**Boss of The Soc v1**

**Overview**

**Write-ups**

|  |  |
| --- | --- |
|  | #1. This is a simple question to get you familiar with submitting answers. What is the name of the company that makes the software that you are using for this competition? Just a six-letter word with no punctuation. |

**SPLUNK**

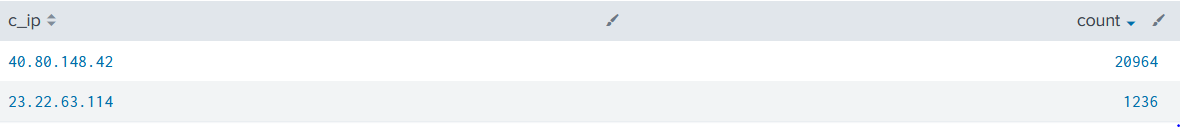
#2. What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?

Khi scan thì địa chỉ máy scan sẽ gửi một lượng lớn bất thường các request tới server. Tìm kiếm số lượng request theo ip.

sourcetype="stream:http" "imreallynotbatman.com"

| stats count by c\_ip





Xác định được địa chỉ scan là **40.80.148.42**

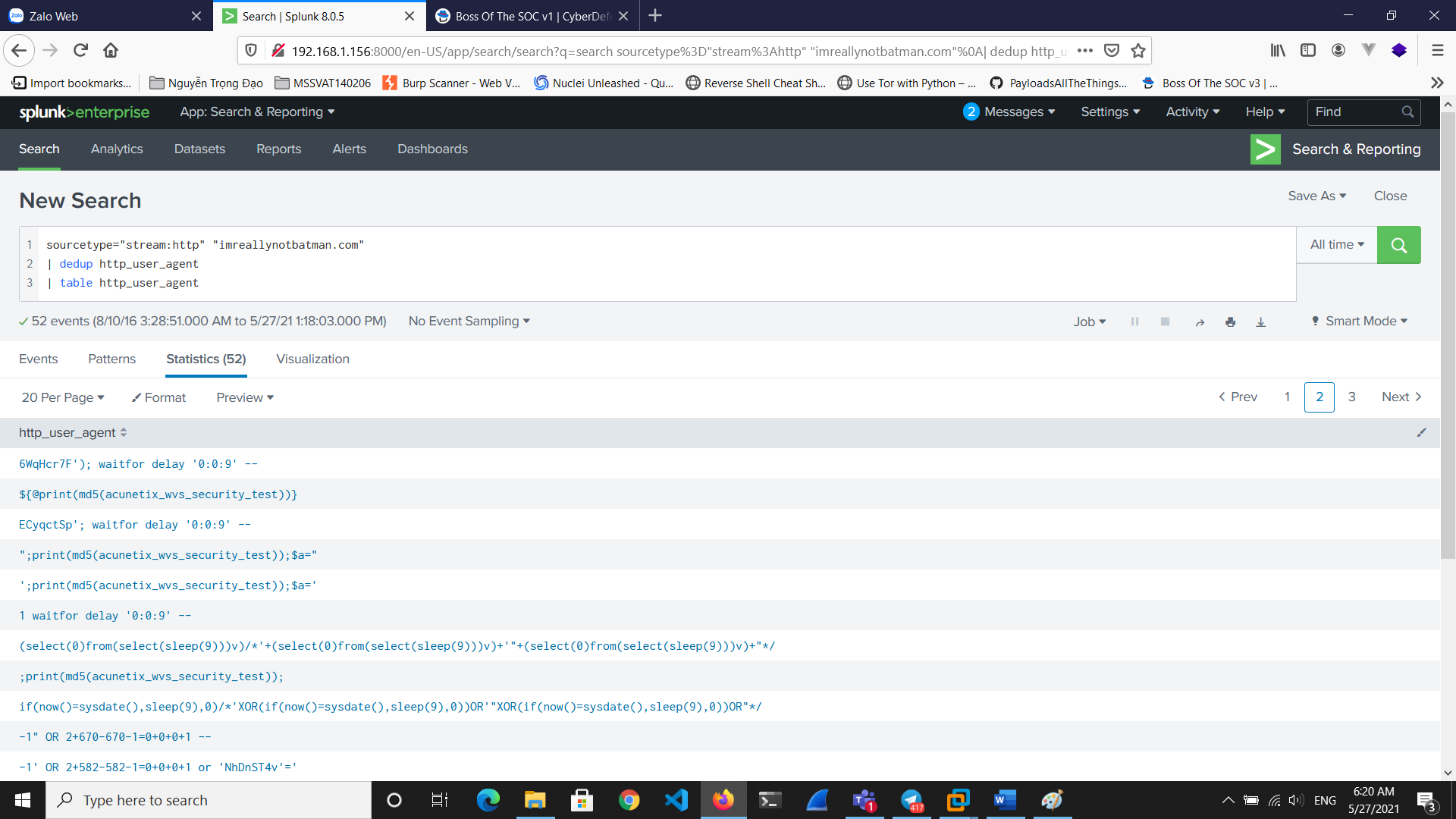
#3. What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example "Microsoft" or "Oracle").

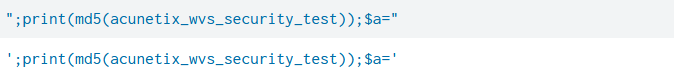
Theo kinh nghiệm, khi dùng các công cụ scan, trong trường User-Agent của một số gói tin sẽ có tên của công cụ đó.

sourcetype="stream:http" "imreallynotbatman.com"

| dedup http\_user\_agent

| table http\_user\_agent

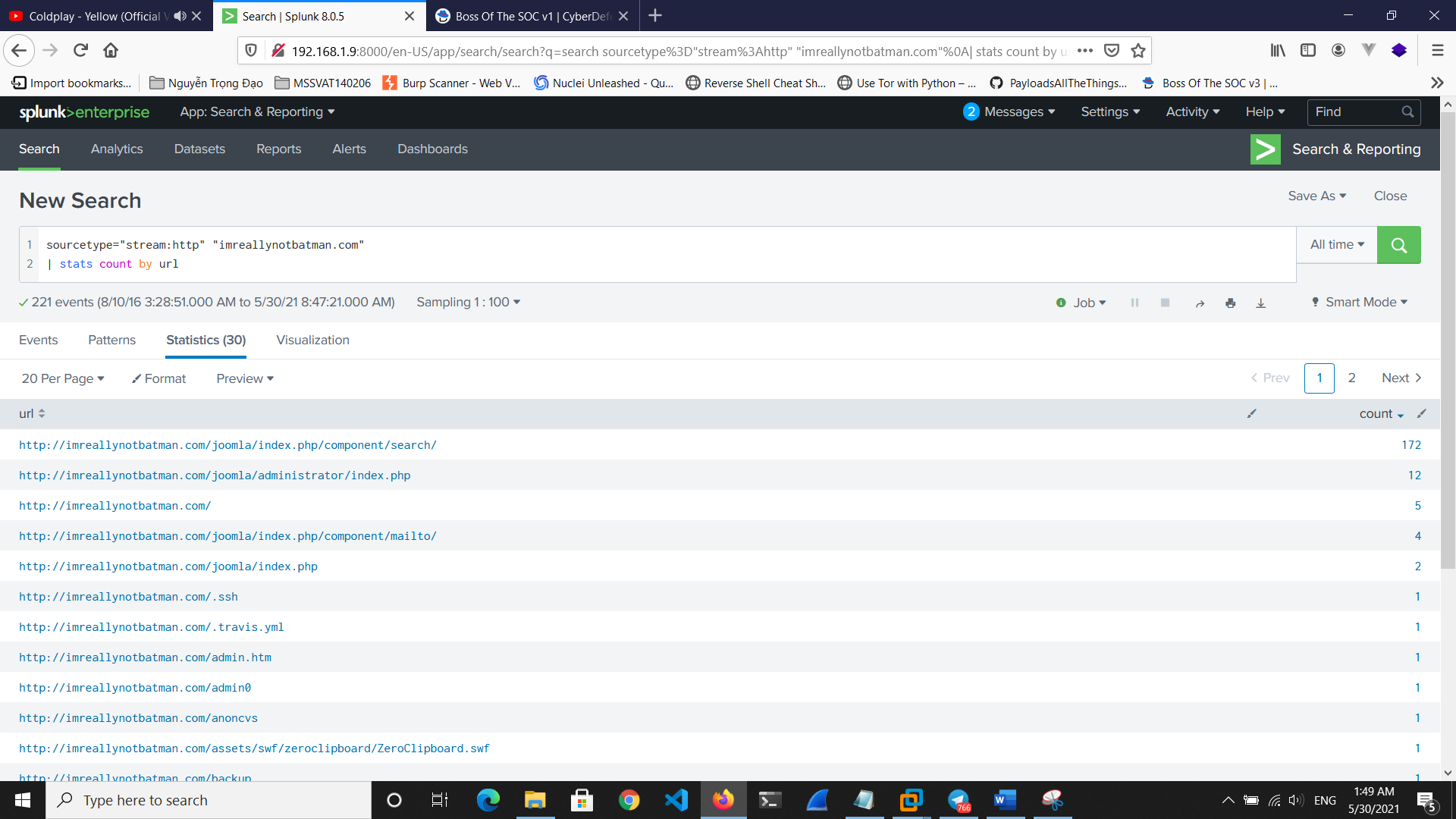


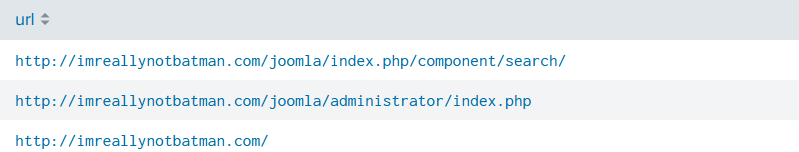


Xác định được attacker sử dụng **Acunetix** thực hiện scan.

#4. What content management system is imreallynotbatman.com likely using?(Please do not include punctuation such as . , ! ? in your answer. We are looking for alpha characters only.)

Xem một số url mà attacker truy cập đến:





Xác định được CMS được sử dụng là **joomla**.

#5. What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with extension (For example "notepad.exe" or "favicon.ico").

Trong kịch bản có nhắc đến cộng động người dùng report là trang bị deface khi họ vào website của Wayne Enterprises nhưng hoàn toàn không có log.

#6. This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

#7. What IP address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

#8. Based on the data gathered from this attack and common open source intelligence sources for domain names, what is the email address that is most likely associated with Po1s0n1vy APT group?

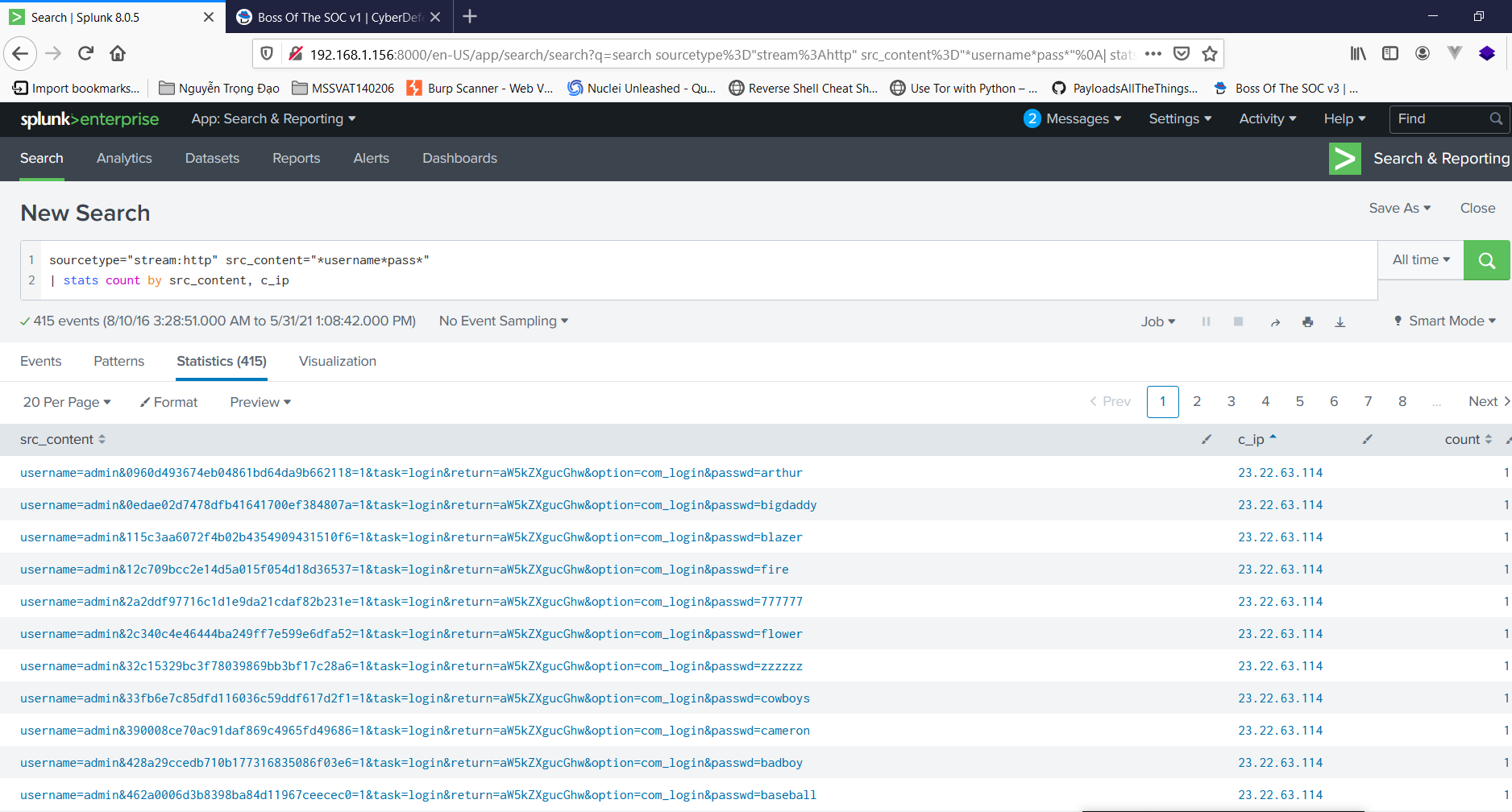
#9. What IP address is likely attempting a brute force password attack against imreallynotbatman.com?

