây... cô đoán máy anh đã bị dính ransomware. Sau khi nói chuyện với Bob, Alice biết được rằng Bob đã tìm thấy một chiếc USB ở bãi đậu xe sáng nay, anh đã cắm nó vào máy tính để kiểm tra và vô tình mở một tài liệu word trên ổ USB có tên "Miranda\_Tate\_unveiled.dotm". Nắm bắt được tình hình trên, Alice bắt tay vào điều tra nguyên nhân...

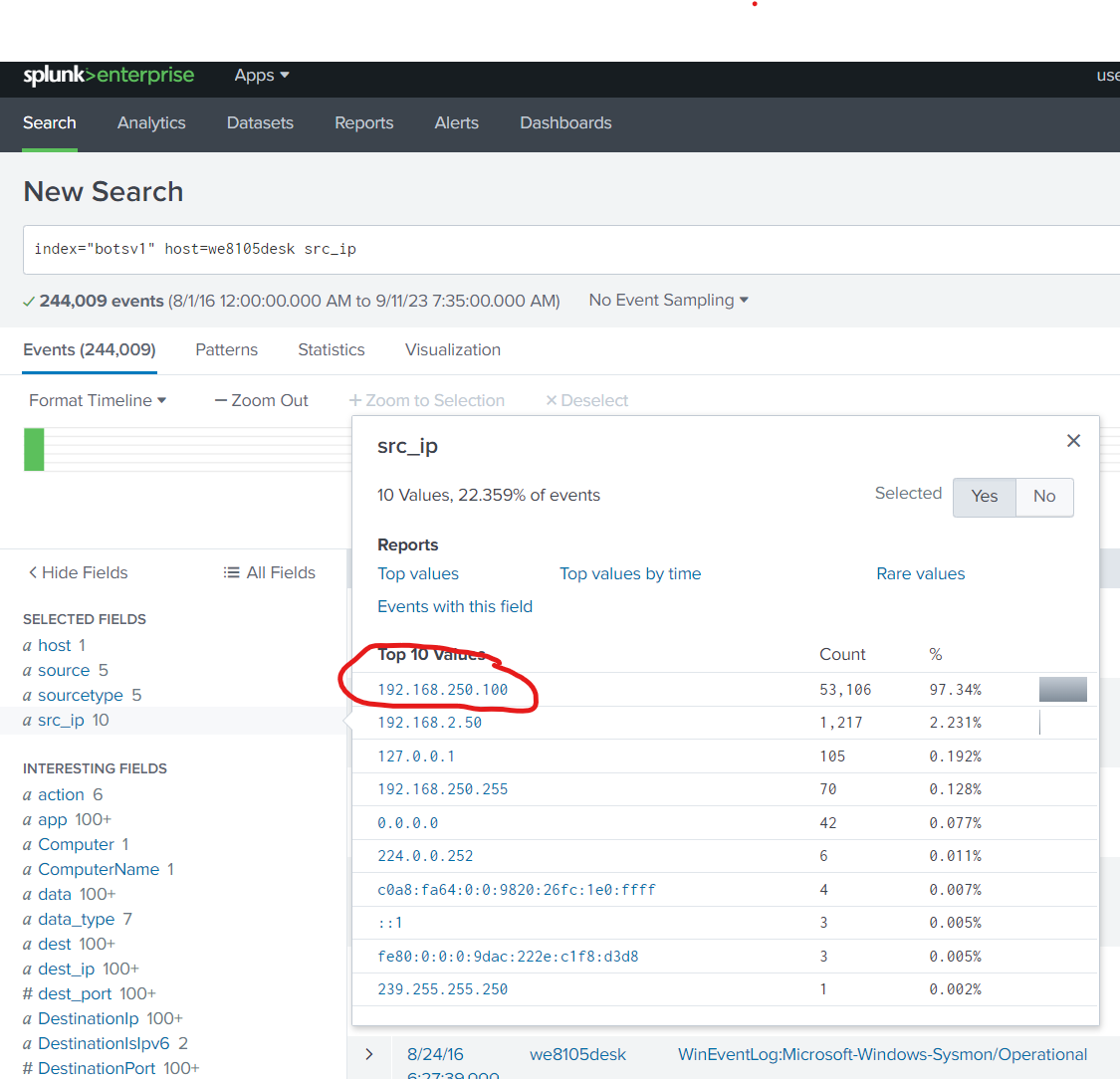
1. Đâu là địa chỉ IPv4 gần đúng nhất của user we8105desk vào ngày 24AUG2016

Query :

Index=”botsv1”

Host=we8105desk

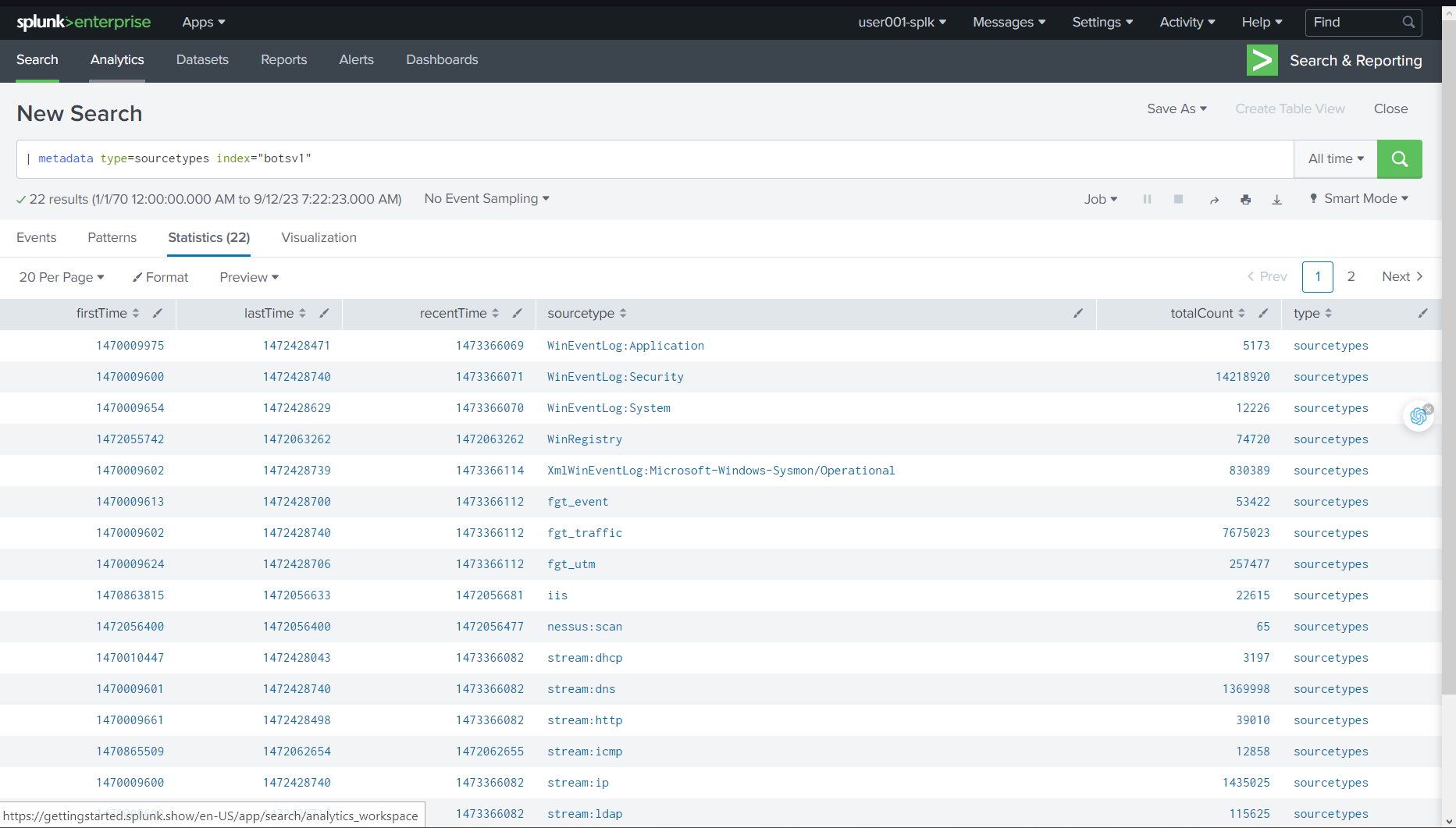
Src\_ip

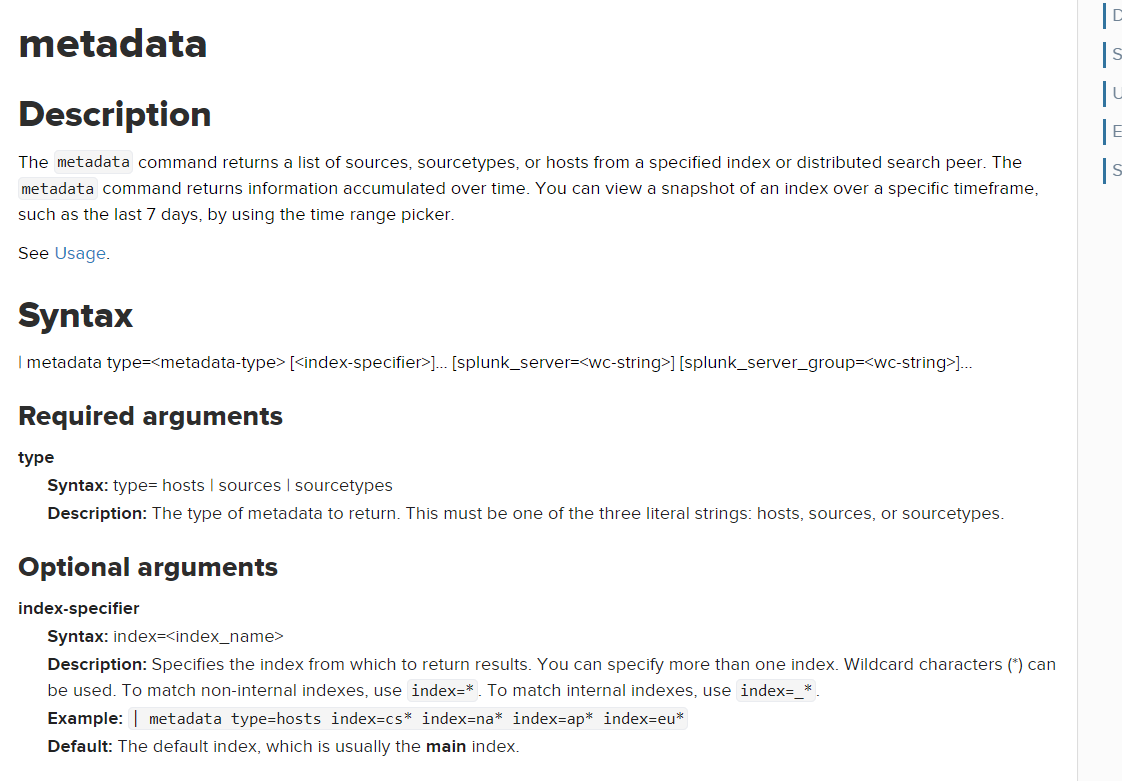


192.168.250.100

C2:

