Security Information and Event Monitoring (Splunk)

Overview

In this lab you act as the on-call responder for an active web-facing incident. Across four coordinated Splunk investigations you will: identify and quantify credential brute-force attempts against a Joomla admin endpoint; track a high-volume vulnerability scanner (and its tools and origin) via Fortigate UTM logs; investigate a suspicious executable discovered in the Windows registry using Sysmon, OSINT, and reputation services; and validate / extend an operational security dashboard using Suricata and Fortigate alerts. The scenario emphasizes rapid triage, event correlation across multiple sourcetypes, enrichment with external intelligence, and turning log findings into containment- and remediation-focused actions.

Tools, log sources & techniques used

- **Splunk** — complex searches, spath, table, stats, sorting, saved dashboards, and event sampling controls.
- **Web/application logs** — stream:http sourcetype, POST body inspection (form_data), HTTP status analysis.
- **Firewall / UTM** — fortigate_utm sourcetype for scanner identification, source geolocation, destination IPs, and enrichment fields.
- **Network IDS/IPS** — Suricata alerts for signature-based detection (Information Leak, Trojan, CVE-linked signatures).
- **Endpoint telemetry** — Sysmon (xmlwineventlog) for process creation, ImageLoaded hashes, network connections, and EventID correlation.
- **OSINT & reputation services** — Google (osk.exe research), VirusTotal (SHA256 lookup), and NVD for CVE/CVSS lookups.
- **Investigation workflow** — pivoting from events to fields (e.g., src_ip, destination ports), narrowing queries with spath / field filters, exporting evidence, and using stats / table to find counts, uniques, and timelines.

Splunk Investigation 1

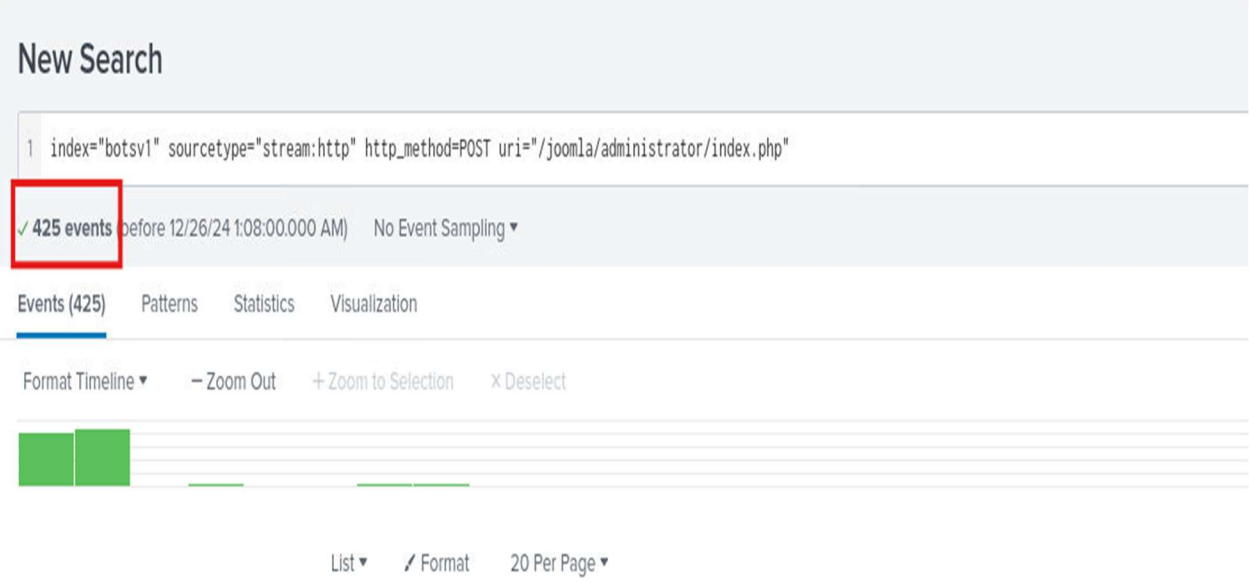
PROMPT:

Alongside the vulnerability scan our security tools have alerted us to a malicious actor that is brute forcing accounts for the website. We need you to investigate, find out where the attack is coming from, if they were successful, and if they were, what did they do with their access. This is an extremely time-sensitive investigation, every second is potentially more time the attacker has control over systems on the server.