Brute force login thì trường src\_content sẽ chứa các kí tự username, pass…

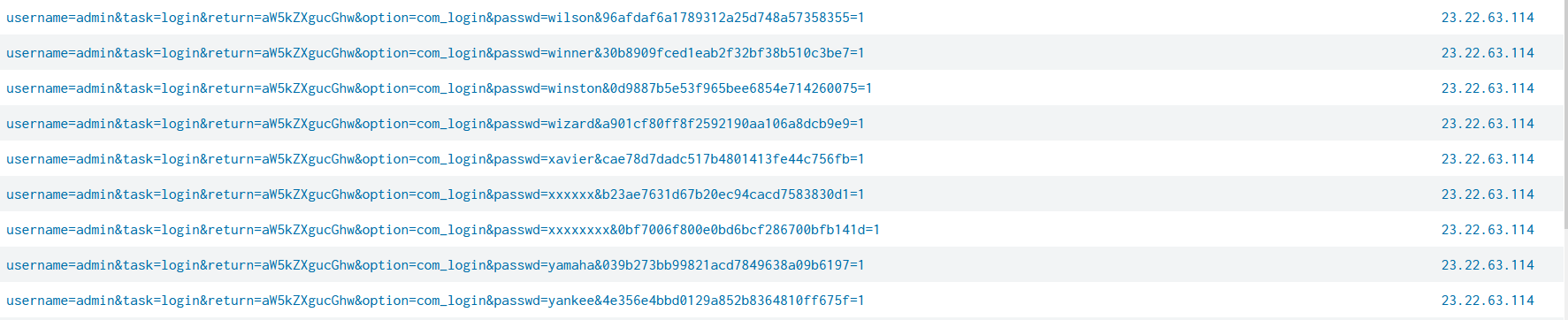
Tìm kiếm những event có src\_content có định dạng đó.

sourcetype="stream:http" src\_content="\*username\*pass\*"

| stats count by src\_content, c\_ip



Thấy rõ ip 23.22.63.114 gửi một loạt các password.



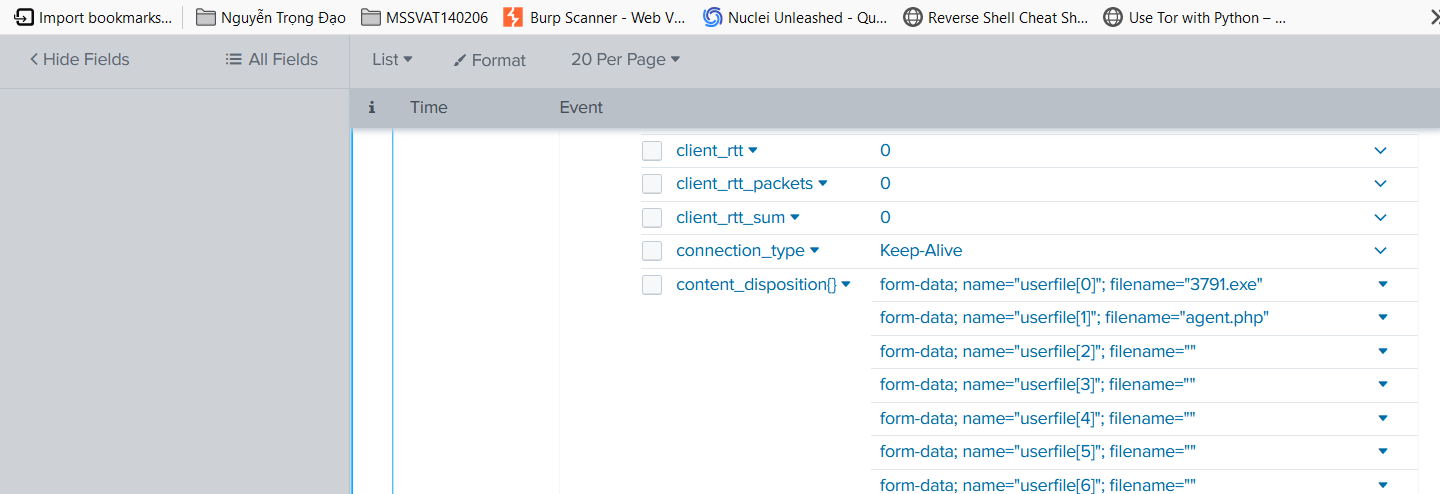
Phát hiện thêm ip 40.80.148.42 cũng gửi gói tin với user=admin và password=batman.

#10. What is the name of the executable uploaded by Po1s0n1vy? Please include file extension. (For example, "notepad.exe" or "favicon.ico")

Gói tin upload file sẽ có các đặc tính như: HTTP\_method=POST, trong trường content-type= multipart/form-data

sourcetype="stream:http" http\_method=POST cs\_content\_type="\*multipart/form-data\*"

Phát hiện ip 40.80.148.42 có upload file **3791.exe** (có thể file này là nguyên nhân dẫn tới deface)

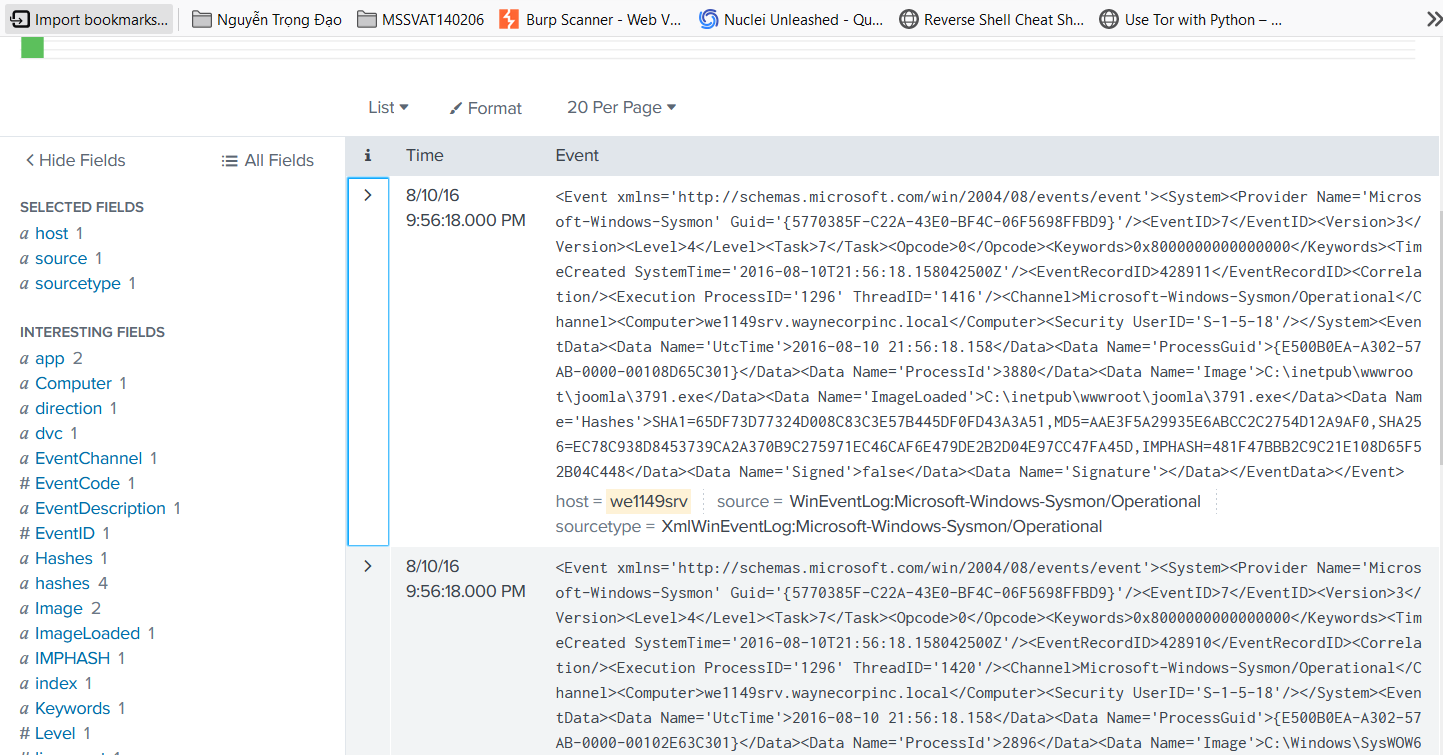


#11. What is the MD5 hash of the executable uploaded?

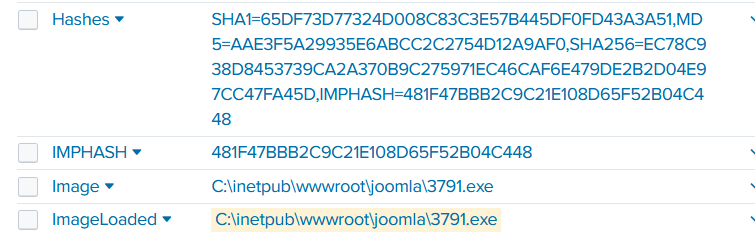
Có được thông tin host=we1149srv là máy chủ web server ip [192.168.250.70](http://192.168.1.156:8000/en-US/app/search/search?q=search%20sourcetype%3D%22stream%3Ahttp%22&sid=1622518708.623&display.page.search.mode=smart&dispatch.sample_ratio=100&workload_pool=&earliest=0&latest=now)

Tìm kiếm tiến trình event liên quan tới 3791.exe

host="we1149srv" "3791.exe" ImageLoaded="C:\\inetpub\\wwwroot\\joomla\\3791.exe"



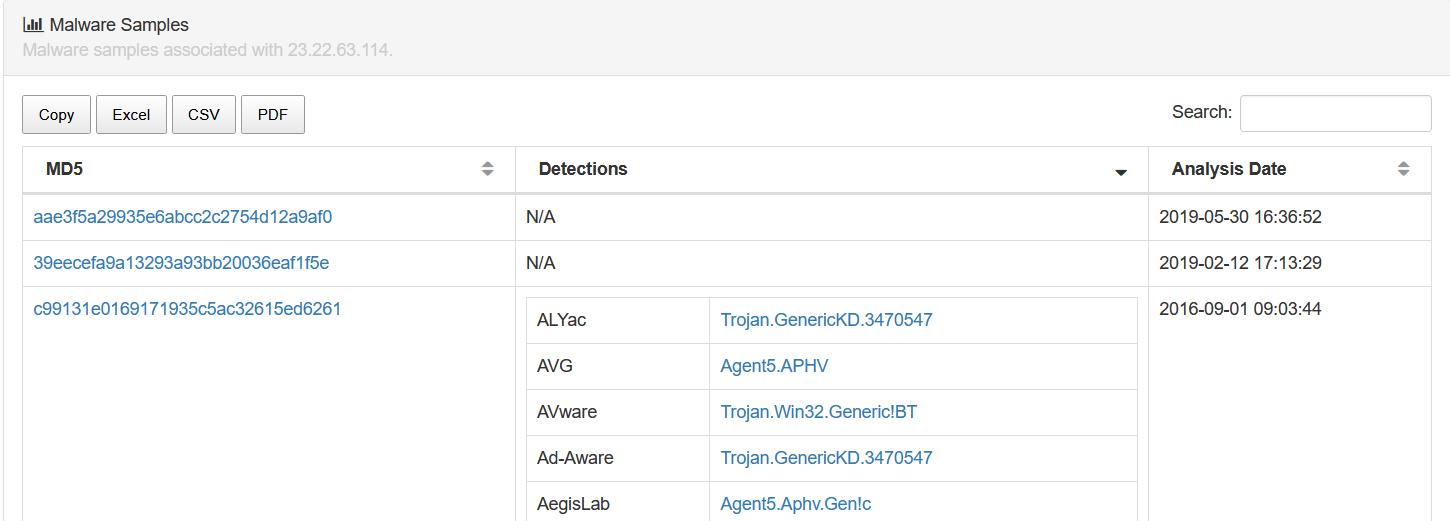
Thông tin về mã băm MD5 **AAE3F5A29935E6ABCC2C2754D12A9AF0**



#12. GCPD reported that common TTPs (Tactics, Techniques, Procedures) for the Po1s0n1vy APT group, if initial compromise fails, is to send a spear phishing email with custom malware attached to their intended target. This malware is usually connected to Po1s0n1vys initial attack infrastructure. Using research techniques, provide the SHA256 hash of this malware.