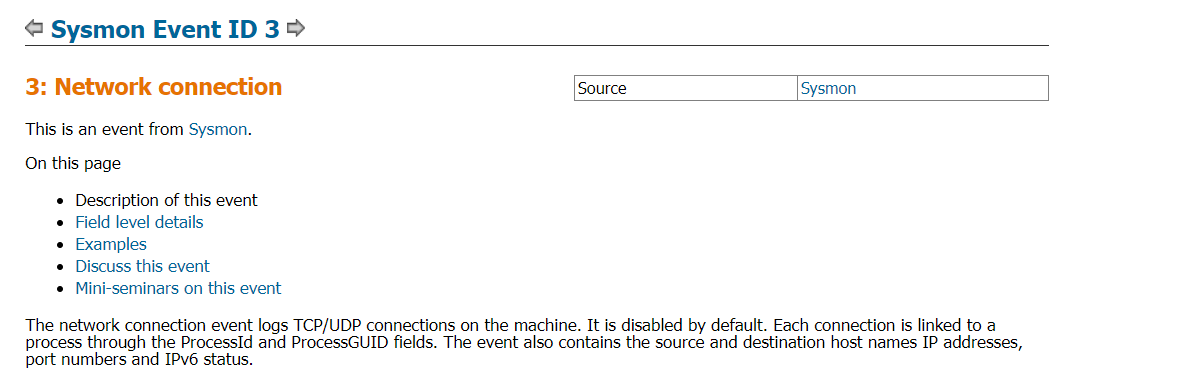
| metadata type=sourcetypes index="botsv1"



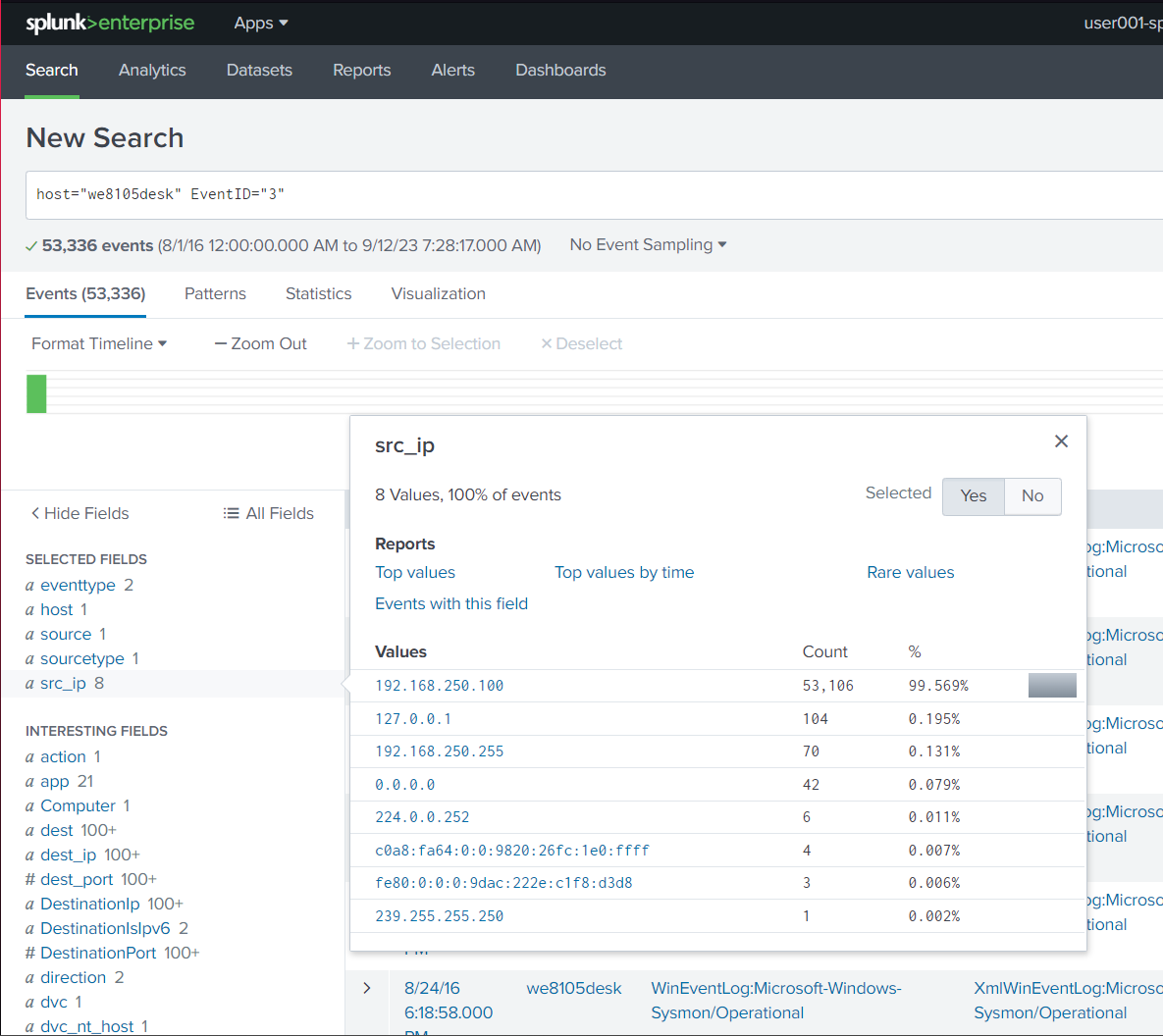


Thấy rất nhiều logs từ Sysmon, Fortigate firewalls, IIS và NIDS từ Suricata

Thử bắt đầu tìm kiếm từ Sysmon event id 3



host=”we8105desk” EventID=”3”

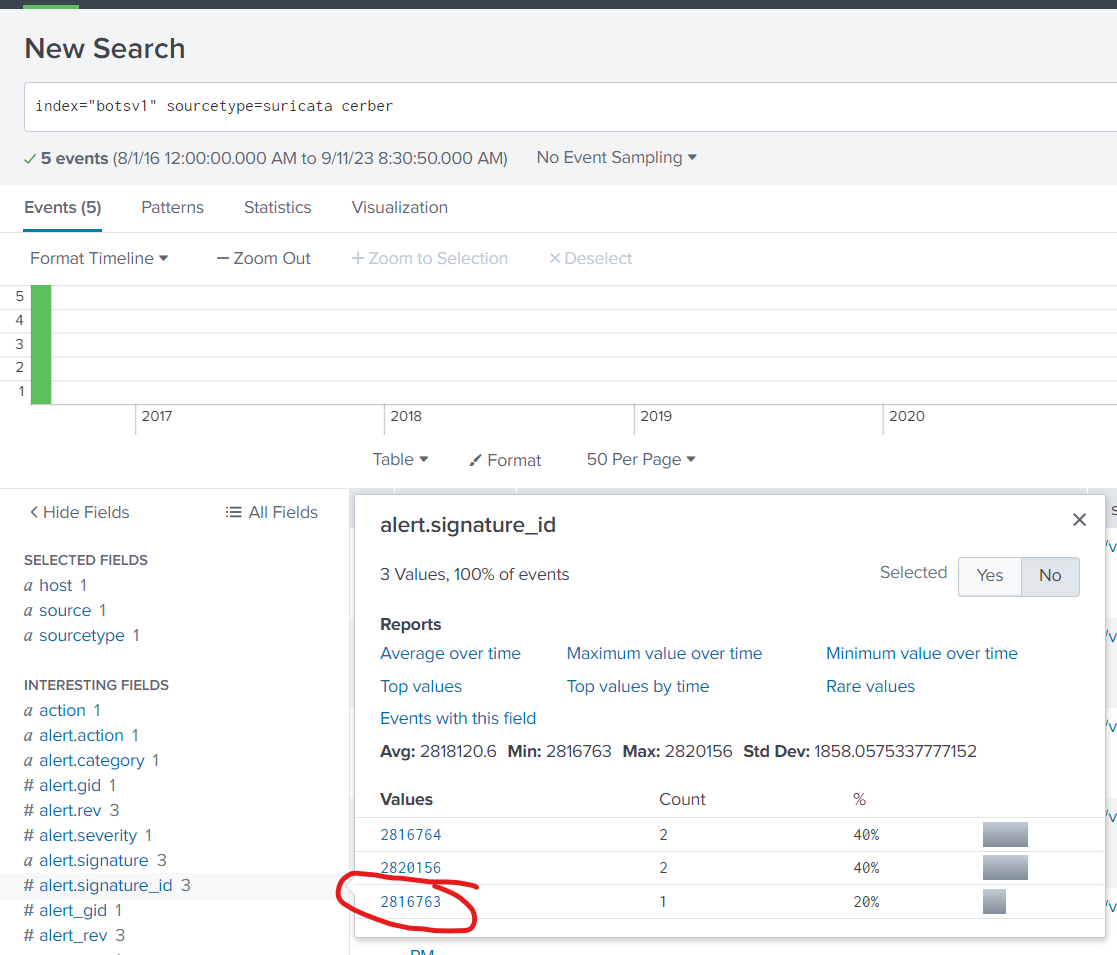


2. Trong số các signature của suricata mà phát hiện ra mã độc Cerber, đâu là cảnh báo được gửi ít nhất? (Chỉ submit giá trị của signature ID vào câu trả lời)

Query :

Index=”botsv1”