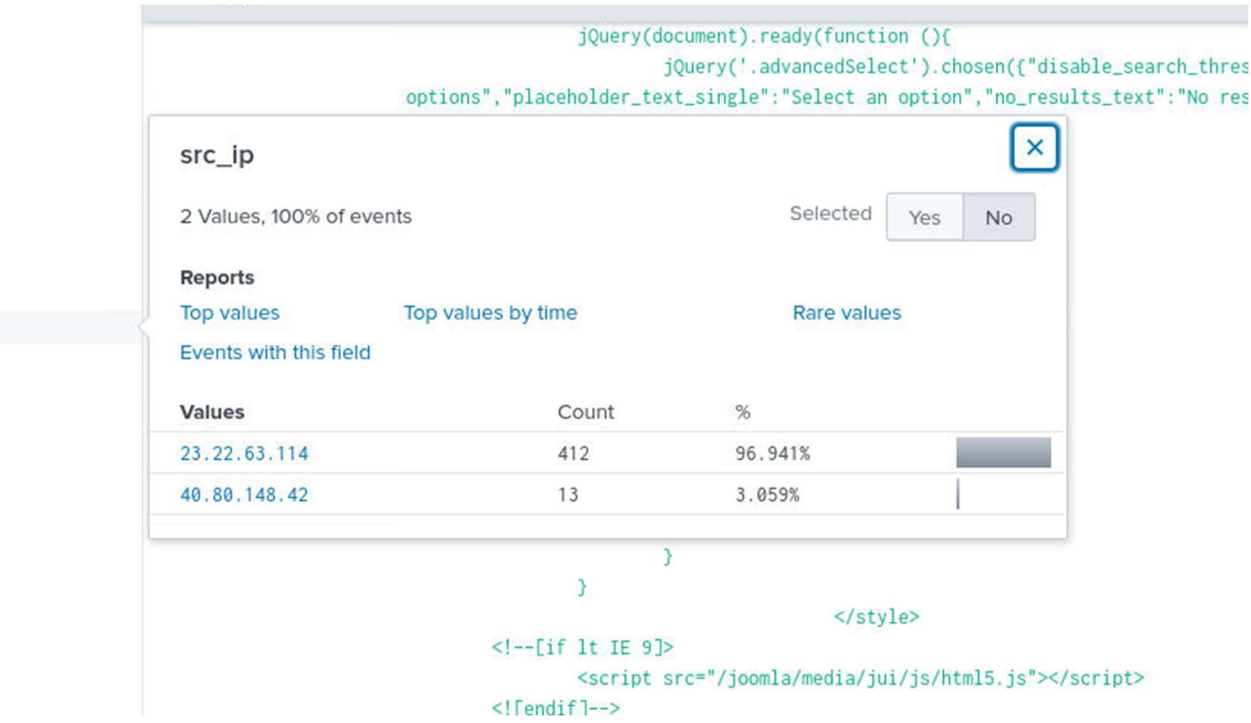
This investigation isn't as simple as looking at one type of event sourcetype. You will need to use your analysis skills to investigate and compare different log types to work out exactly what has happened. As a starting point, we know the administrator URL is

http://imreallynotbatman.com/joomla/administrator/index.phpand that usernames and passwords will be submitted in an HTTP POST request (http_method=POST). Ensure that event sampling is set to 'No Event Sampling' so we can see every single event. Let's investigate!

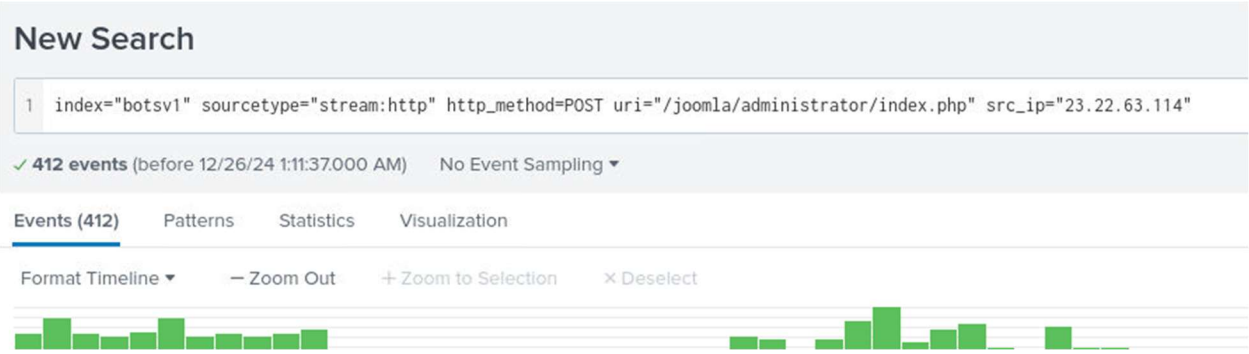
1. Use the following search query to identify the malicious activity index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php". How many events have been identified?