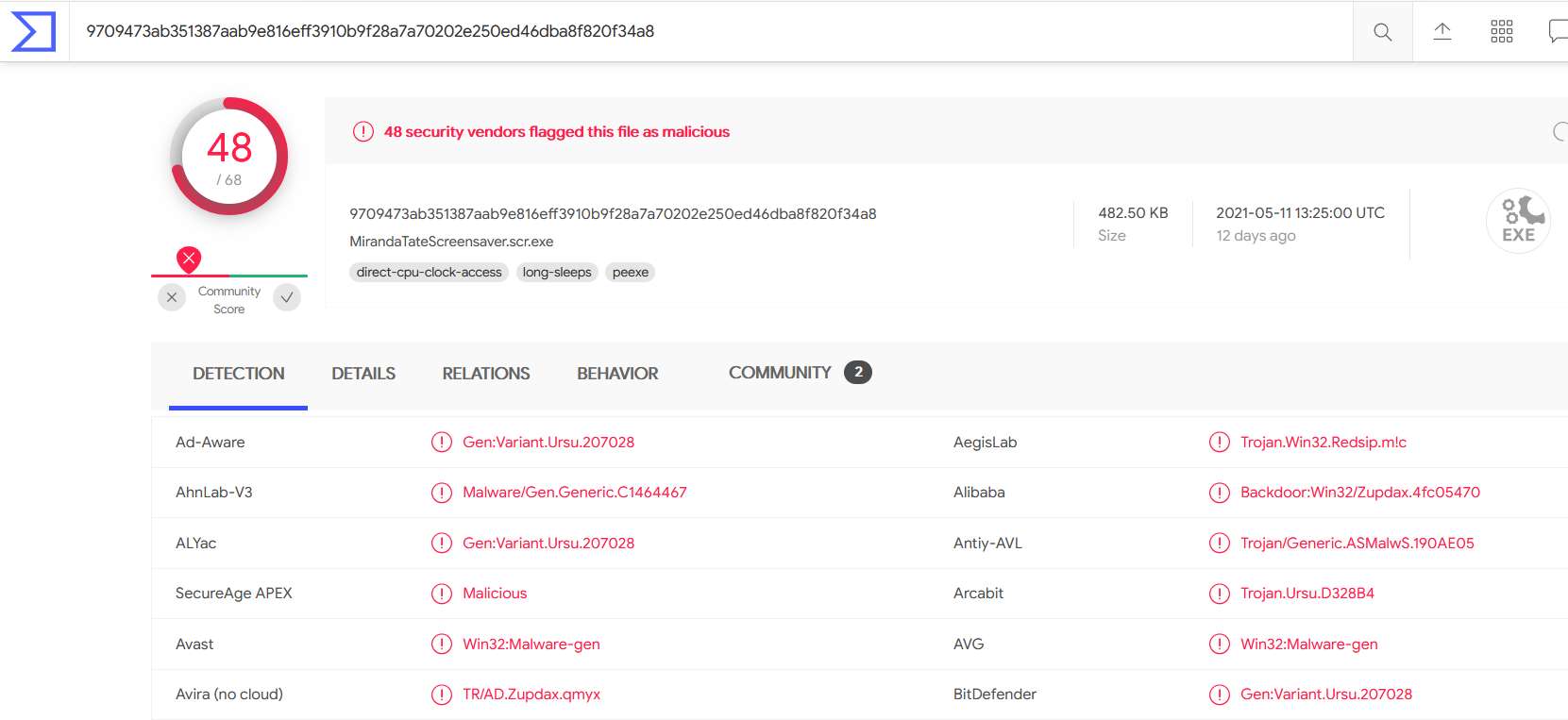
Xác định được 2 ip của kẻ tấn công. Search ip với từ khóa “malware”. Thử tìm kiếm với key: “23.22.63.114” “malware”, tìm thấy thông tin tại : <https://www.threatminer.org/host.php?q=23.22.63.114#gsc.tab=0&gsc.q=23.22.63.114&gsc.page=1>

Kéo đến dưới cùng sẽ thấy Malware Samples, cùng mã hash md5



Kiểm tra trên <https://www.virustotal.com> đoạn hash [c99131e0169171935c5ac32615ed6261](https://www.threatminer.org/sample.php?q=c99131e0169171935c5ac32615ed6261)

Có 48 vendors detect là malicious



Vào tab DETAILS là ra được mã hash SHA-256.

#13. What special hex code is associated with the customized malware discussed in question 12? (Hint: It's not in Splunk).

Ở câu 12 vào tab COMMUNITY là ra hex code



#14. One of Po1s0n1vy's staged domains has some disjointed "unique" whois information. Concatenate the two codes together and submit as a single answer.

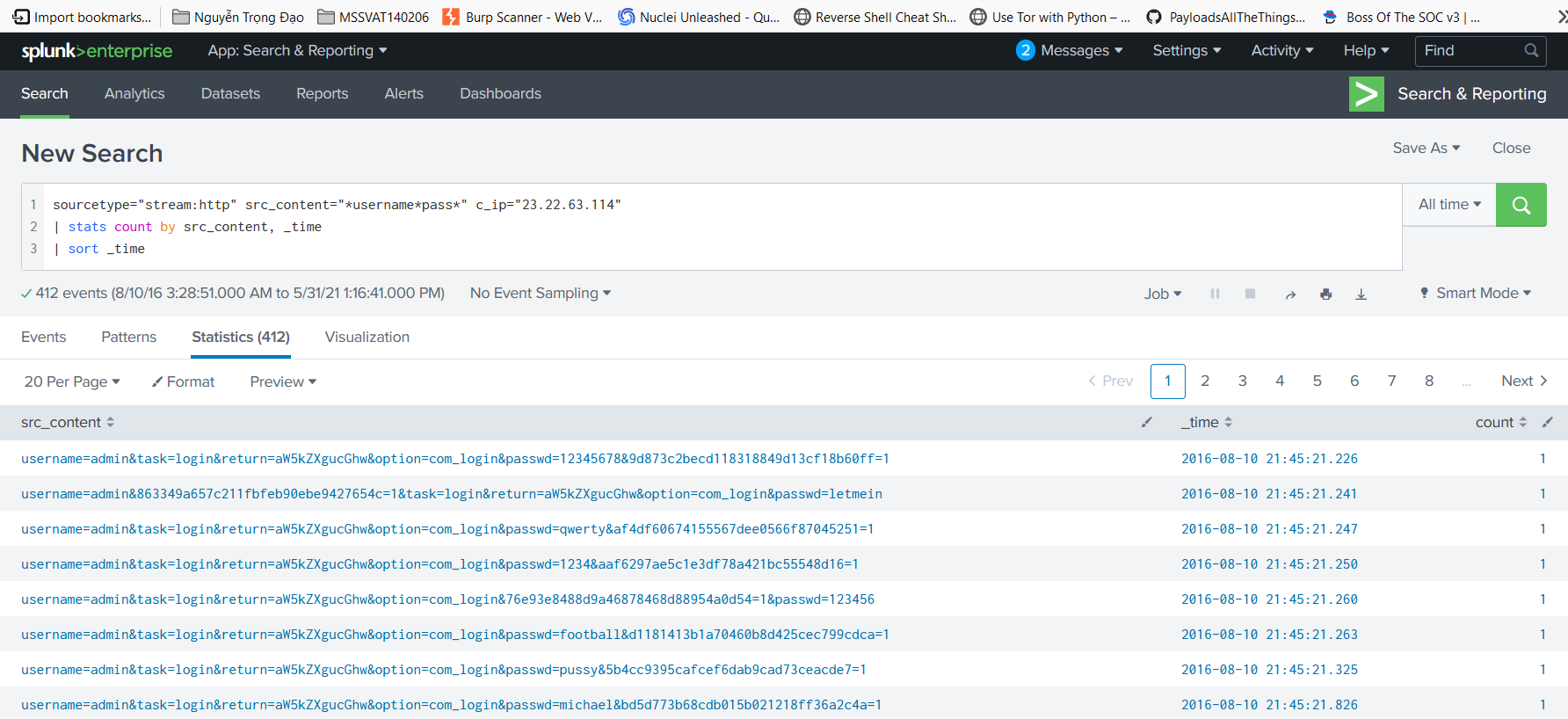
#15. What was the first brute force password used?

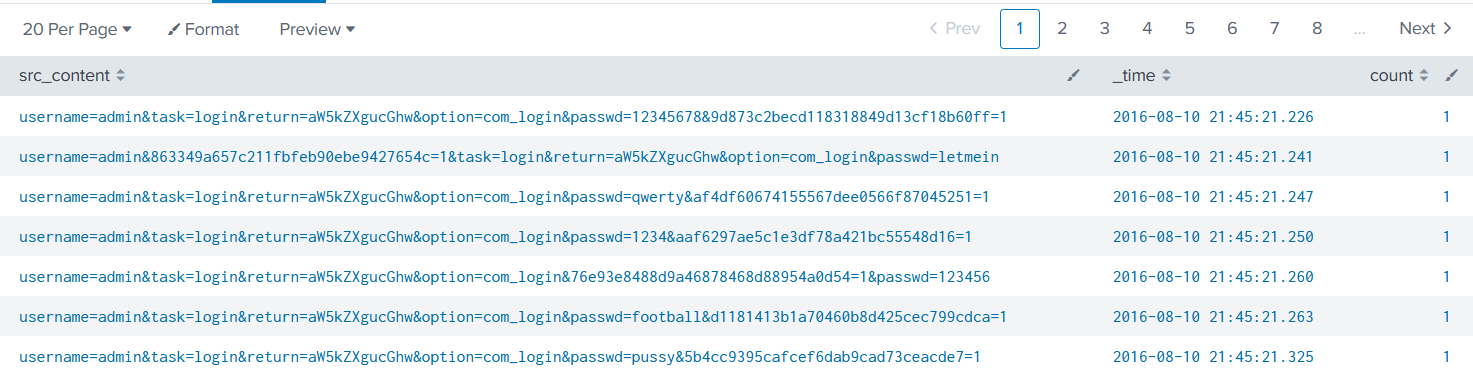
Tìm kiếm những password được gửi đi rồi sort theo \_time.

sourcetype="stream:http" src\_content="\*username\*pass\*" c\_ip="23.22.63.114"

| stats count by src\_content, \_time

| sort \_time

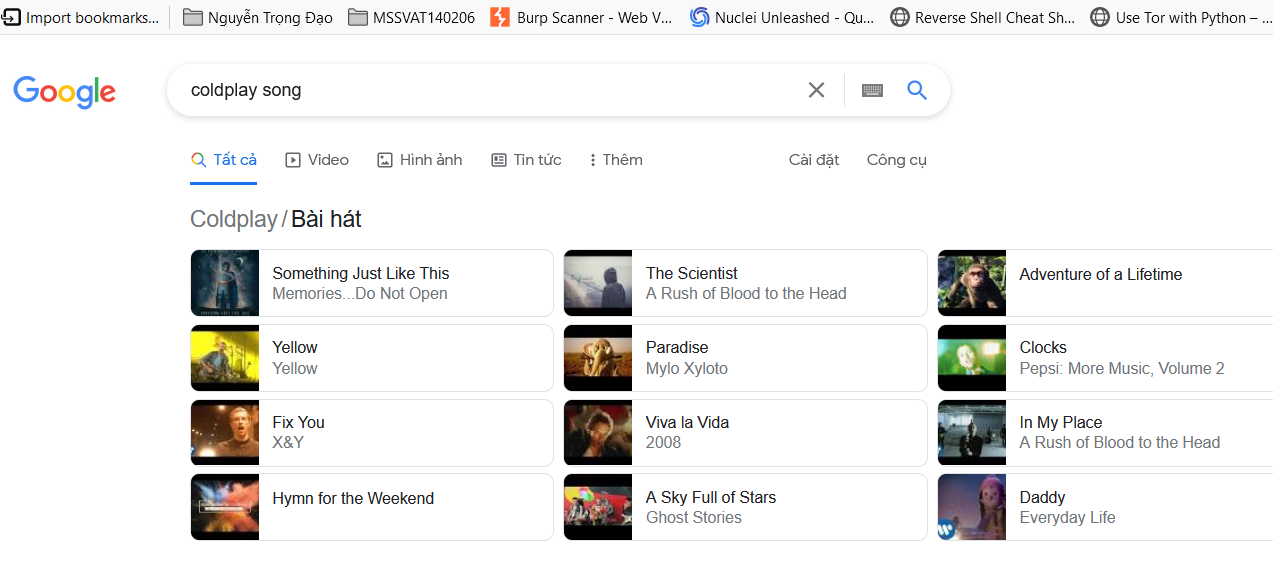




Password đầu tiên nhập là **12345678**

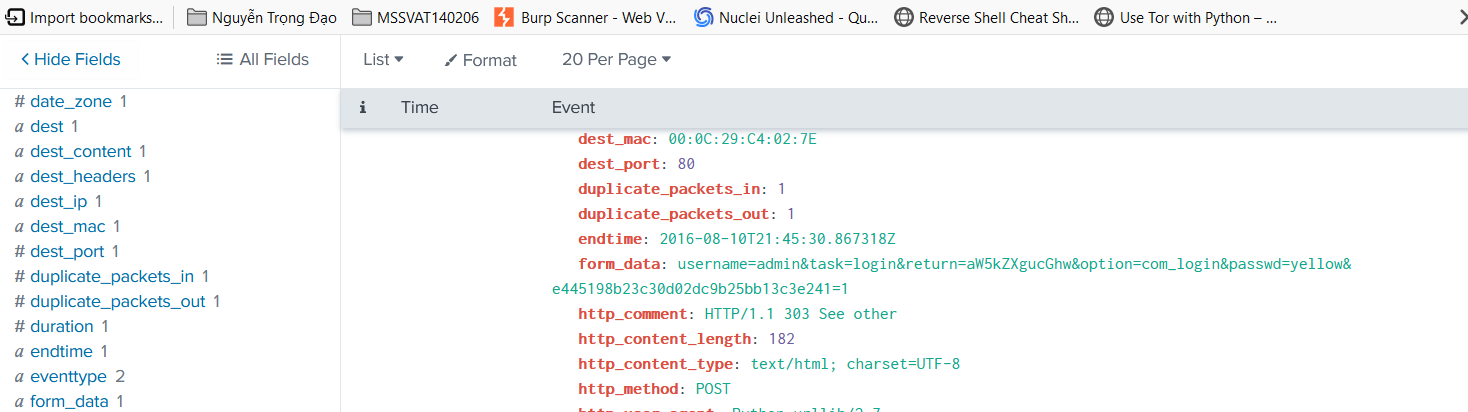
#16. One of the passwords in the brute force attack is James Brodsky's favorite Coldplay song. Hint: we are looking for a six character word on this one. Which is it?