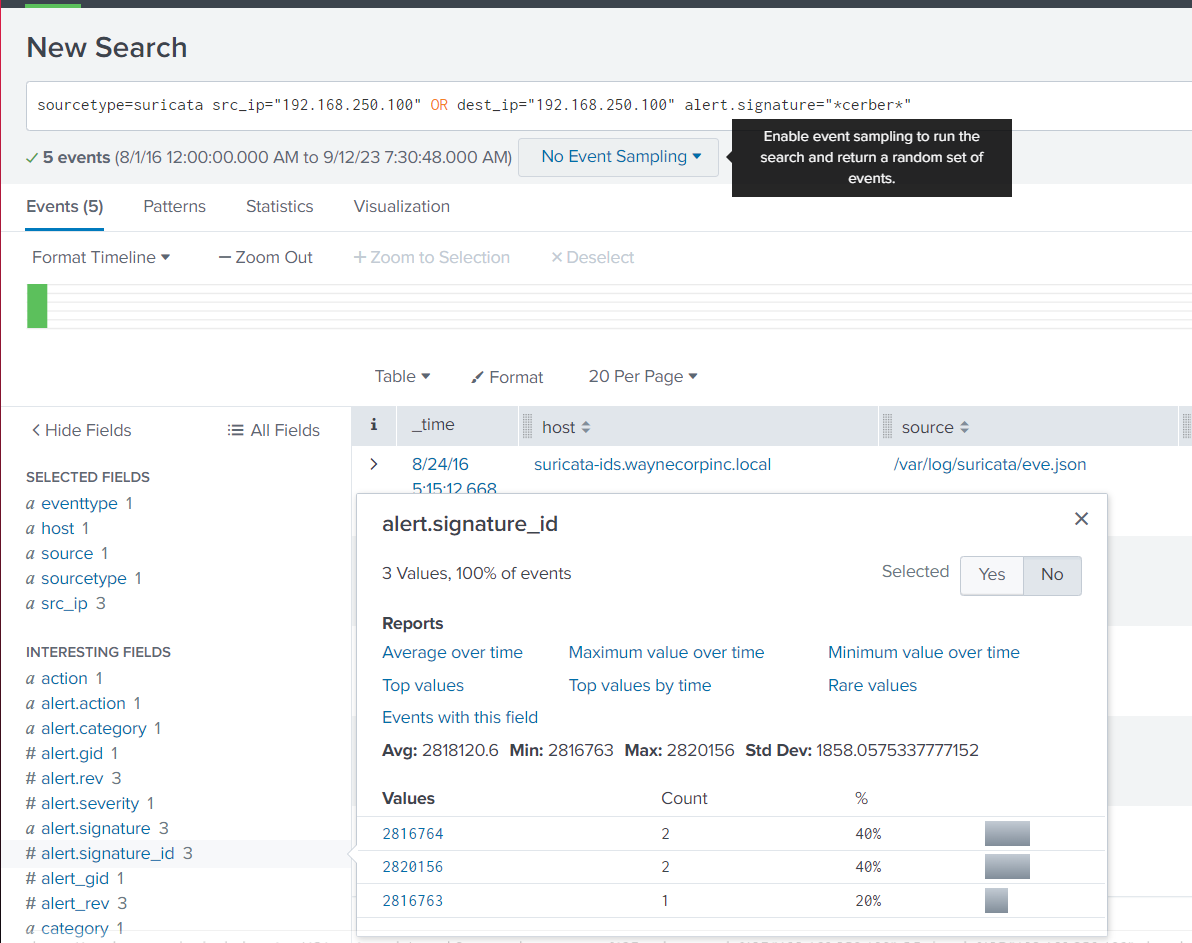
Sourcetype = suricata cerber



2816763

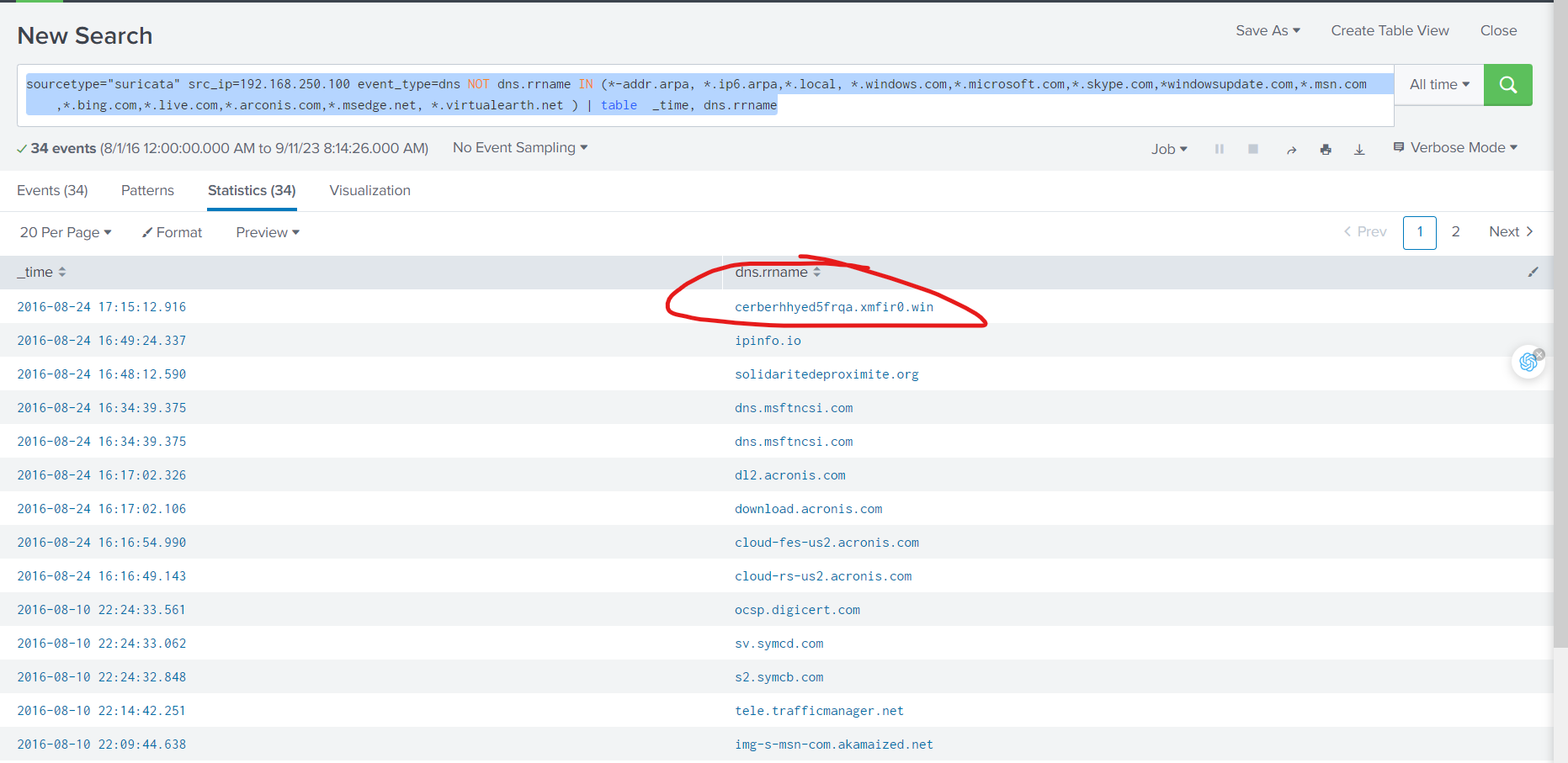
C2:

Query : sourcetype=suricata src\_ip="192.168.250.100" OR dest\_ip="192.168.250.100" alert.signature="\*cerber\*"

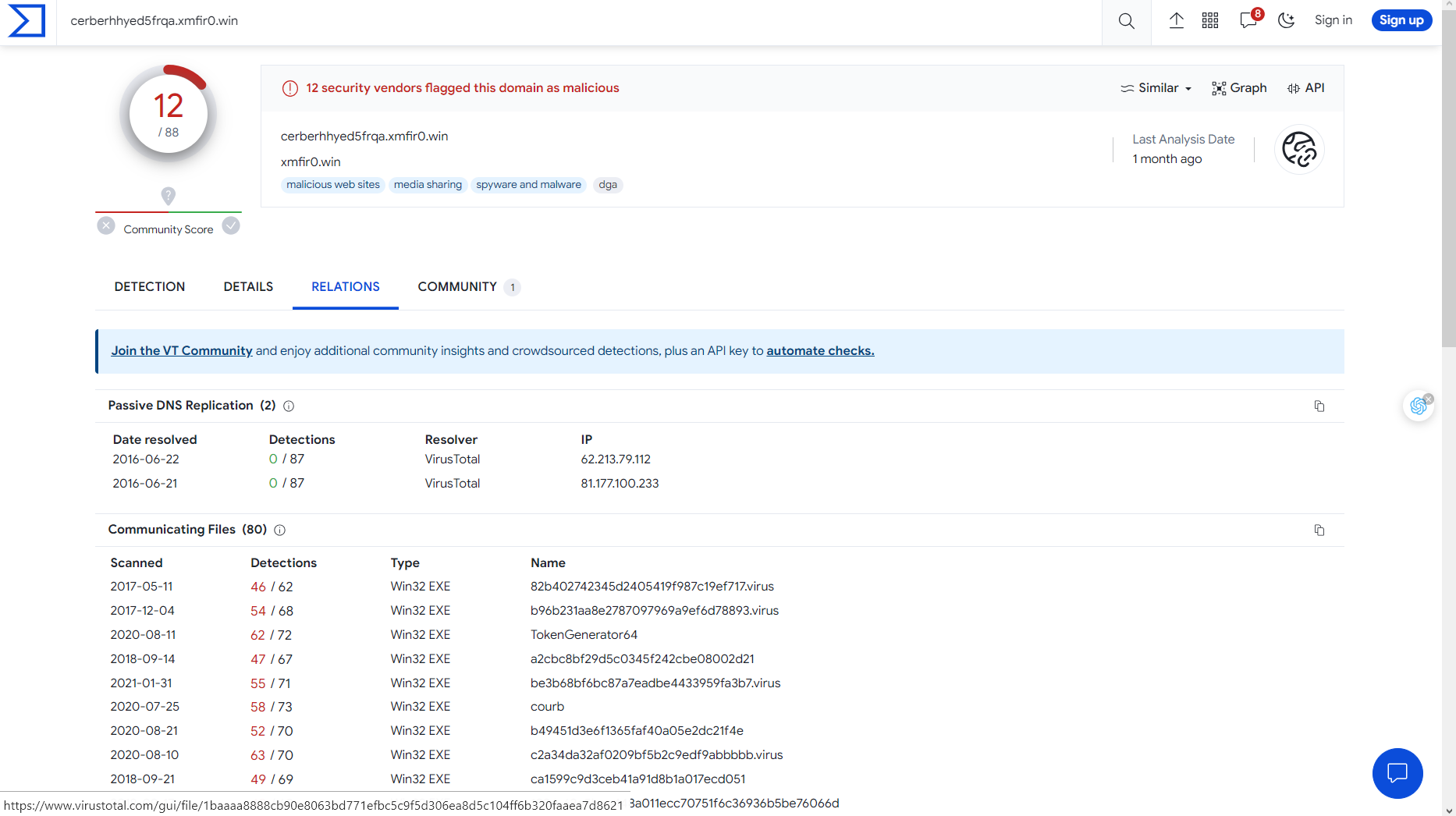


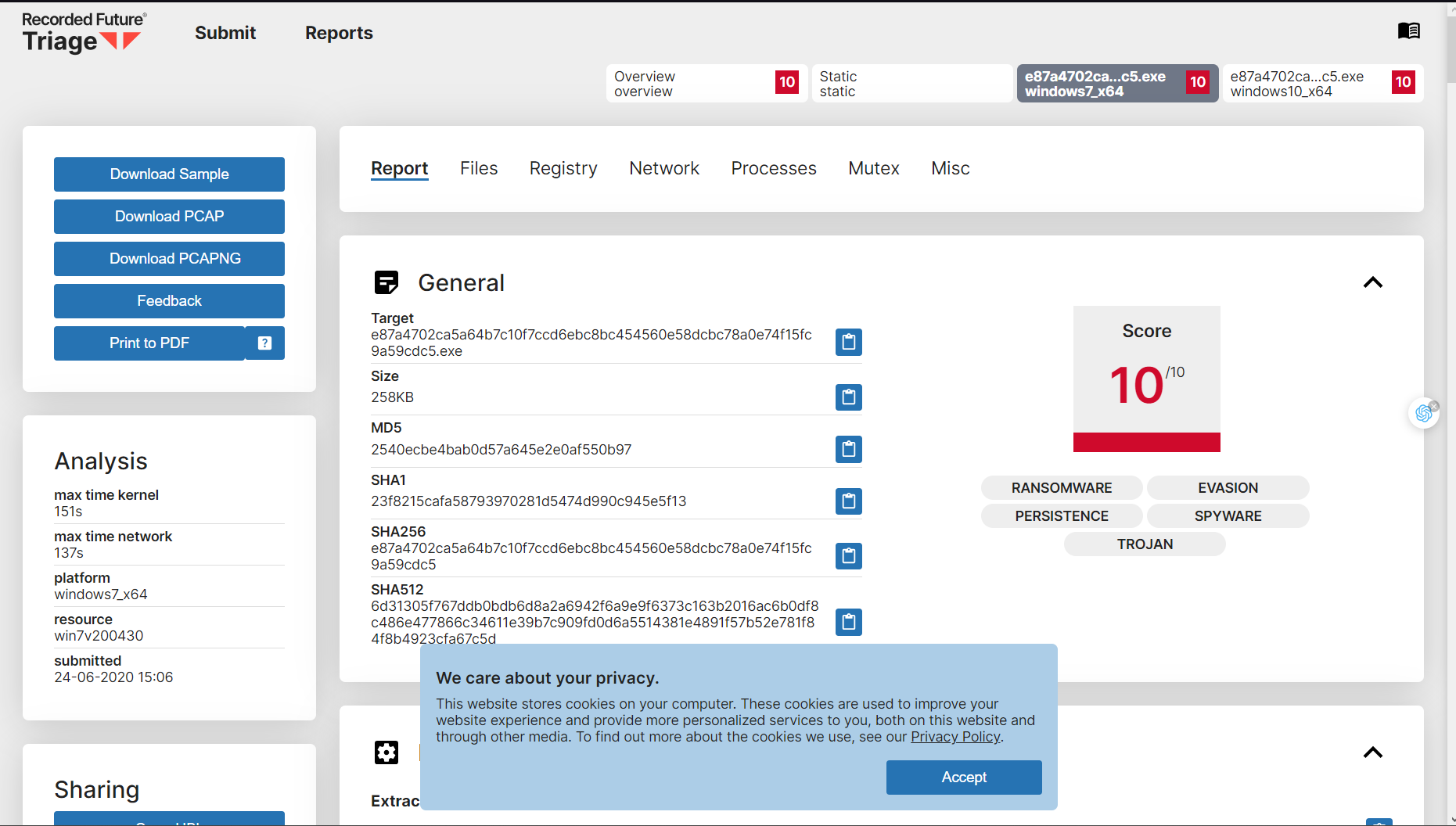
3. Tên miền nào mà mã độc Cerber cố gắng chuyển hướng người dùng khi kết thúc quá trình mã hóa?