2. Under the 'Interesting Fields' on the left scroll down to 'src_ip'. Click on it to view the count of events per source IP. Which IP address is the source IP for the majority of the traffic?



3. Left-click the IP address with the highest % of events to add it to our search query. How many events are there in total now?



4.What is the destination IP? (IP address of our web server hosting imreallynotbatman.com)

After adding "imreallynotbatman.com" to the search

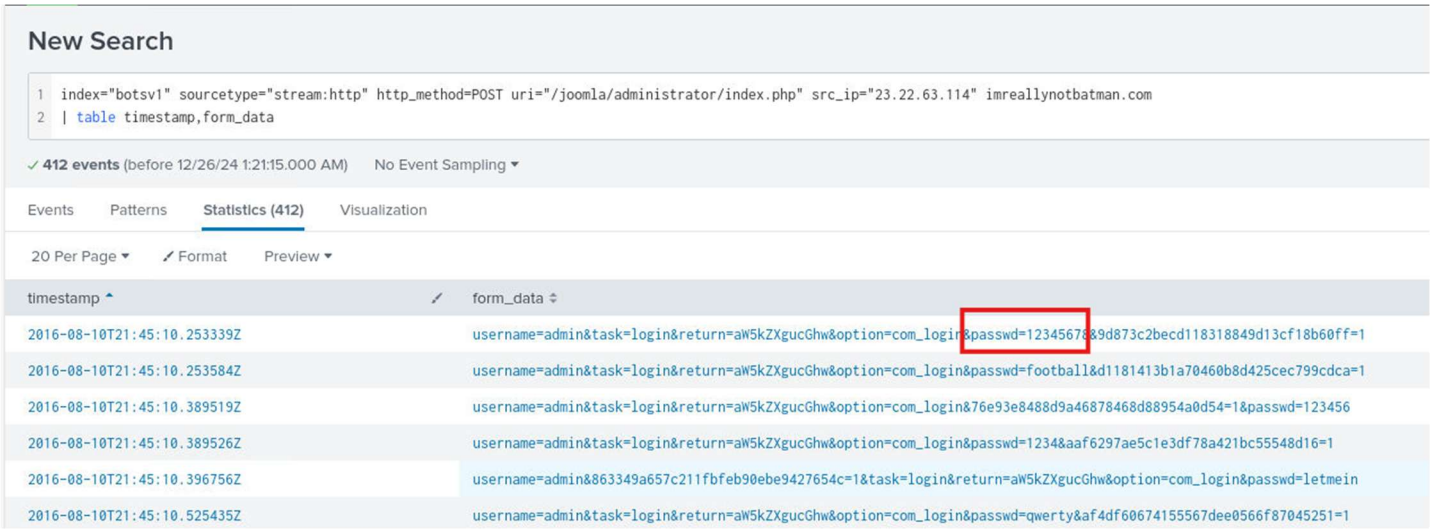
5. Let's take a look at one of these requests to see exactly what's going

on. Add the following to the end of your current search query | spath timestamp | search timestamp="2016-08-10T21:46:44.453730Z". Identify the form_data value in the event. What is the username the attacker is trying to use? (only include the string before the '&')

6. What is the password that is being entered in the form_data value? (only include the string before the '&')

7. We can better visualize the form_data values using the table functionality. Remove the details about timestamps from your search query and add the following | table timestamp,form_data. Once this has loaded click the timestamp column heading to sort by

the oldest event first (arrow pointing up). What was the first password in the brute-force attack? (only include the string before the '&')



Splunk Investigation 2

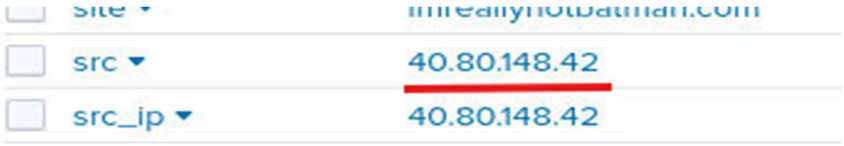
PROMPT:

Our website has shown signs of high resource usage, but it doesn't look like a distributed denial-of-service attack, because the requests are coming from one single IP address. They seem to be performing a port scan and trying to access different resources on the website - it could be a vulnerability scanner. We need you to investigate and gather information about this activity, including where it's coming from, what tools they are using, and the resources they have accessed. We run routine checks, but if they find something we haven't seen before, this could get bad really quick.