Tìm kiếm Coldplay song trên mạng.



Được gợi ý là có 6 kí tự, khả năng là bài yellow, kiểm tra yellow có trong list password không.

sourcetype="stream:http" src\_content="\*username\*pass\*" src\_content="\*yellow\*" c\_ip="23.22.63.114"



**Yellow** có tồn tại.

#17. What was the correct password for admin access to the content management system running "imreallynotbatman.com"?

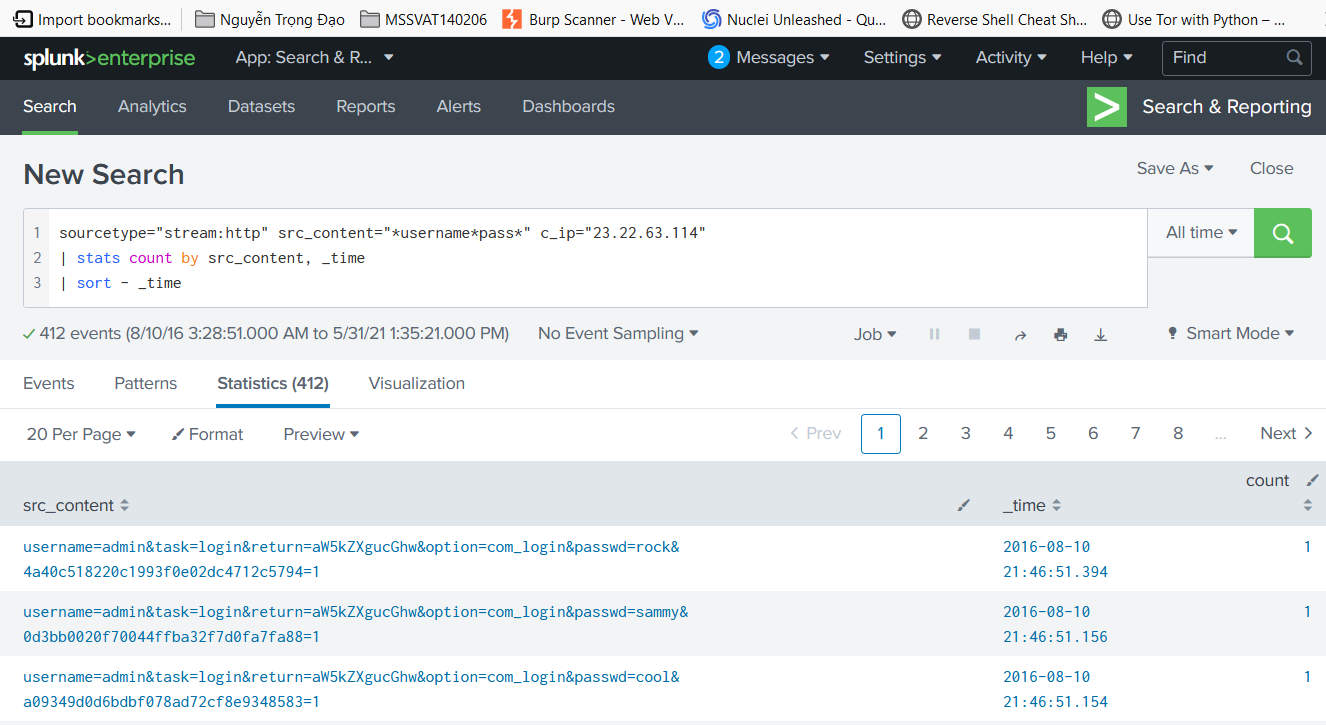
Có 2 khả năng:

Khả năng 1 là attacker sẽ brute force khi nào gặp password đúng thì dừng 🡺 password đúng là password được nhập cuối cùng.

sourcetype="stream:http" src\_content="\*username\*pass\*" c\_ip="23.22.63.114"

| stats count by src\_content, \_time

| sort - \_time



Nhưng password=rock không đúng.

Khả năng 2 là attacker brute force tất cả password có trong wordlist. Thêm nữa tại câu 9 phát hiện thêm ip 23.22.63.114, 40.80.148.42 đều submit password=batman. Chứng tỏ đây là password đúng.

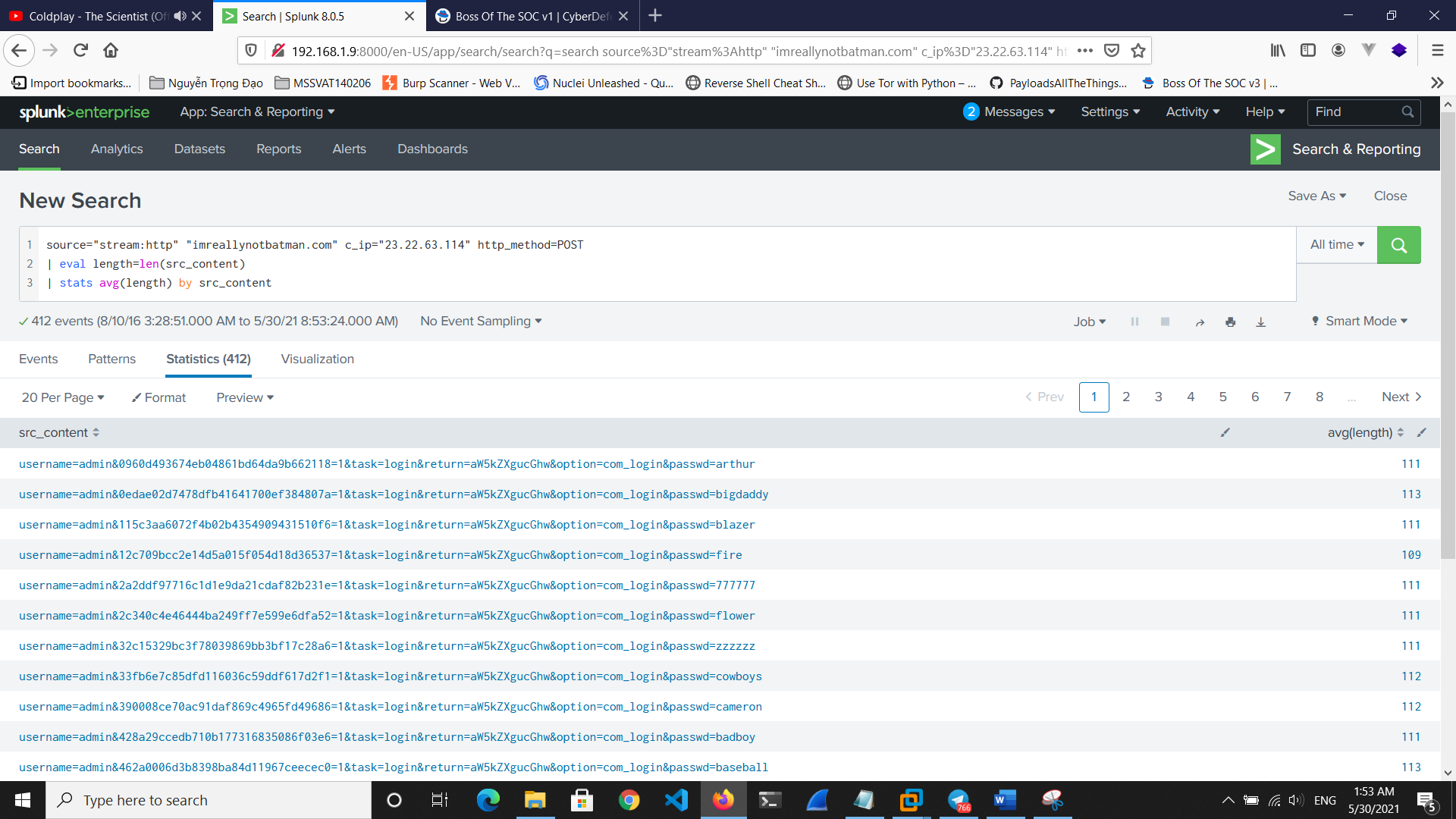
#18. What was the average password length used in the password brute forcing attempt? (Round to closest whole integer. For example "5" not "5.23213").

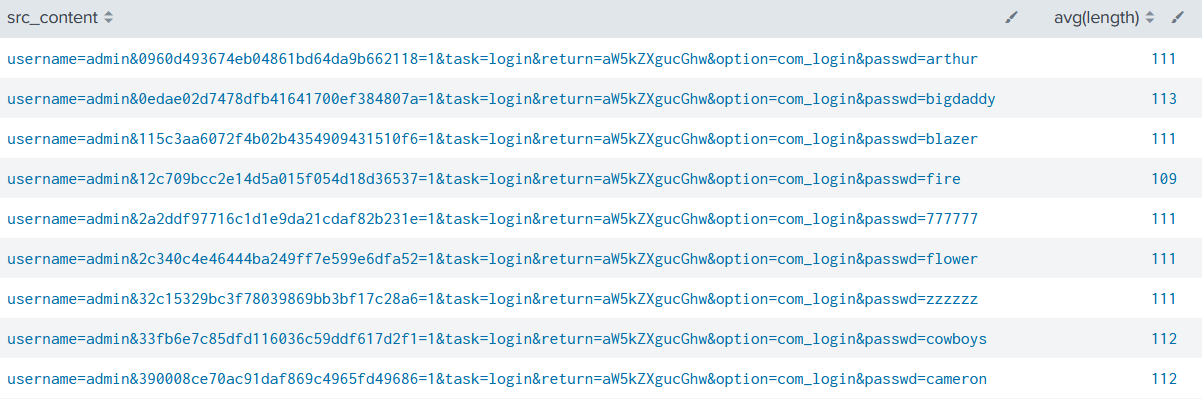
Xác định độ dài của src\_content trong mỗi request bruteforce:

source="stream:http" "imreallynotbatman.com" c\_ip="23.22.63.114" http\_method=POST

| eval length=len(src\_content)

| stats avg(length) by src\_content





Từ đó biết được độ dài của src\_content nếu không tính giá trị của passwd là 105 kí tự.

Từ câu trước, xác định được attacker bruteforce 412 lần.

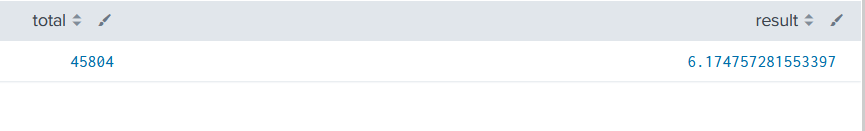
Tính trung bình độ dài password được nhập vào: (trung bình cộng độ dài src\_content) – 105.

source="stream:http" "imreallynotbatman.com" c\_ip="23.22.63.114" http\_method=POST

| eval length=len(src\_content)

| stats sum(length) as total

| eval result=total/412-105



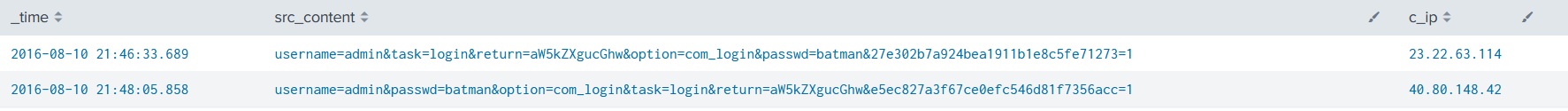
Kết quả là **6**.

#19. How many seconds elapsed between the time the brute force password scan identified the correct password and the compromised login? Round to 2 decimal places.