Tìm tất cả truy vấn dns xuất phát từ máy tính 192.168.250.100



Check từng cái một thì có Domain **cerberhhyed5frqa.xmfir0.win**

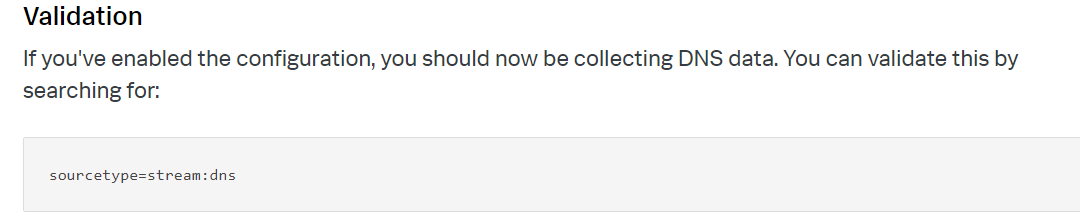




**cerberhhyed5frqa.xmfir0.win**

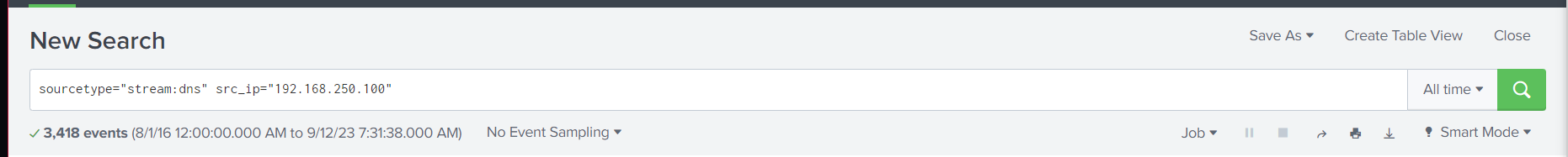
**C2:**

**Đầu tiên muốn truy cập dữ liệu data của dns dùng lệnh**

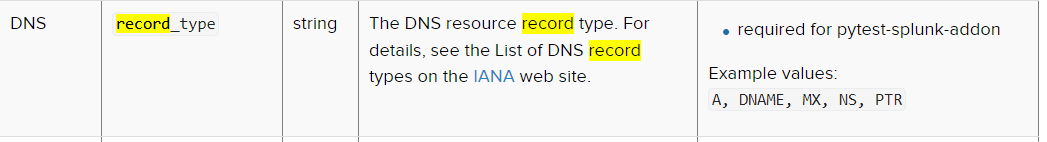


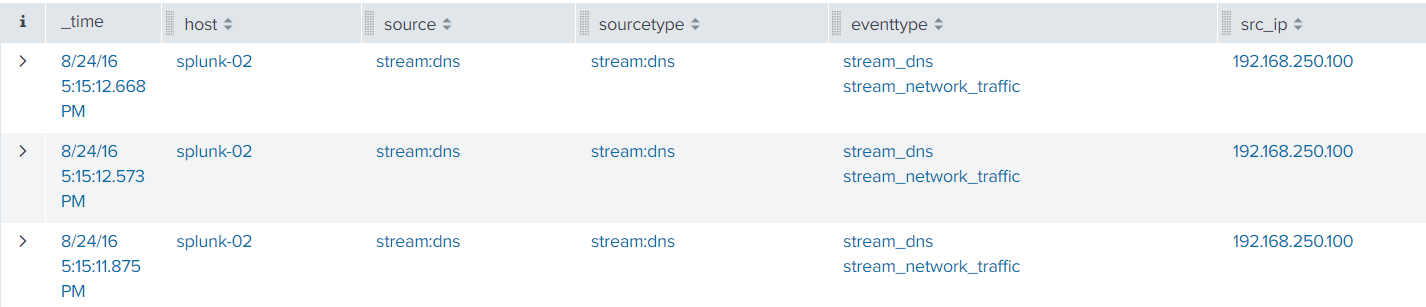
+ với địa chỉ ip mình tìm được là 192.168.250.100

Ta có được 3418 events

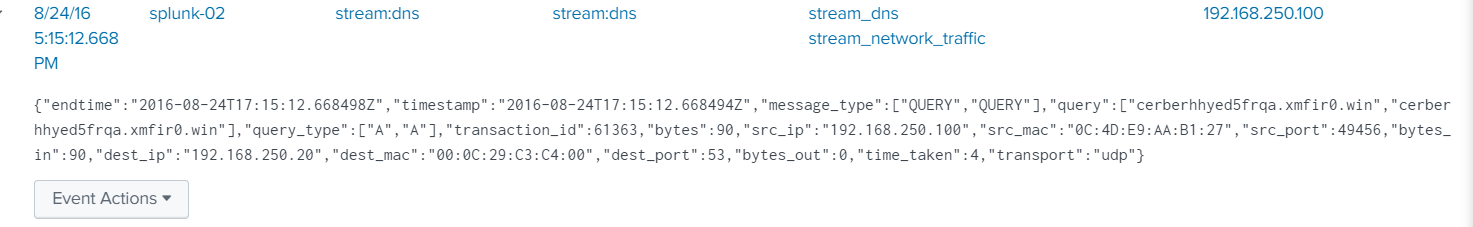


Sau một hồi tra lệnh thì ta có thể dung được lệnh truy ra address



* record\_type A
* và thấy được 3 events
* 

xem chi tiết từng cái 1 thì thấy địa chỉ domain là **cerberhhyed5frqa.xmfir0.win**

* 

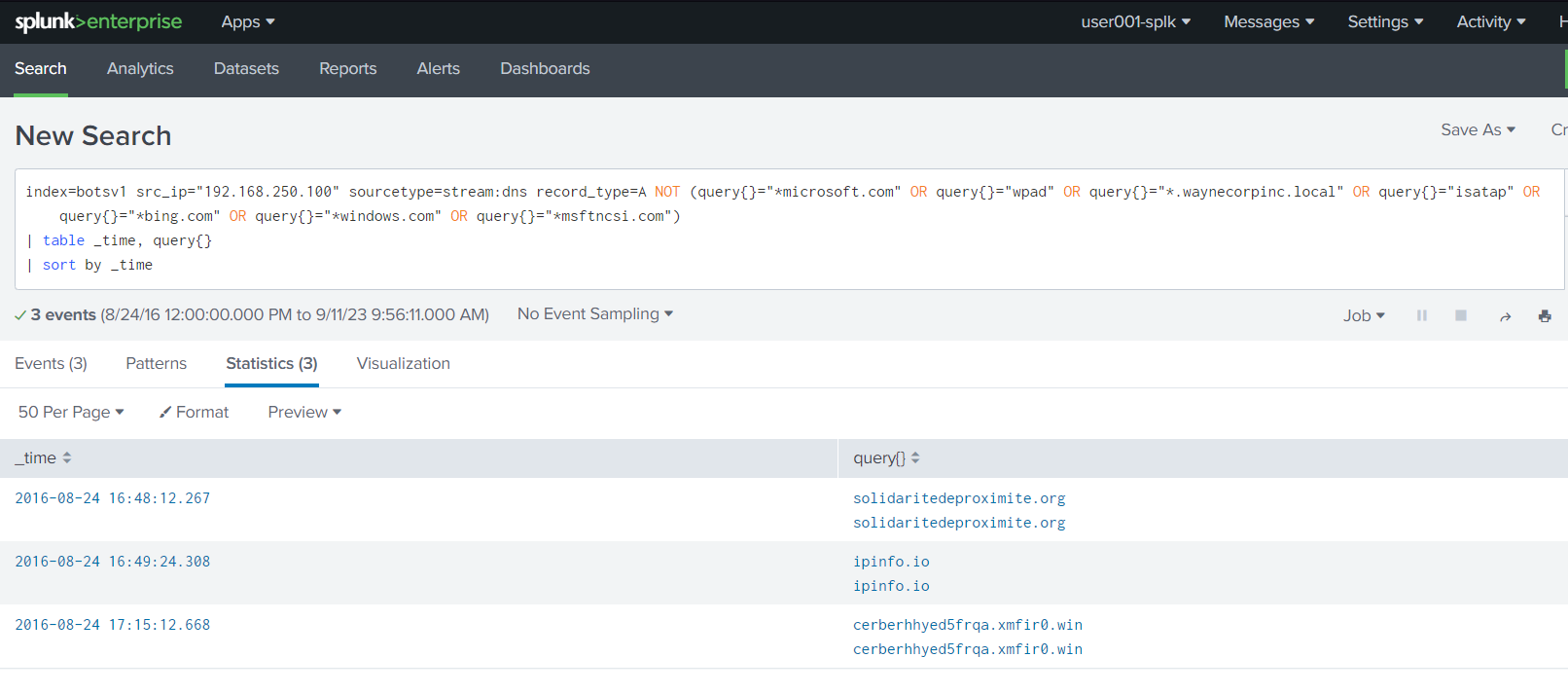
4. Đâu là tên miền bị nghi ngờ đầu tiên mà user we8105desk truy cập ngày 24AUG2016?

Query :

index="botsv1" source="stream:dns" src\_ip="192.168.250.100" NOT query IN ("\*.local", "\*.arpa", "\*.microsoft.com", "\*.acronis.com", "\*msn.com", "\*.windows.com", "\*.windowsupdate.com", "\*.live.com", "\*.edge.com", "\*.bing.com") AND query=\*.\*

| table \_time, query

| sort -\_time| sort by \_time



solidaritedeproximite.org

5. Trong quá trình lây nhiễm Cerber lần đầu, một file VBS sẽ được chạy. Toàn bộ tập lệnh trong quá trình thực thi này được khởi chạy bởi 1 tiến trình .exe, có thể được tìm thấy trong một trường trong Splunk. Độ dài của giá trị của trường này là gì? Hướng dẫn trả lời: Nhập số ký tự (tức "độ dài") của trường.