Instead of looking through thousands of web logs we can look at logs from the Fortigate firewall, specifically the Unified Threat Management solution, so make sure to set your sourcetype as fortigate_utm. You should search for our domain name as a string, "imreallynotbatman.com" and the string "vulnerability" to find events related to this activity.

1. What is the name of the web vulnerability scanner that is being used?

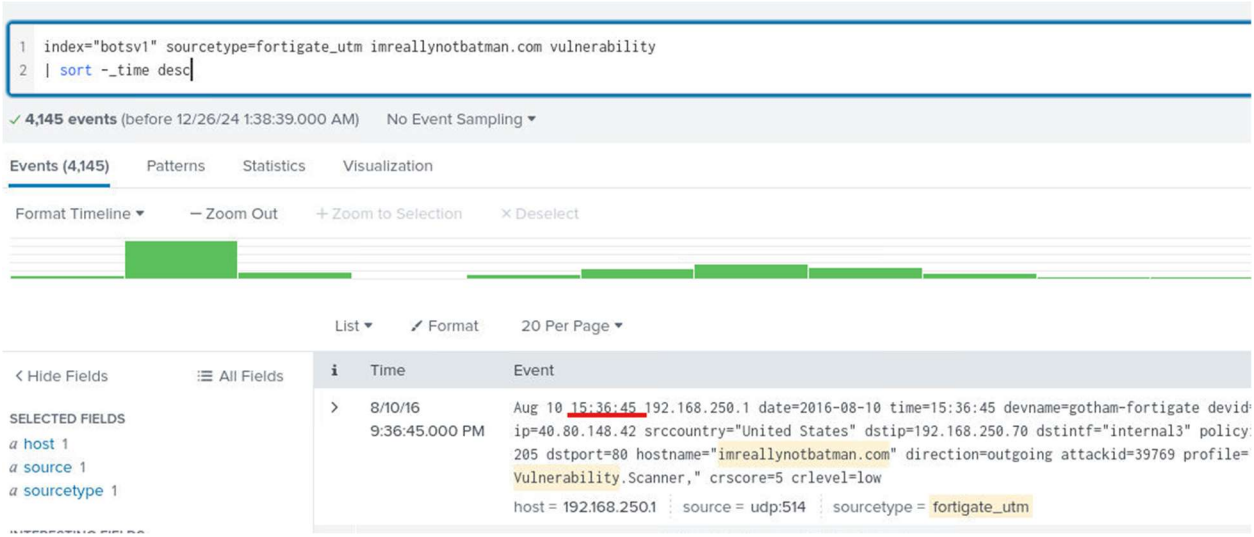
2. What is the source IP of the vulnerability scanner, and therefore the attacker?



3.What is the destination IP? (the internal address for our web server)

4. Fortigate UTM provides enrichment, and can tell us the source IP country based on a lookup. What country is the scanning IP associated with?

5. What is the log 'time' field value for the first Fortigate UTM log referencing the vulnerability scan, on 8/10/16, in the format HH:MM:SS? (Use Sort!)



Splunk Investigation 3

PROMPT:

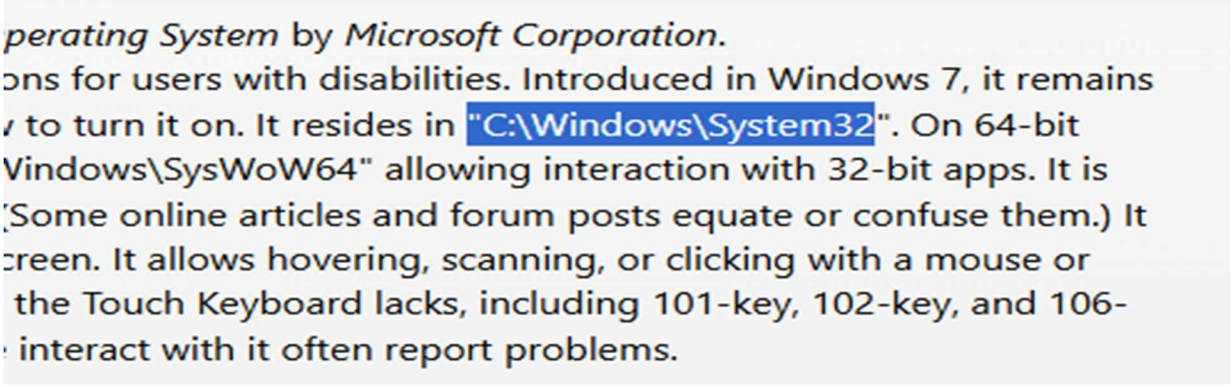
One of our IT technicians has reported an unexpected file in the registry of an employee they were assisting. You have been tasked with investigating using various log sources and OSINT to understand if the file is legitimate or malicious, and what it is doing.