Từ câu 17 xác định được, attacker sử dụng ip=23.22.63.114 để bruteforce đăng nhập. Khi tìm được mật khẩu đúng attacker đăng nhập bằng ip=40.80.148.42; thực hiện lệnh search tìm ra thời gian tìm mật khẩu đúng và thời gian login:

sourcetype="stream:http" "imreallynotbatman.com" http\_method=POST src\_content="\*passwd=batman\*"

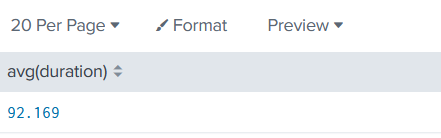
| stats count by \_time, src\_content, c\_ip



Tính toán thời gian:

| makeresults | eval duration = toString(strptime("2016-08-10 21:48:05.858","%Y-%m-%d %H:%M:%S.%3N") - strptime("2016-08-10 21:46:33.689","%Y-%m-%d %H:%M:%S.%3N"))

| stats avg(duration)



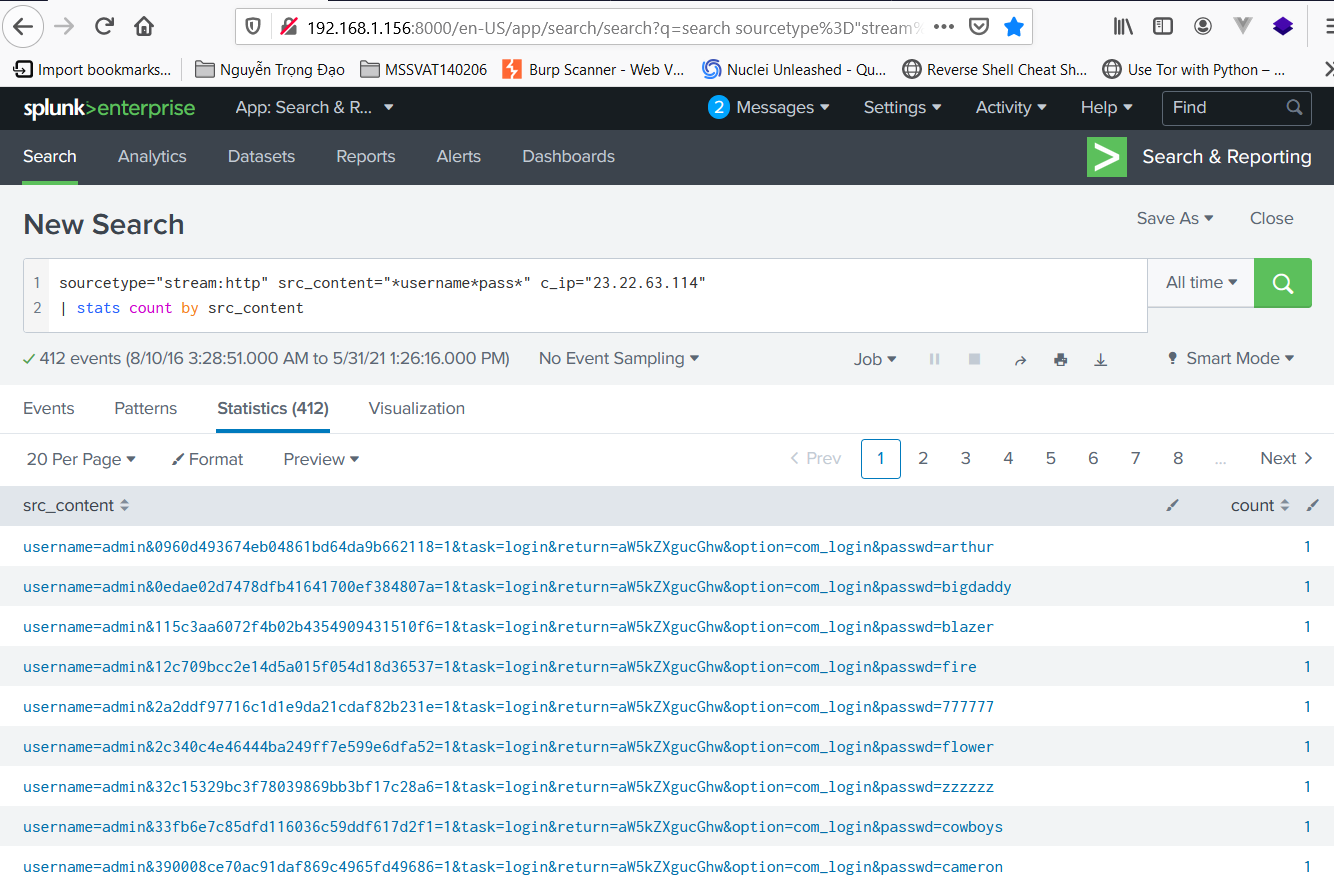
Kết quả là **92.17**

#20. How many unique passwords were attempted in the brute force attempt?

Tìm kiếm số password mà ip 23.22.63.114 brute force.

sourcetype="stream:http" src\_content="\*username\*pass\*" c\_ip="23.22.63.114"

| stats count by src\_content



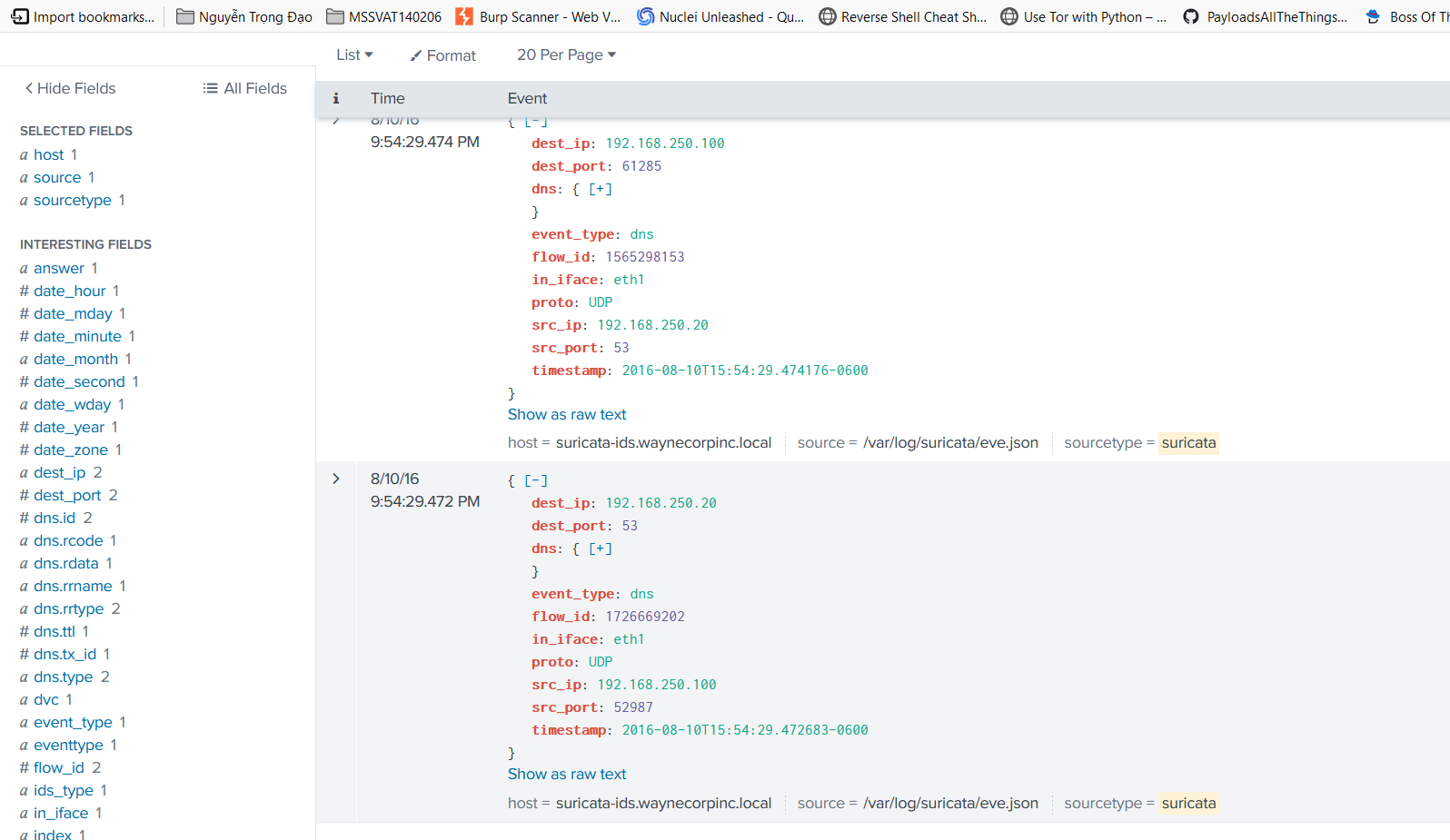
Có **412** event.

#21. What was the most likely IP address of we8105desk on 24AUG2016?

Tìm kiếm tại sourctype=suricata

sourcetype=suricata "we8105desk"

ra 2 event



Xác định được ip của we8105desk là: **192.168.250.100**

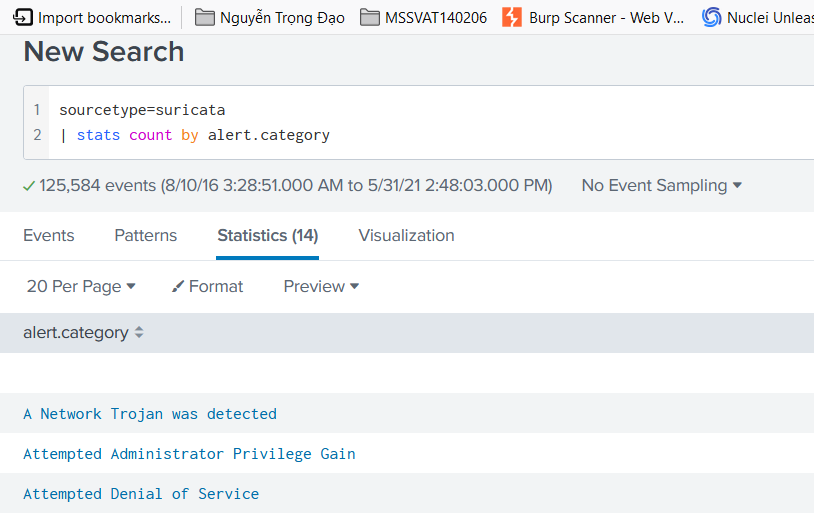
#22. Amongst the Suricata signatures that detected the Cerber malware, which one alerted the fewest number of times? Submit ONLY the signature ID value as the answer. (No punctuation, just 7 integers.)

Xem có những loại cảnh báo gì trên suricata

sourcetype=suricata

| stats count by alert.category

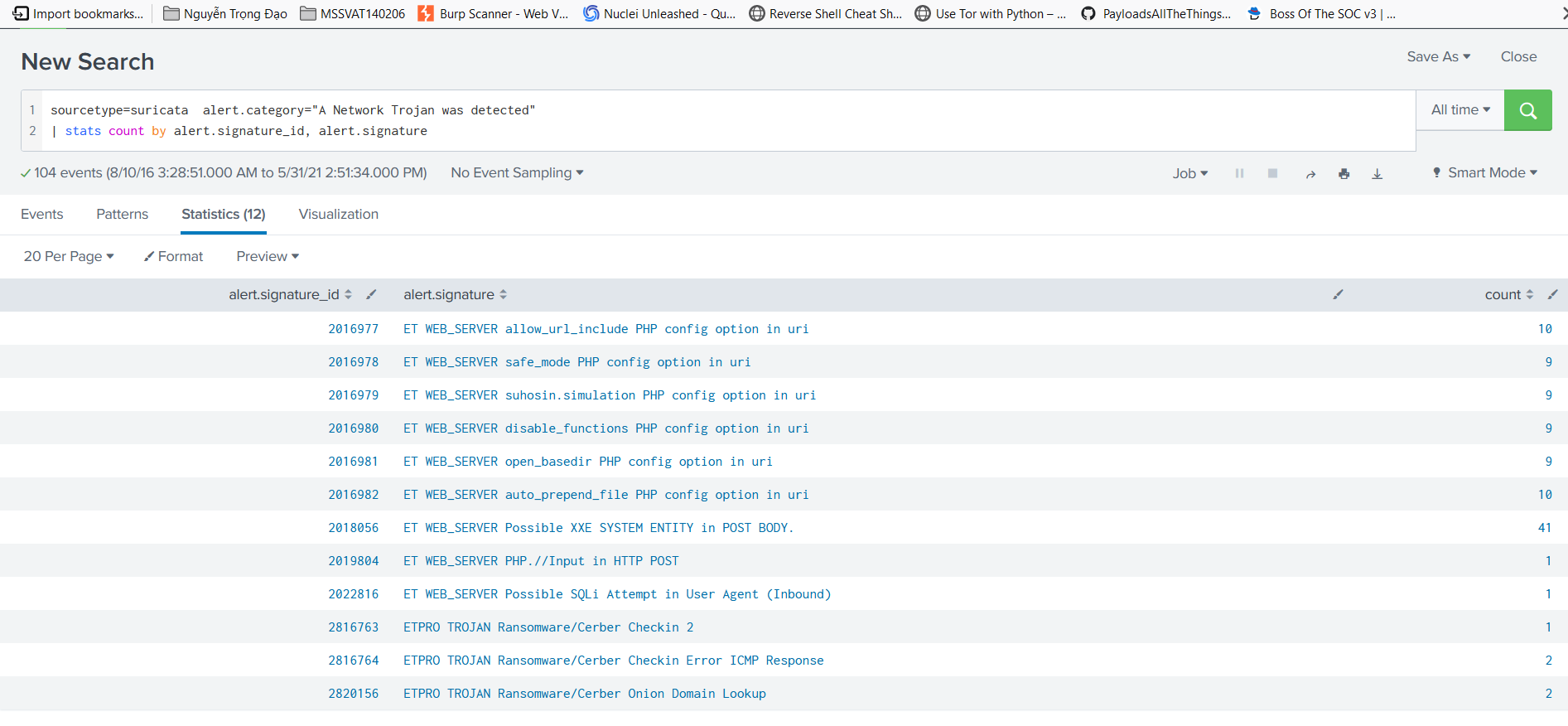
Phát hiện có cảnh báo về network Trojan



Tìm kiếm alert.signature và số lần cảnh báo

sourcetype=suricata alert.category="A Network Trojan was detected"