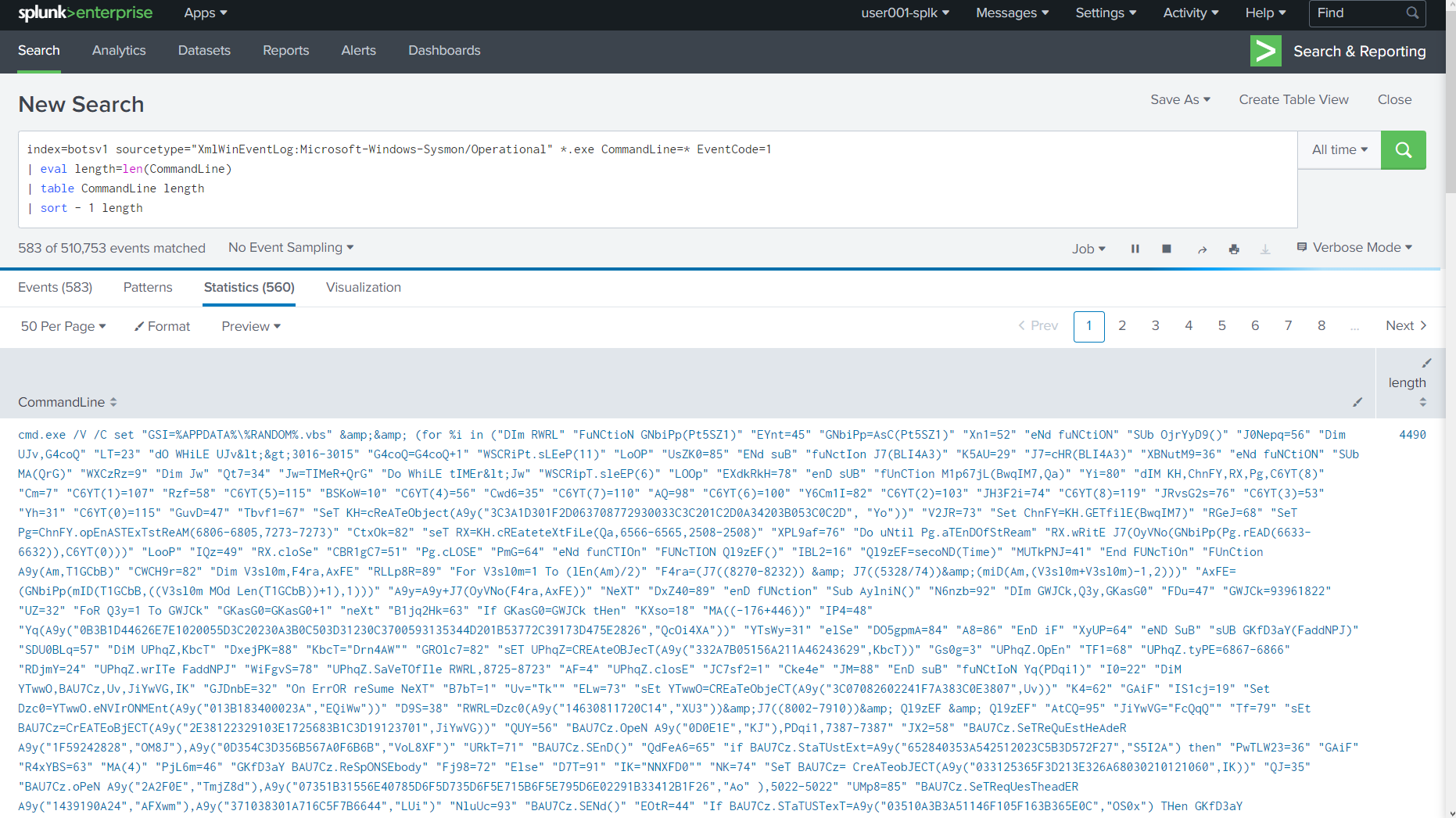
Query :

index=botsv1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" \*.exe CommandLine=\* EventCode=1

| eval length=len(CommandLine)

| table CommandLine length

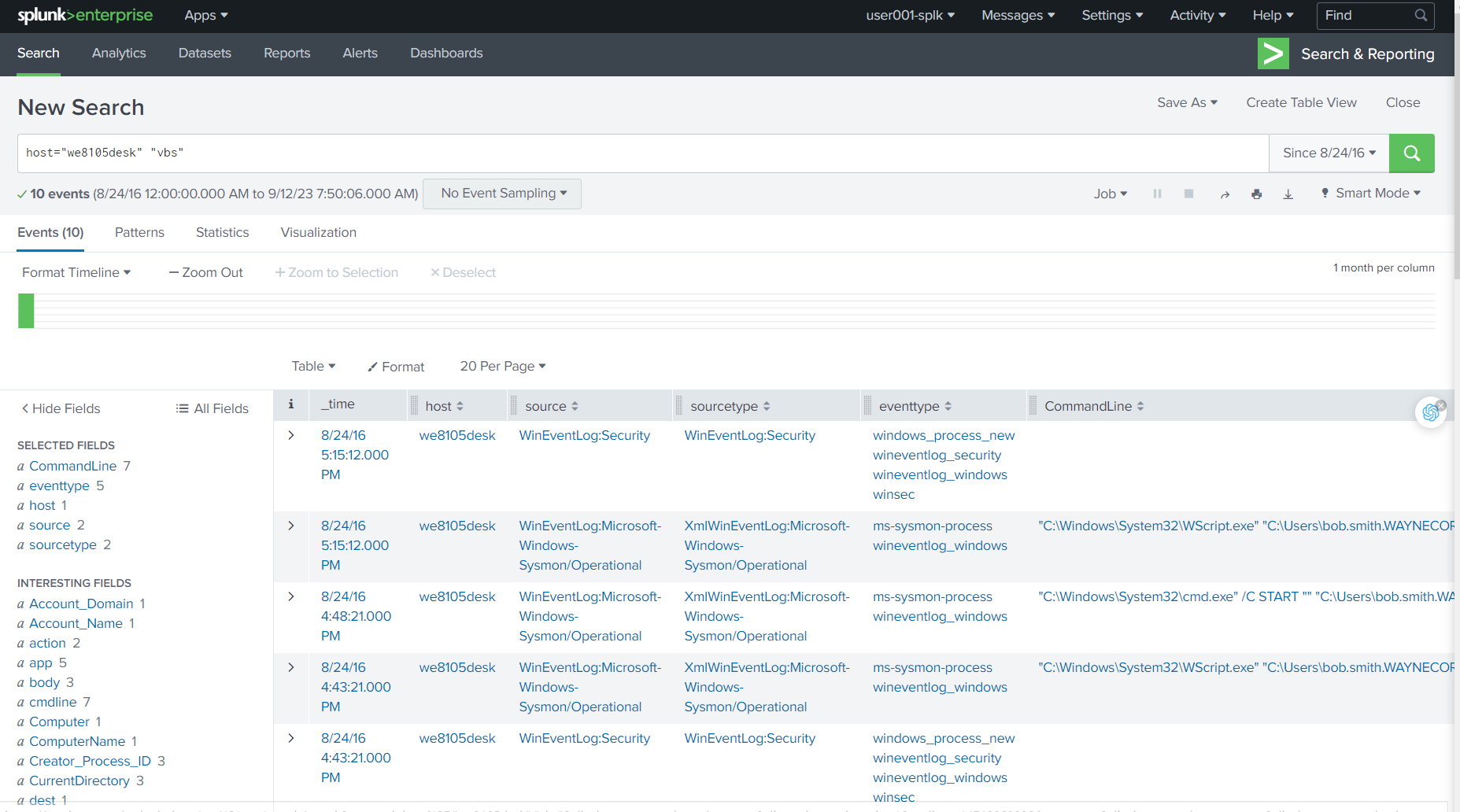
| sort - 1 length



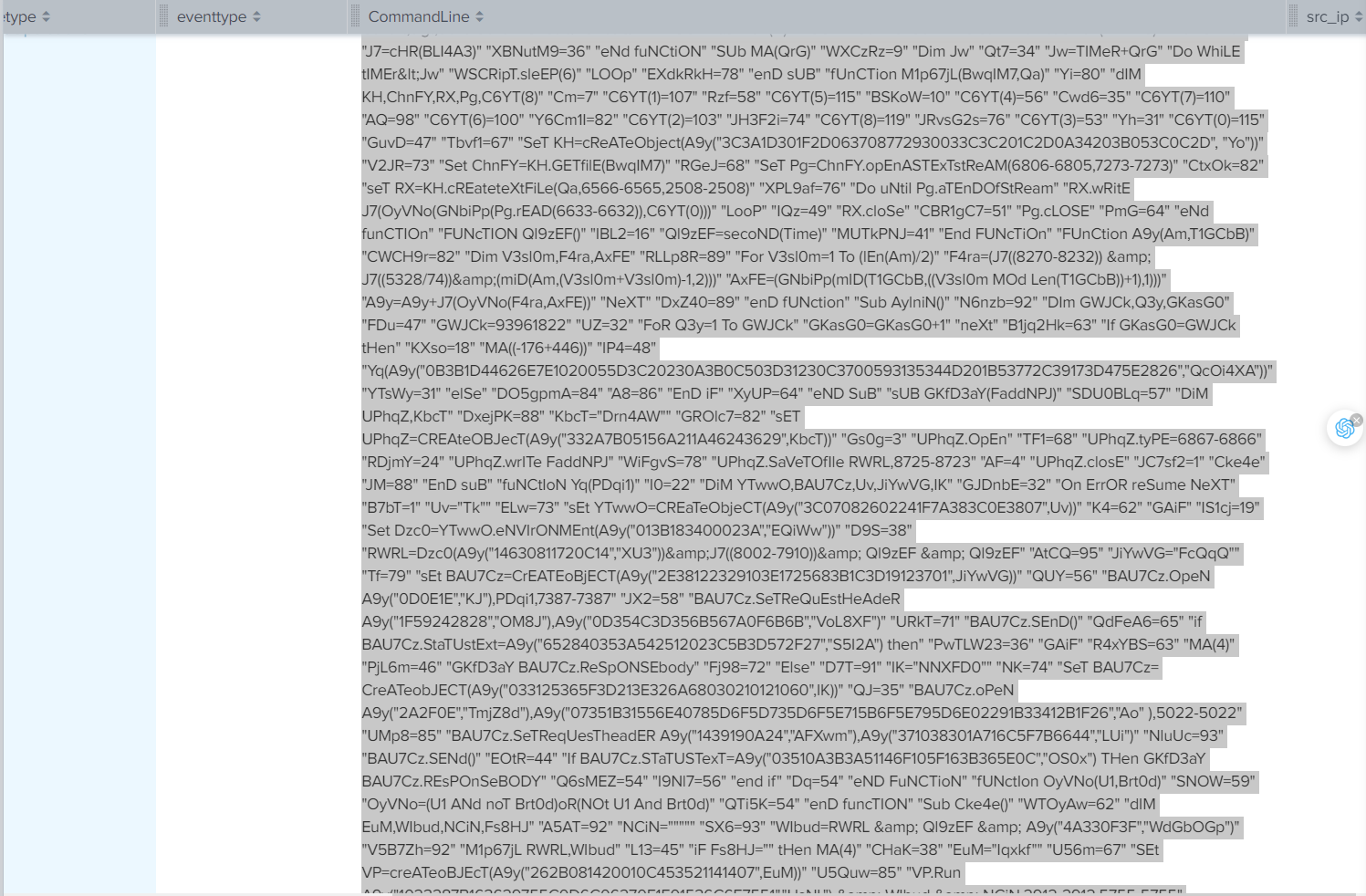
4490

C2

Đầu tiên tra code .vbs theo host vào ngày 24/8/2016 để xem file là file gì



Và kéo xuống thấy một dòng command line rất là dài



Count ra được thì nó là 4490

6. Tên của USB được Bob Smith cắm vào là gì?

Query :

Tìm hiểu trên trang <https://learn.microsoft.com/en-us/windows-hardware/drivers/usbcon/usb-device-specific-registry-settings>