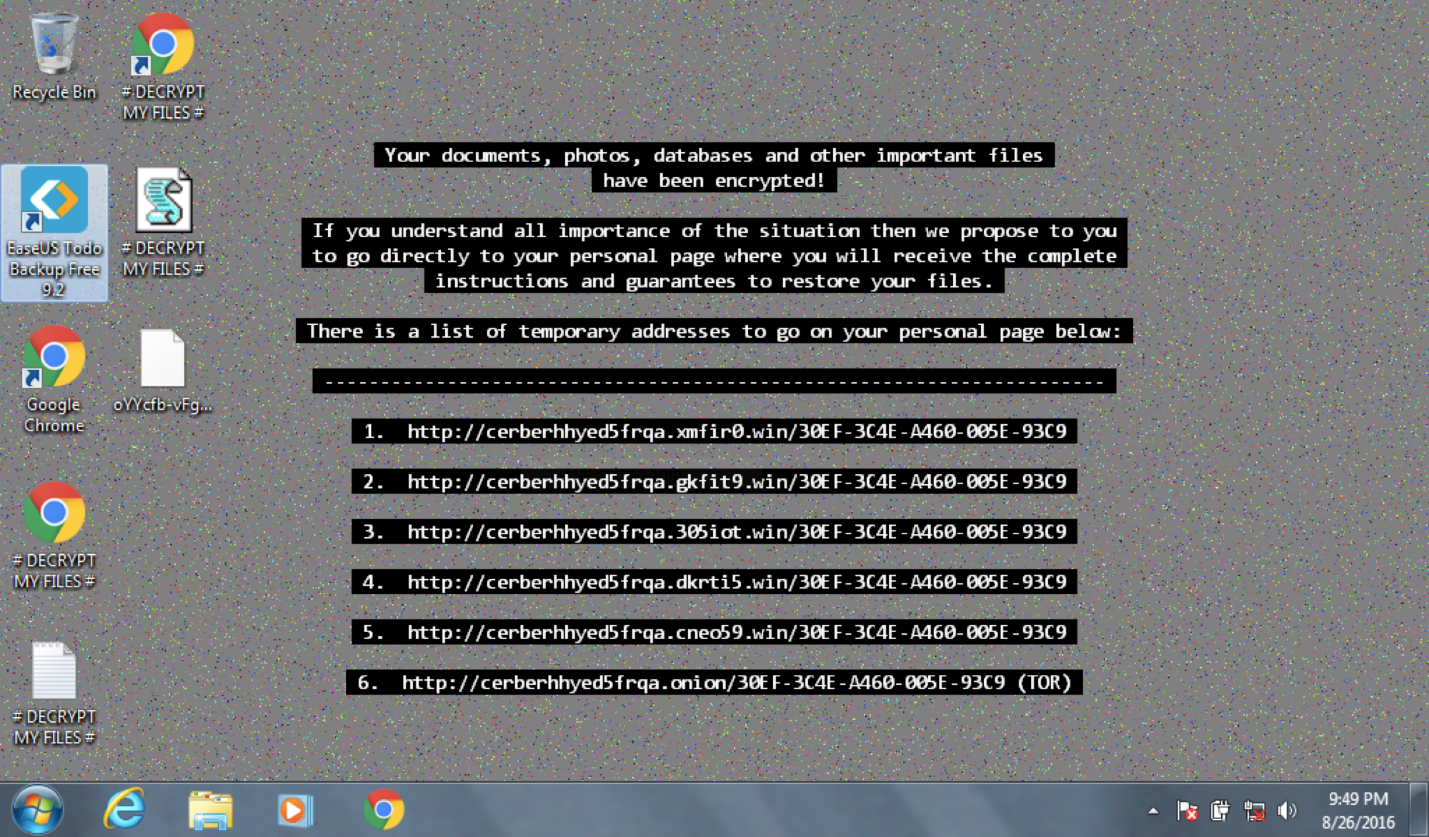
| stats count by alert.signature\_id, alert.signature





Kết quả là **2816763**

#23. What fully qualified domain name (FQDN) does the Cerber ransomware attempt to direct the user to at the end of its encryption phase?

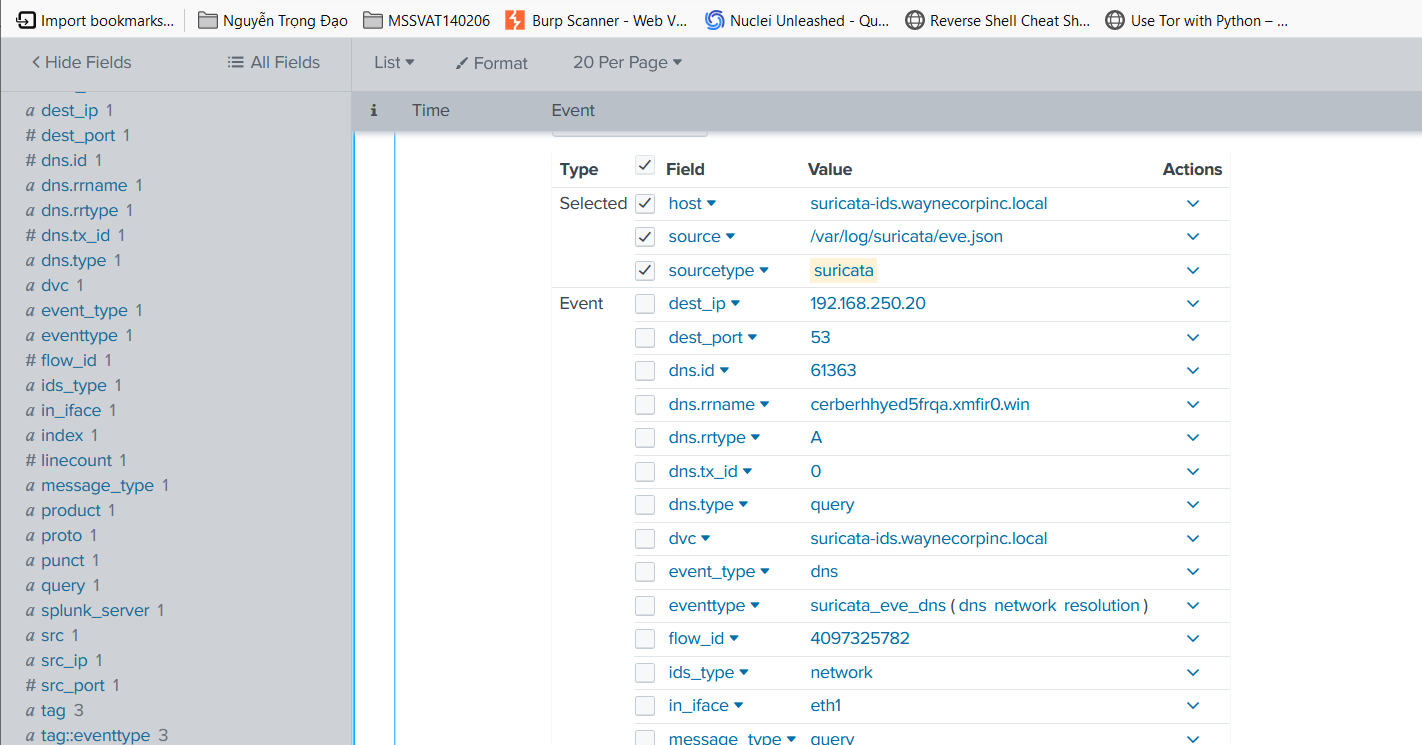


Hình trên là máy nạn nhân bị dính ransomware, các file bị mã hóa và bị đổi background kèm theo 6 link đòi tiền chuộc.

Tìm kiếm xem có sự kiện gì liên quan đến cerberhhyed5frqa hay không.

sourcetype="suricata" src\_ip="192.168.250.100" "\*cerberhhyed5frqa\*"

phát hiện 1 event truy vấn dns



Trong đó có yêu cầu phân giải tên miền [cerberhhyed5frqa.xmfir0.win](http://192.168.1.156:8000/en-US/app/search/search?q=search%20sourcetype%3D%22suricata%22%20src_ip%3D%22192.168.250.100%22%20%22*cerberhhyed5frqa*%22&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=now&display.page.search.tab=events&display.general.type=events&sid=1622515311.513)

#24. What was the first suspicious domain visited by we8105desk on 24AUG2016?

Xác định được ip của host **we8105desk** là 192.168.250.100.

Setting thời gian search trong ngày 24/08/2016

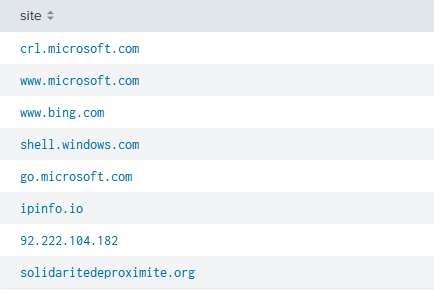


Sử dụng sourcetype stream:http, tìm kiếm những site 192.168.250.100 truy cập trong ngày 24/08/2016.

sourcetype="stream:http" c\_ip="192.168.250.100"

| dedup site

| table site



Thấy domain **solidaritedeproximite.org** và ip 92.222.104.182 là bất thường.

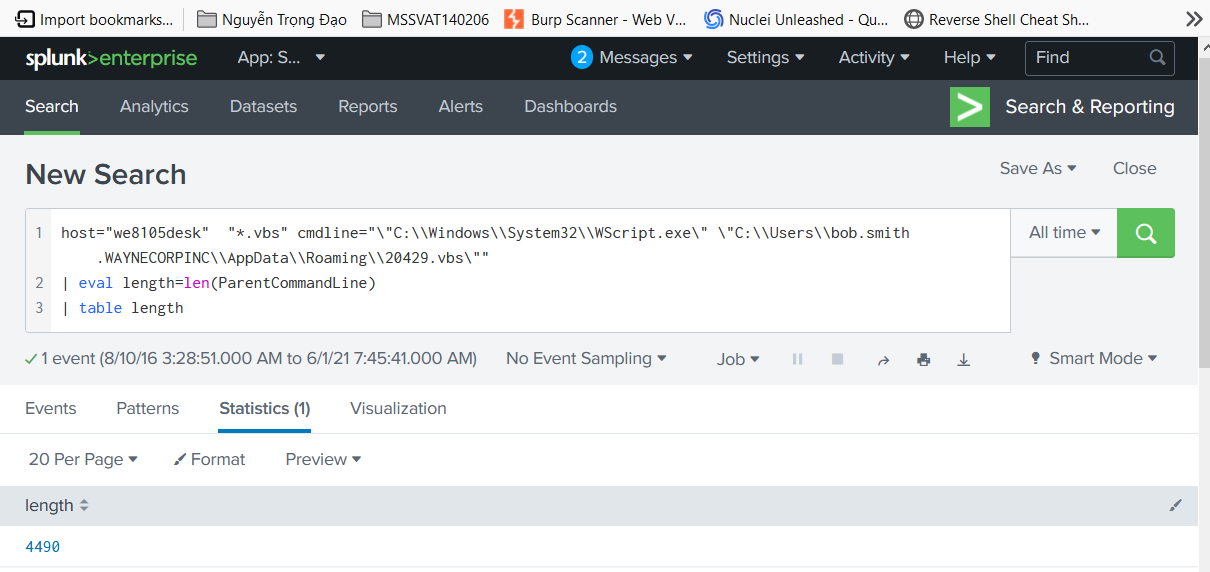
#25. During the initial Cerber infection a VB script is run. The entire script from this execution, pre-pended by the name of the launching .exe, can be found in a field in Splunk. What is the length in characters of the value of this field?

host="we8105desk" "\*.vbs" cmdline="\"C:\\Windows\\System32\\WScript.exe\" \"C:\\Users\\bob.smith.WAYNECORPINC\\AppData\\Roaming\\20429.vbs\""

host="we8105desk" "\*.vbs" cmdline="\"C:\\Windows\\System32\\WScript.exe\" \"C:\\Users\\bob.smith.WAYNECORPINC\\AppData\\Roaming\\20429.vbs\""

| eval length=len(ParentCommandLine)

| table length



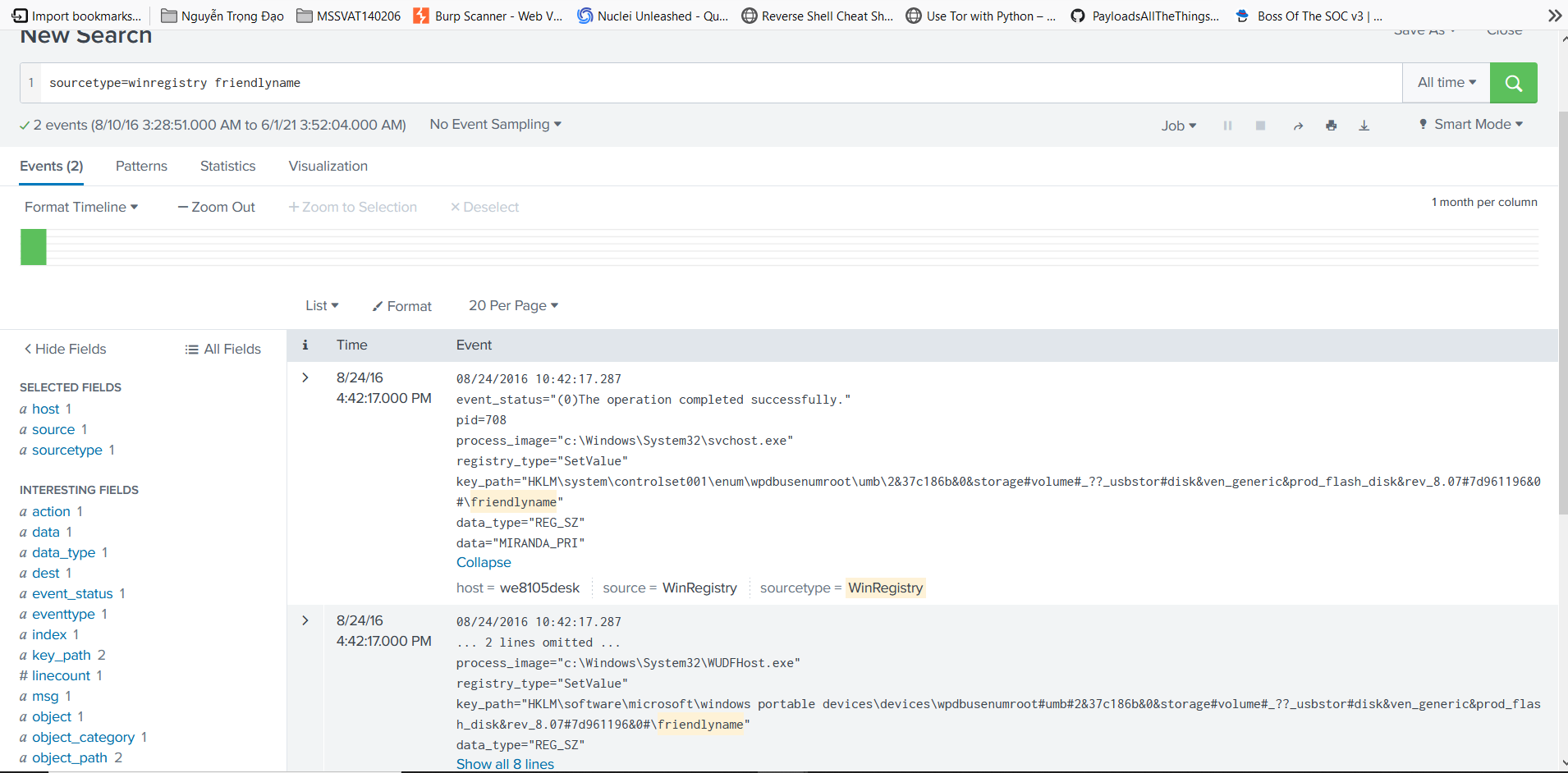
Đáp án là **4490**

#26. What is the name of the USB key inserted by Bob Smith?

Tìm kiếm các thiết bị USB trong WinRegistry

sourcetype=winregistry friendlyname

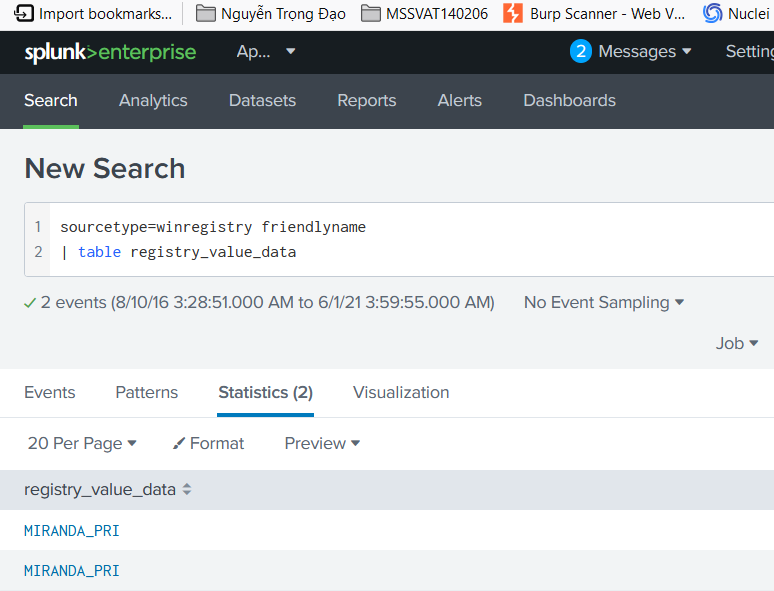
Có 2 event



Tên của USB sẽ nằm trong trường registry\_value\_data

sourcetype=winregistry friendlyname

| table registry\_value\_data



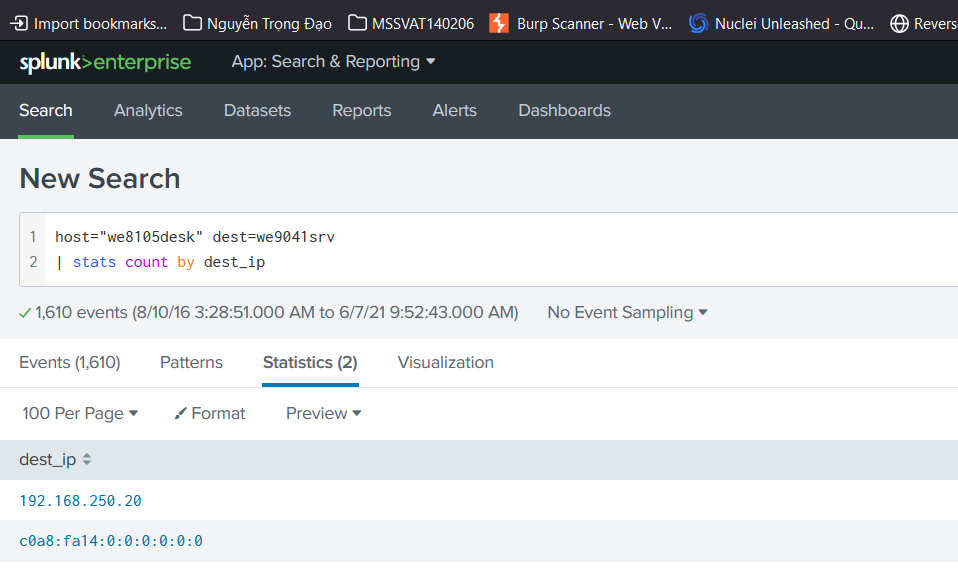
#27. Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak. What is the IP address of the file server?

Có 2 server là we1149srv, we9041srv ; trong đó we1148srv là web server, từ đó biết được we9041srv là file server, hơn nữa trong log của we9041 có trường share\_path, đường dẫn các thư mục được share.

Tìm kiếm địa chỉ ip của we9041srv

host="we8105desk" dest=we9041srv

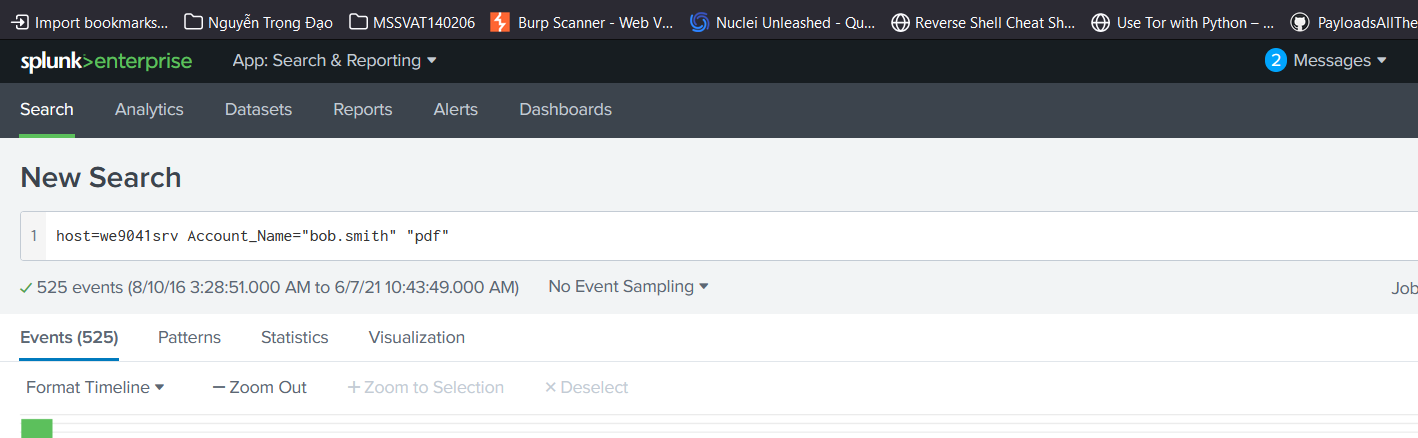
| stats count by dest\_ip



#28. How many distinct PDFs did the ransomware encrypt on the remote file server?

Tìm kiếm những event liên quan tới bob.smith tại file server.

host=we9041srv Account\_Name="bob.smith" "pdf"

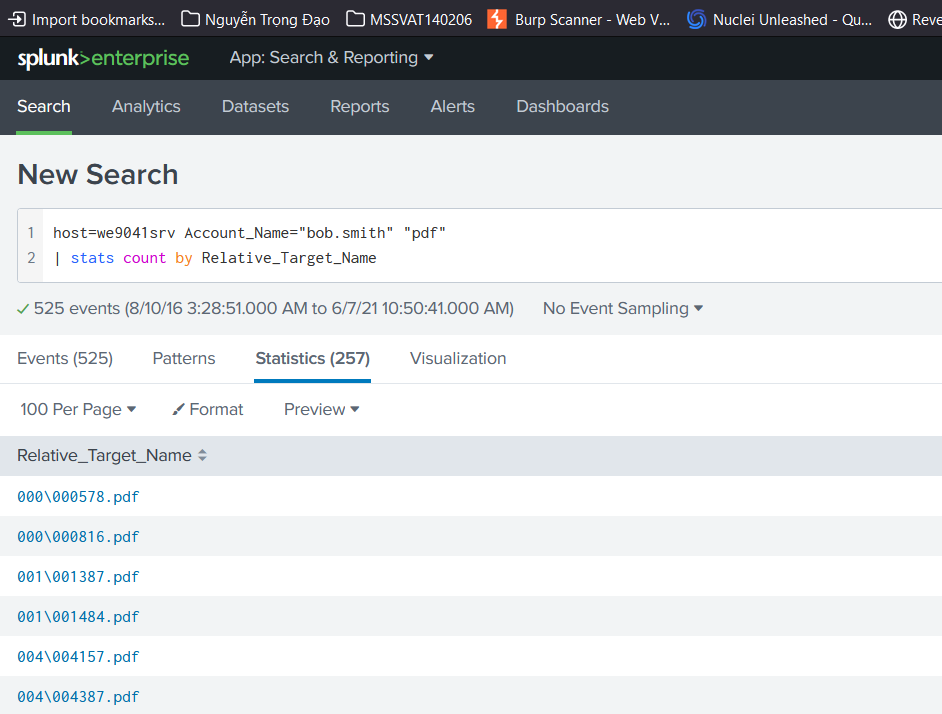


Có hơn 500 event.