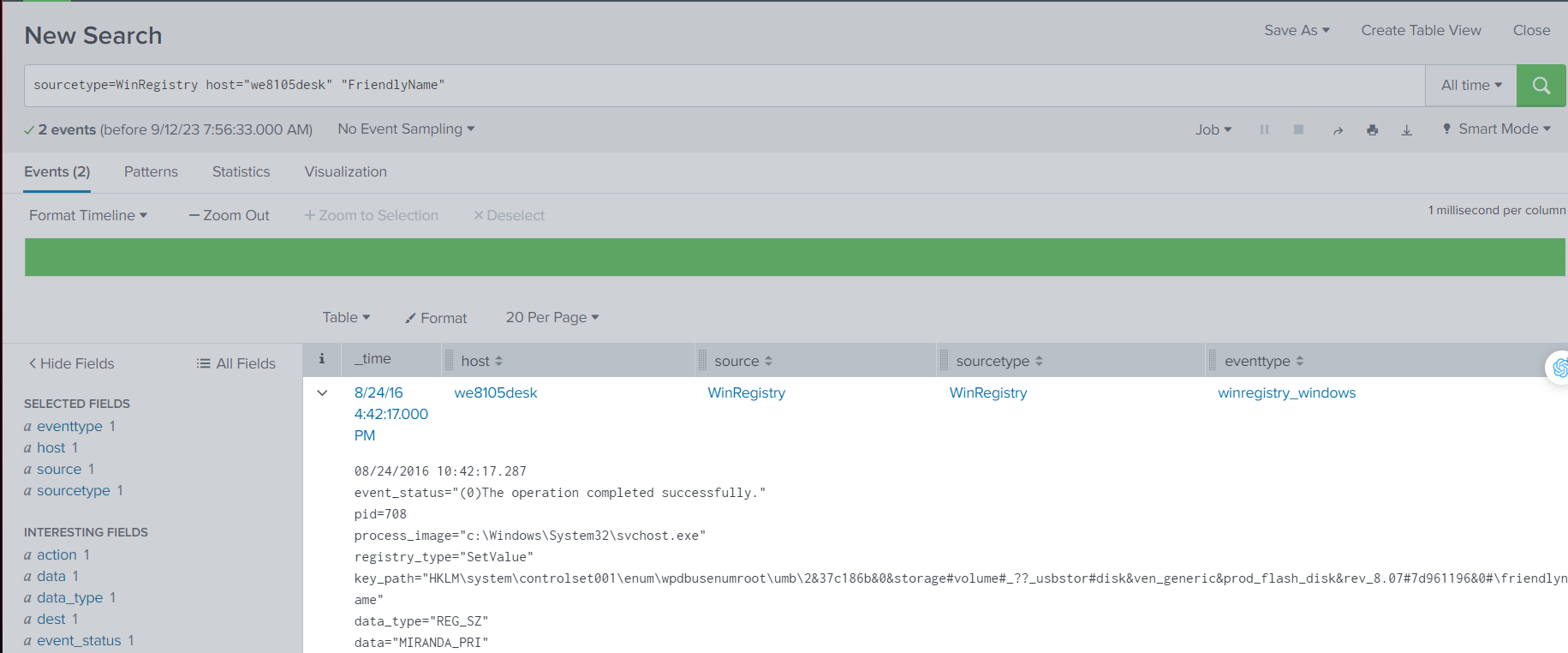
Tìm được registry của nó

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

Key name của nó tên là “Friendly Name”

Search theo key name ta có được

sourcetype=WinRegistry host=”we8105desk” “FriendlyName”

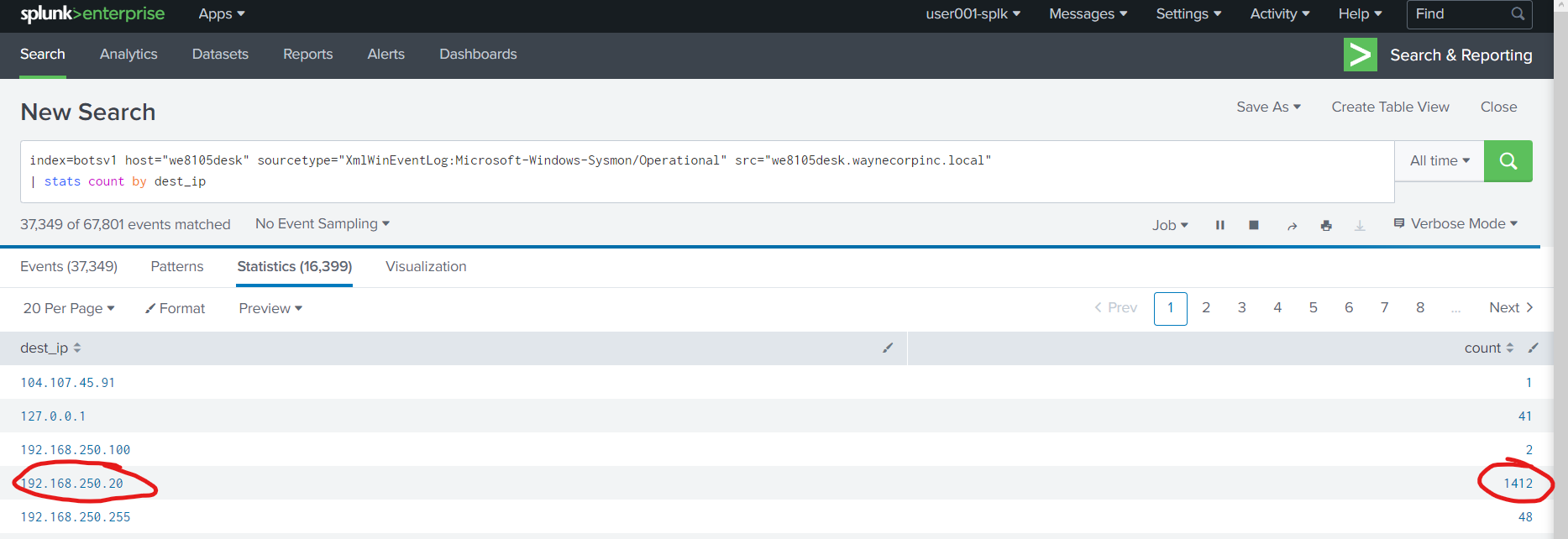


**MIRANDA\_PRI**.

7. Bob Smith's workstation (we8105desk) đã được kết nối đến 1 máy chủ fileserver trong lúc bùng phát ransomware. Địa chỉ IPv4 của máy chủ fileserver trên là gì?

Query:

index=botsv1 host="we8105desk" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" src="we8105desk.waynecorpinc.local"

| stats count by dest\_ip 

**192.168.250.20**.

8. Có bao nhiêu tệp PDF riêng biệt mà ransomware đã mã hóa trên máy chủ fileserver?

Query

index=botsv1 sourcetype="\*win\*" pdf dest="we9041srv.waynecorpinc.local" Source\_Address="192.168.250.100"

| stats dc(Relative\_Target\_Name)



257

C2:

Count sourcetype ra tất cả các file pdf

index=botsv1 \*.pdf  
| stats count by sourcetype  
| sort -count



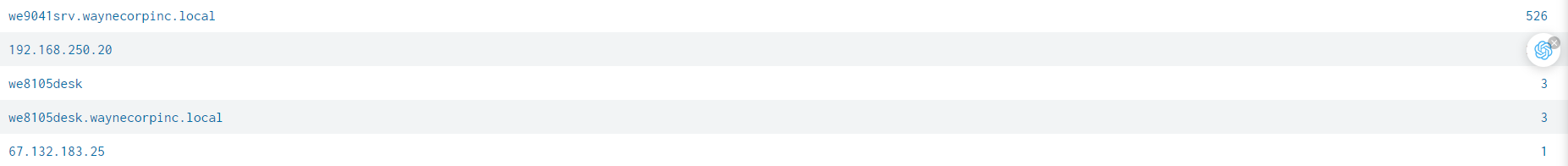
Hầu hết các tài nguyên pdf đều có trong wineventlog.

* Chúng ta sẽ tra được cái dest của pdf

index=botsv1 \*.pdf sourcetype=wineventlog

| stats count by dest

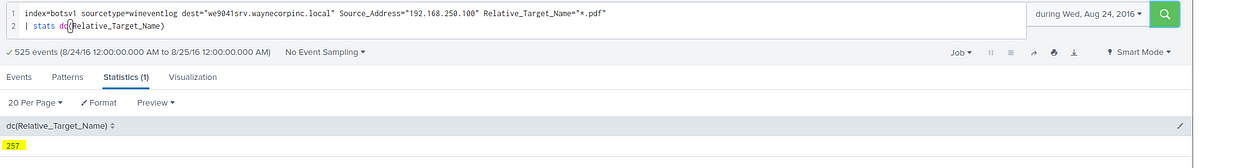
| sort -count



=>

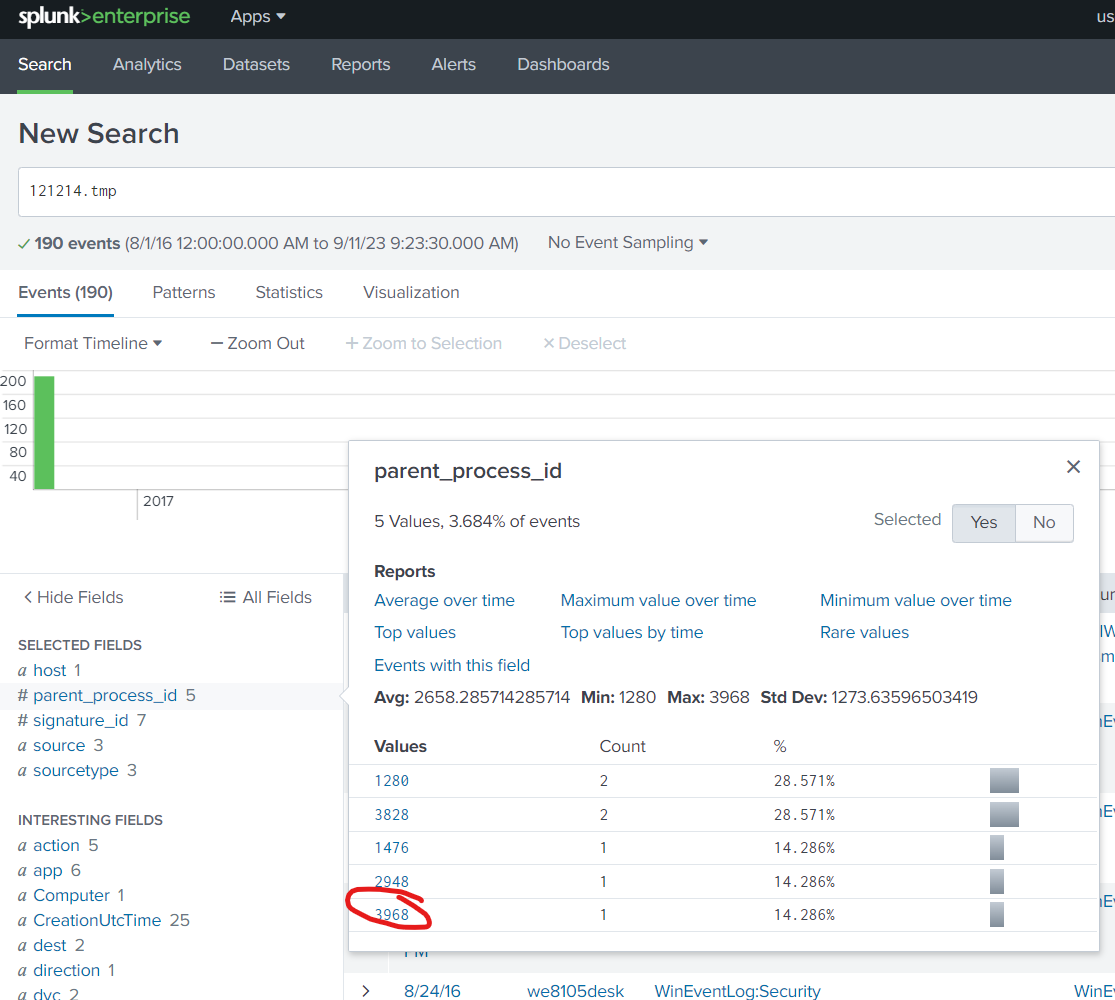
Dc của nó tìm được sẽ là

index=botsv1 sourcetype=wineventlog dest=”we9041srv.waynecorpinc.local” Source\_Address=”192.168.250.100" Relative\_Target\_Name=”\*.pdf”  
| stats dc(Relative\_Target\_Name)



257

9. Tệp VBscript được tìm thấy trong câu hỏi sô 5 thực hiện chạy file "121214.tmp", hãy cho biết ParentProcessID của lần đầu tiên khởi chạy file trên?

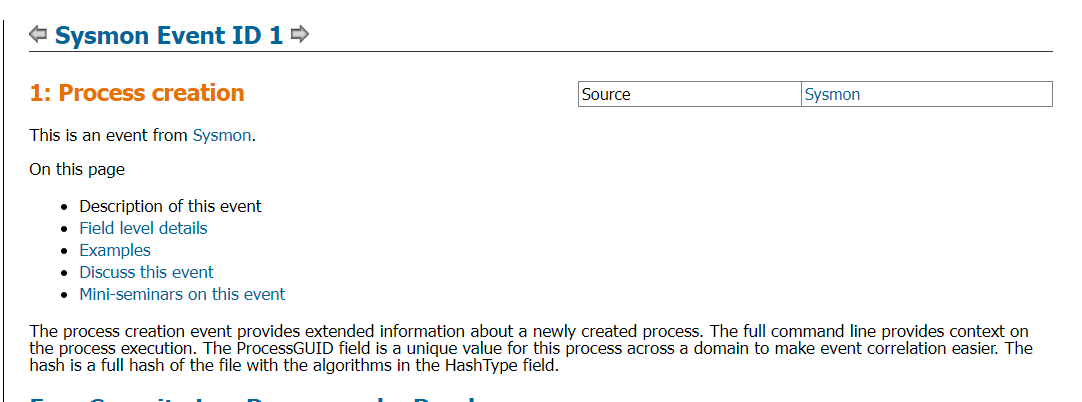


3968

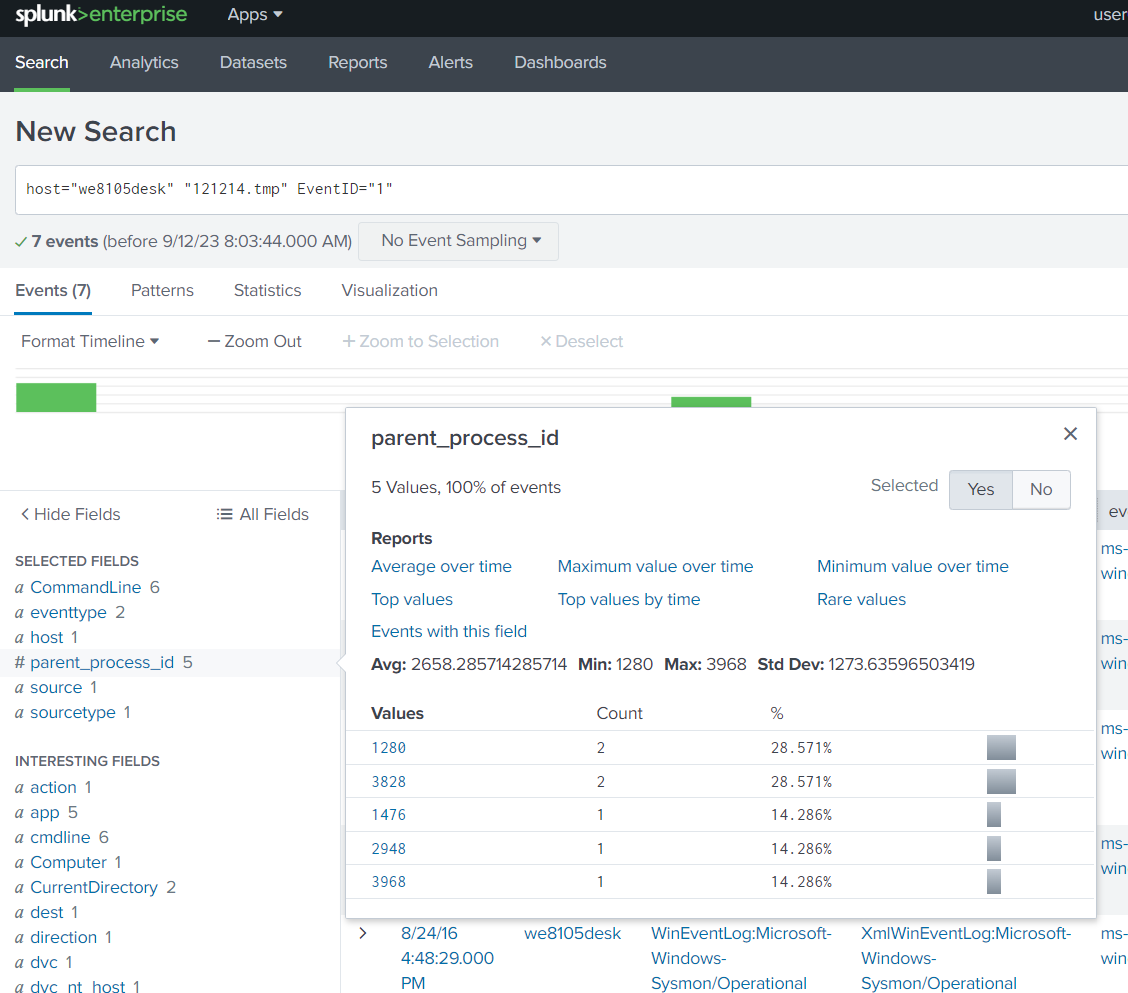
C2:

Vì nó là file đầu tiên được khởi chạy nên Sysmon event id = 1 nơi mà tệp tin 121214.tmp được nhắc tới ở trên

host="we8105desk" "121214.tmp" EventID="1"

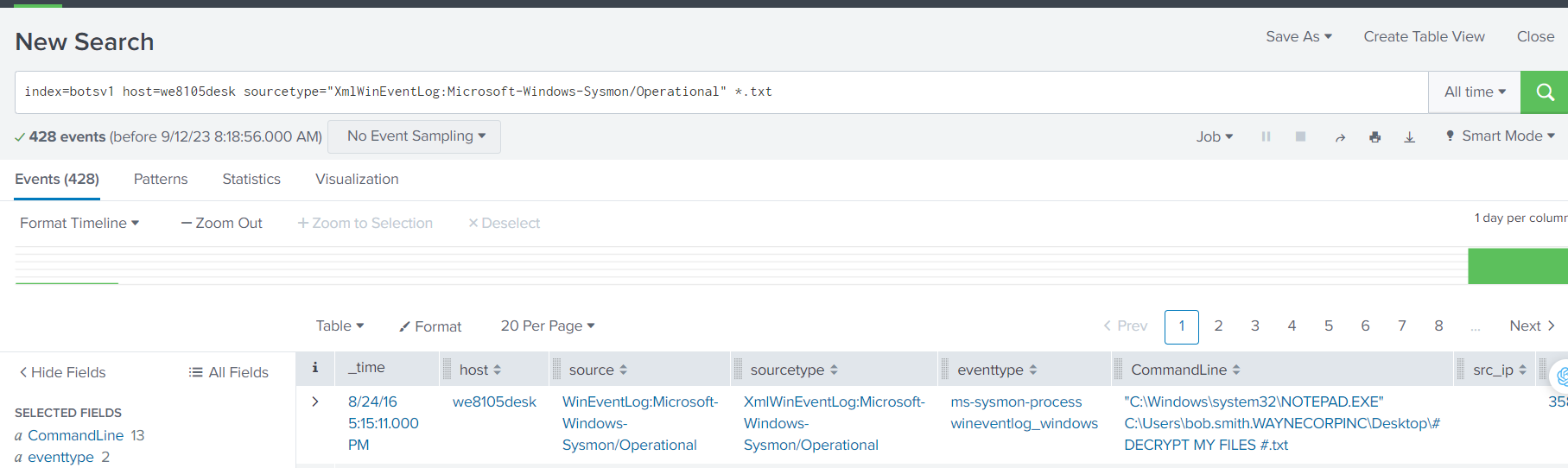


Tra ra được ppid của nó sẽ là 3968

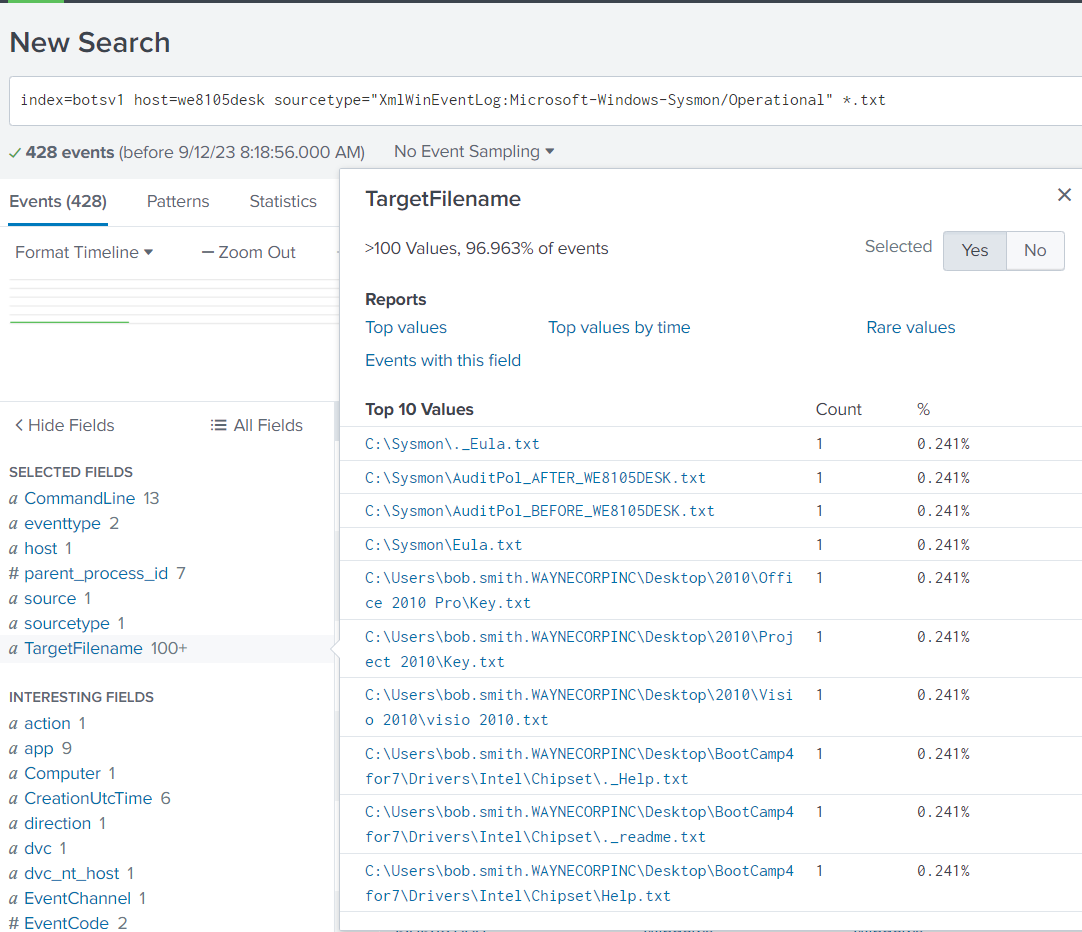


10. Các file mà mã độc Cerber mã hóa nằm trong máy của Bob Smith's. Có bao nhiêu tệp file .txt bị mã hóa?

Như chúng ta đã tra cứu ở trên thì chúng ta đã biết được loại sourcetype của nó là XmlWinEventLog:Microsoft-Windows-Sysmon/Operational host => chúng ta sẽ tìm txt bằng lệnh \*txt tìm tất cả txt