Search những file pdf mà bob.smith có khả năng truy cập đến.

host=we9041srv Account\_Name="bob.smith" "pdf"

| stats count by Relative\_Target\_Name

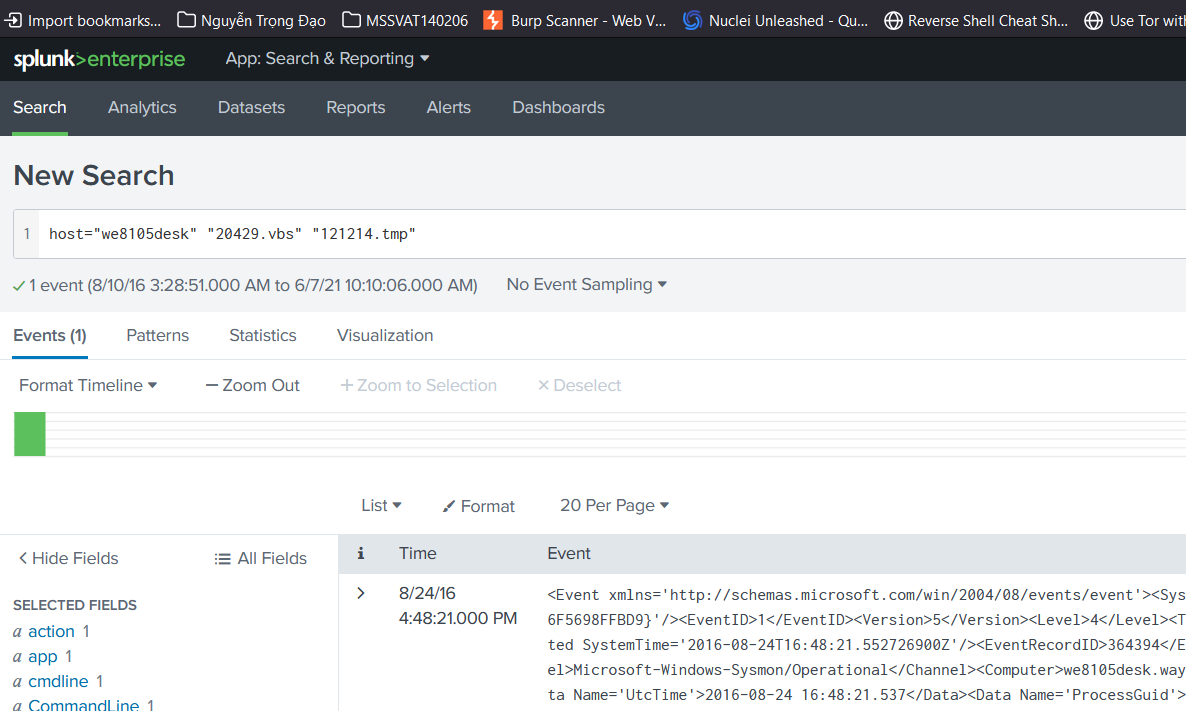


Đáp án là **257**

#29. The VBscript found in question 25 launches 121214.tmp. What is the ParentProcessId of this initial launch?

Tại câu 25, xác định được file 20429.vbs sẽ được khởi chạy, tìm kiếm event liên quan tới 20429.vbs và 121214.tmp

host="we8105desk" "20429.vbs" "121214.tmp"



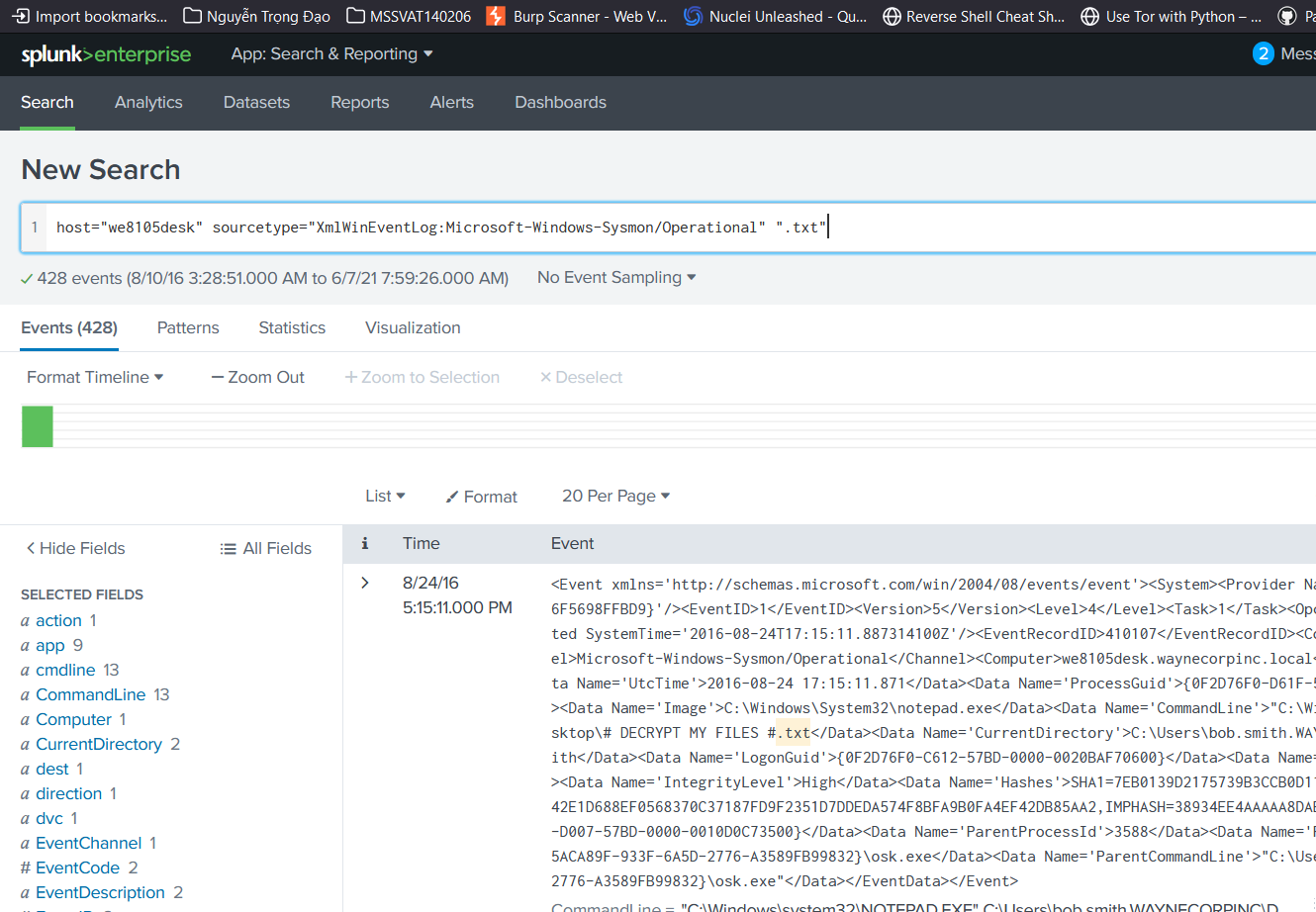
Có 1 event, tìm kiếm trường ParentProcessId

Đáp án là **3968**

#30. The Cerber ransomware encrypts files located in Bob Smith's Windows profile. How many .txt files does it encrypt?

Tìm kiếm theo log Sysmon của we8105desk, các event liên quan tới file .txt

host="we8105desk" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" ".txt"



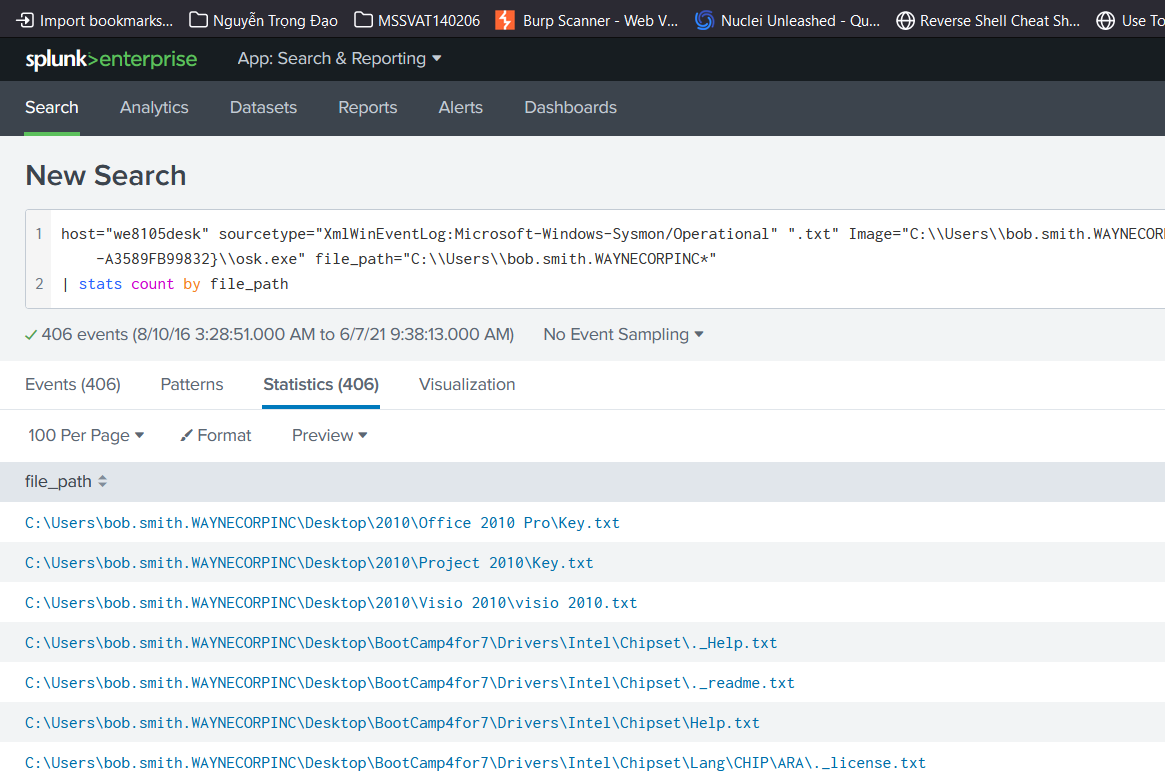
Có 428 event, đọc qua một số event thấy có tiến trình osk.exe tác động đến nhiều file txt.

Osk.exe là tiến trình bình thường của Microsoft nằm trong thư mục C:\Windows\System32 , nhưng tiến trình osk.exe này nằm trong C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\{ 35ACA89F-933F-6A5D-2776-A3589FB99832}\osk.exe 🡪 phần mềm độc hại tự ngụy trang thành osk.exe

Tìm kiếm những file txt trong thư mục của Bob Smith liên quan tới osk.exe

host="we8105desk" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" ".txt" Image="C:\\Users\\bob.smith.WAYNECORPINC\\AppData\\Roaming\\{35ACA89F-933F-6A5D-2776-A3589FB99832}\\osk.exe" file\_path="C:\\Users\\bob.smith.WAYNECORPINC\*"

| stats count by file\_path



Đáp án là **406**

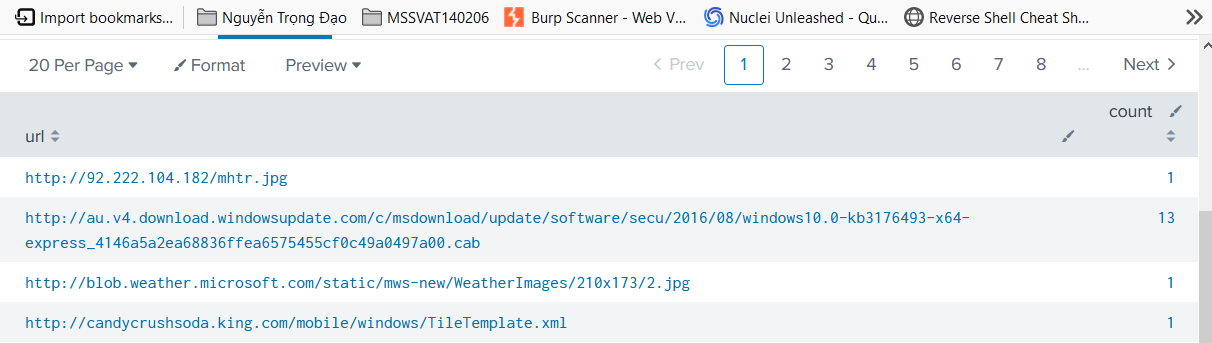
#31. The malware downloads a file that contains the Cerber ransomware cryptor code. What is the name of that file?

Tìm kiếm những kết nối bên ngoài từ we8105desk

sourcetype="stream:http" c\_ip="192.168.250.100"

| stats count by url

Xuất hiện kết nối đáng nghi tới địa chỉ 92.222.104.182 download file mhtr.jpg



Qua tìm kiếm trên mạng phát hiện đây là file độc hại, cerber ransomware được nhúng vào trong file ảnh mhtr.jpg

<https://blog.checkpoint.com/2016/07/05/check-point-forensic-files-cerber-ransomware-distribution-using-office-dotm-files/>

#32. Now that you know the name of the ransomware's encryptor file, what obfuscation technique does it likely use?

Đọc mô tả về Cerber ransomware sẽ biết được nó sử dụng **steganography** để ẩn sự tồn tại.

Tài liệu tham khảo:

Cerber ransomware: <https://www.netskope.com/blog/anatomy-ransomware-attack-cerber-uses-steganography-hide-plain-sight>

WinRegistry: <https://docs.microsoft.com/en-us/windows-hardware/drivers/usbcon/usb-device-specific-registry-settings>

Investigating a ransomware attack: <https://lantern.splunk.com/hc/en-us/articles/360049244873>