Vì chúng ta cần tìm các file txt bị mã hóa nên tìm tới field targetfilename



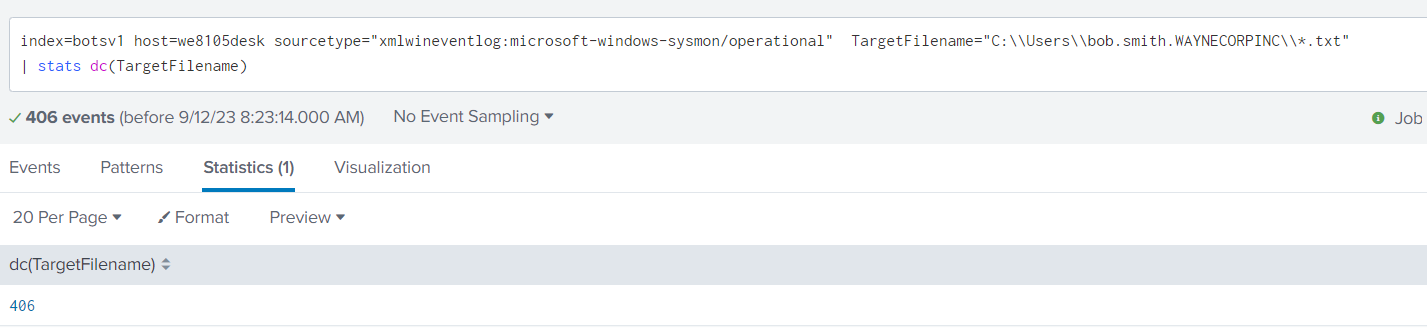
ở đây chúng ta cần tập trung vào các file của bob smith nên file sẽ là

[C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Project 2010\Key.txt](https://gettingstarted.splunk.show/en-US/app/search/search?q=search%20index%3Dbotsv1%20host%3Dwe8105desk%20sourcetype%3D%22XmlWinEventLog%3AMicrosoft-Windows-Sysmon%2FOperational%22%20*.txt&display.page.search.mode=smart&dispatch.sample_ratio=1&earliest=0&latest=&display.general.type=events&display.page.search.tab=events&display.general.enablePreview=1&display.statistics.wrap=0&display.events.fields=%5B%22host%22%2C%22source%22%2C%22sourcetype%22%2C%22eventtype%22%2C%22CommandLine%22%2C%22src_ip%22%2C%22parent_process_id%22%2C%22TargetFilename%22%5D&display.prefs.fieldFilter=targe&sid=1694506736.990)

[C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Office 2010 Pro\Key.txt](https://gettingstarted.splunk.show/en-US/app/search/search?q=search%20index%3Dbotsv1%20host%3Dwe8105desk%20sourcetype%3D%22XmlWinEventLog%3AMicrosoft-Windows-Sysmon%2FOperational%22%20*.txt&display.page.search.mode=smart&dispatch.sample_ratio=1&earliest=0&latest=&display.general.type=events&display.page.search.tab=events&display.general.enablePreview=1&display.statistics.wrap=0&display.events.fields=%5B%22host%22%2C%22source%22%2C%22sourcetype%22%2C%22eventtype%22%2C%22CommandLine%22%2C%22src_ip%22%2C%22parent_process_id%22%2C%22TargetFilename%22%5D&display.prefs.fieldFilter=targe&sid=1694506736.990)

[C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Visio 2010\visio 2010.txt](https://gettingstarted.splunk.show/en-US/app/search/search?q=search%20index%3Dbotsv1%20host%3Dwe8105desk%20sourcetype%3D%22XmlWinEventLog%3AMicrosoft-Windows-Sysmon%2FOperational%22%20*.txt&display.page.search.mode=smart&dispatch.sample_ratio=1&earliest=0&latest=&display.general.type=events&display.page.search.tab=events&display.general.enablePreview=1&display.statistics.wrap=0&display.events.fields=%5B%22host%22%2C%22source%22%2C%22sourcetype%22%2C%22eventtype%22%2C%22CommandLine%22%2C%22src_ip%22%2C%22parent_process_id%22%2C%22TargetFilename%22%5D&display.prefs.fieldFilter=targe&sid=1694506736.990)

* Tổng các tệp .txt bị mã hóa sẽ là

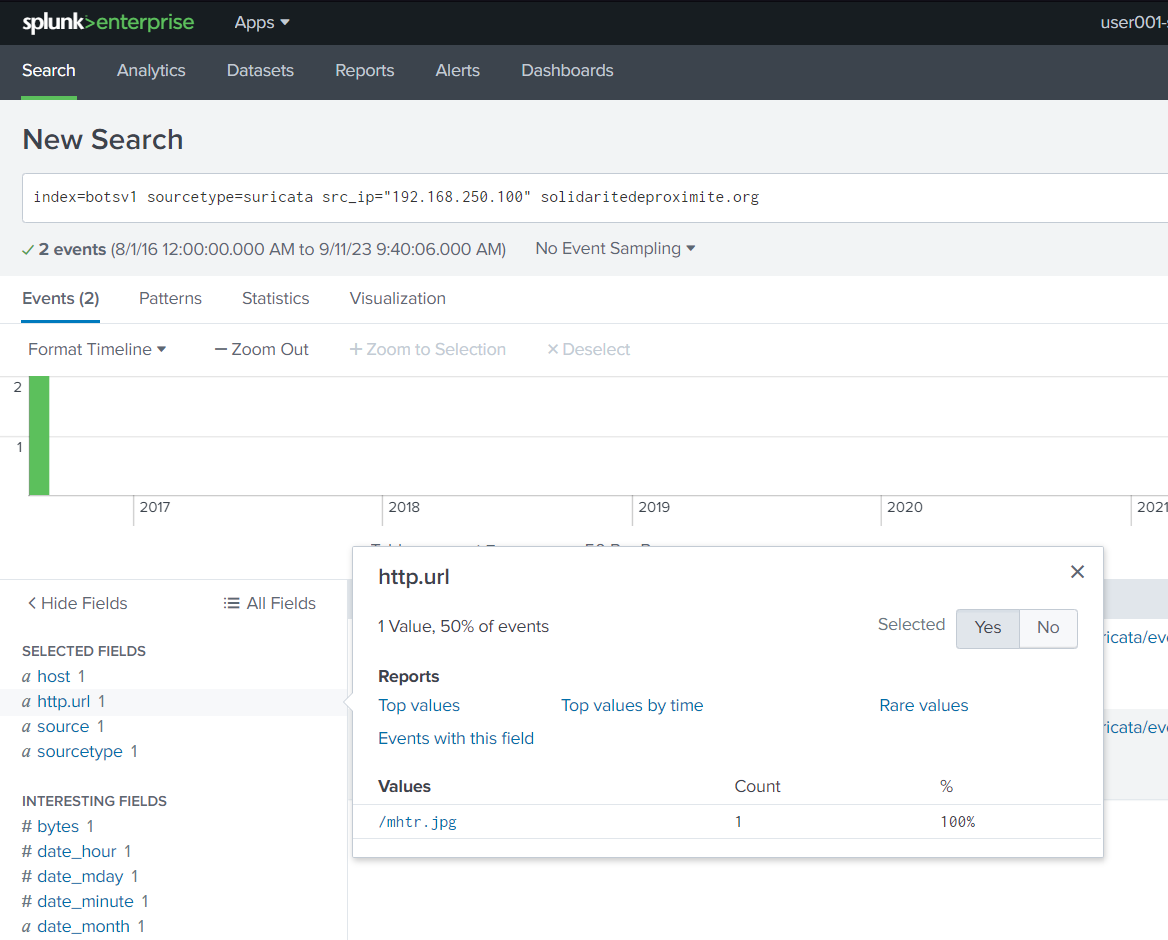


406

11. Mã độc đã tải xuống tệp file có chứa cryptorcode của mã độc Cerber. File được tải xuống có tên là gì?

Query :

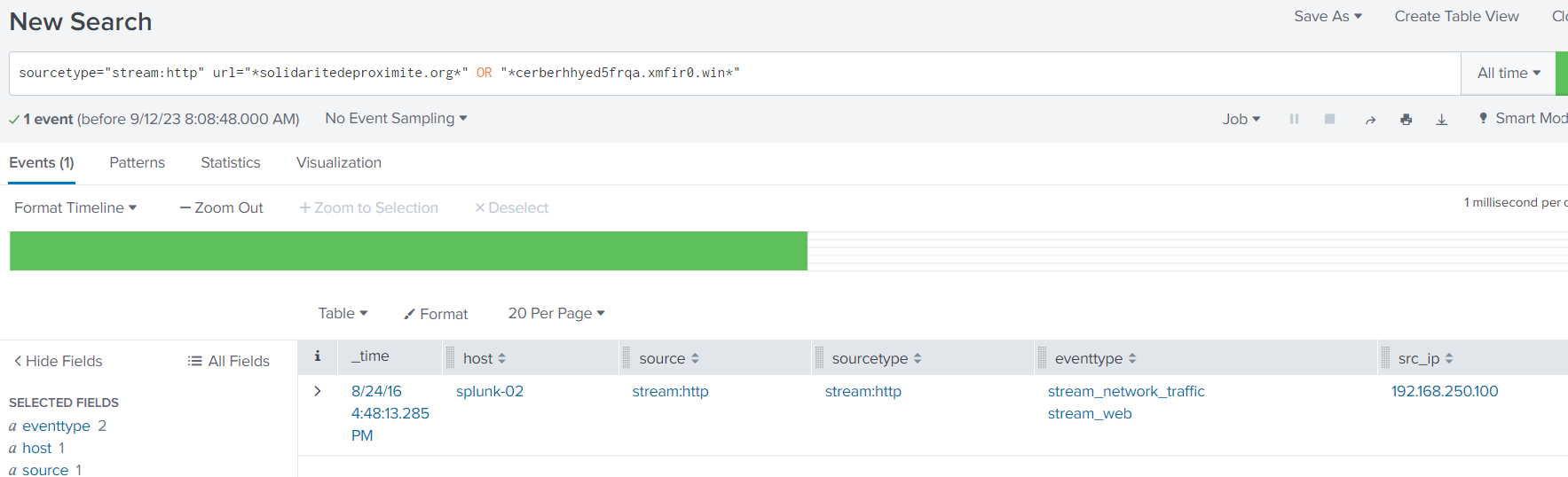
index=botsv1 sourcetype=suricata src\_ip="192.168.250.100" solidaritedeproximite.org



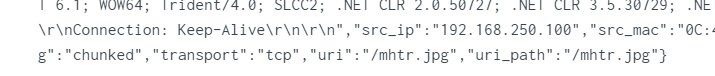
C2 : vì đã biết 2 domain ở trên là solidaritedeproximite.org và cerberhhyed5frqa.xmfir0.win nên chúng ta tìm thử http stream của nó là gì

sourcetype="stream:http" url="\*solidaritedeproximite.org\*" OR "\*cerberhhyed5frqa.xmfir0.win\*"

tìm ra được 1 event name

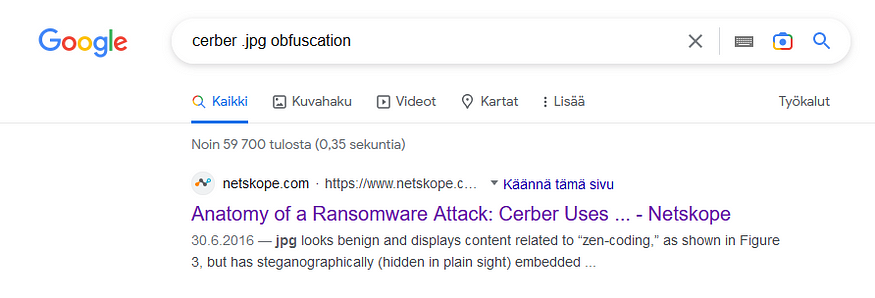


Xem chi tiết của nó là file mhtr.jpg

 mhtr.jpg

12. Sau khi đã phân tích về hành vi mã hóa của mã độc Cerber, hãy cho biết kĩ thuật giấu tin ("obfuscation") được sử dụng ở đây là gì?

Tra trên mạng thì nó hiển thị ra kết quả





**Steganography**