1. OSINT can be extremely useful in almost every investigation. Perform a Google search for osk.exe - what is the full name of the Windows feature associated with osk.exe?

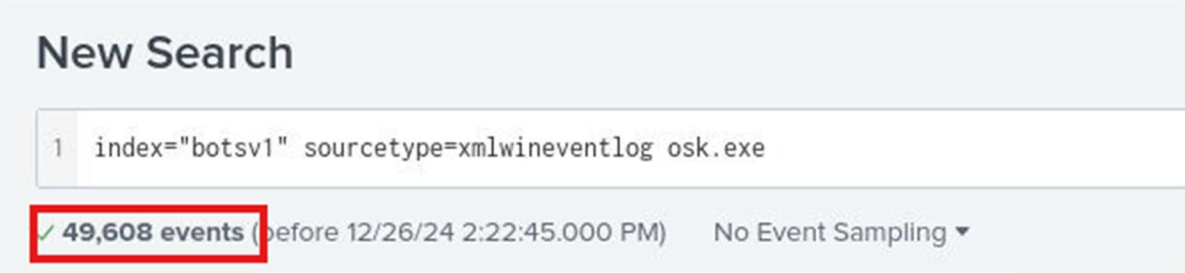
What is osk.exe?

The genuine *osk.exe* file is a software component of *Microsoft Windows Operating System* by *Microsoft Corporation*.
"OSK.exe" is Microsoft's On-Screen Keyboard, part of its Ease of Use options for users with disabilities. Introduced in Windows 7, it remains available in Windows 8.1 and 10, although each version has changed how to turn it on. It resides in "C:\Windows\System32". On 64-bit systems there are two versions with the same name, with the one in "C:\Windows\SysWoW64" allowing interaction with 32-bit apps. It is not the same as the Touch Keyboard in "TabTip.exe" and "TabTip32.exe". (Some online articles and forum posts equate or confuse them.) It presents a virtual keyboard layout in an actual resizable window on the screen. It allows hovering, scanning, or clicking with a mouse or game joystick to select and activate keys, but not touch. It offers features the Touch Keyboard lacks, including 101-key, 102-key, and 106-key layouts. It is convenient for users but developers trying to make code interact with it often report problems.

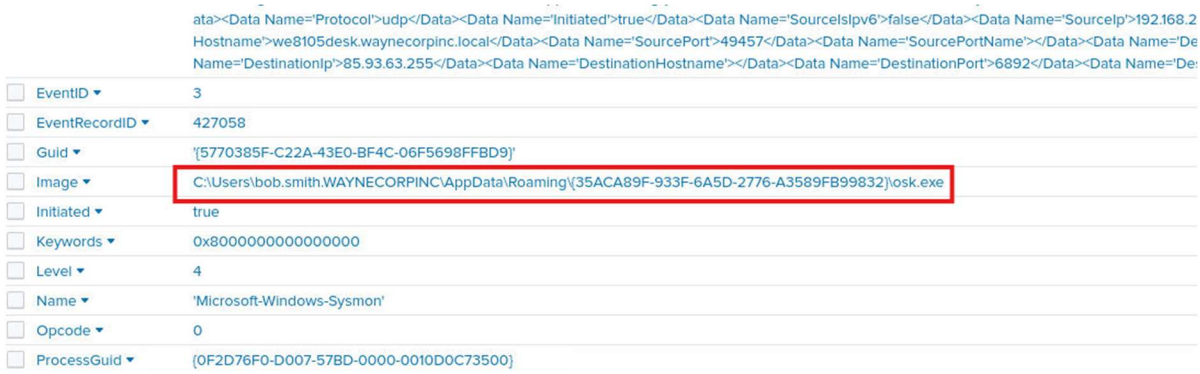
2. Continue with your OSINT research. What is the expected file path for osk.exe? (Path to the folder, or full file paths are accepted)



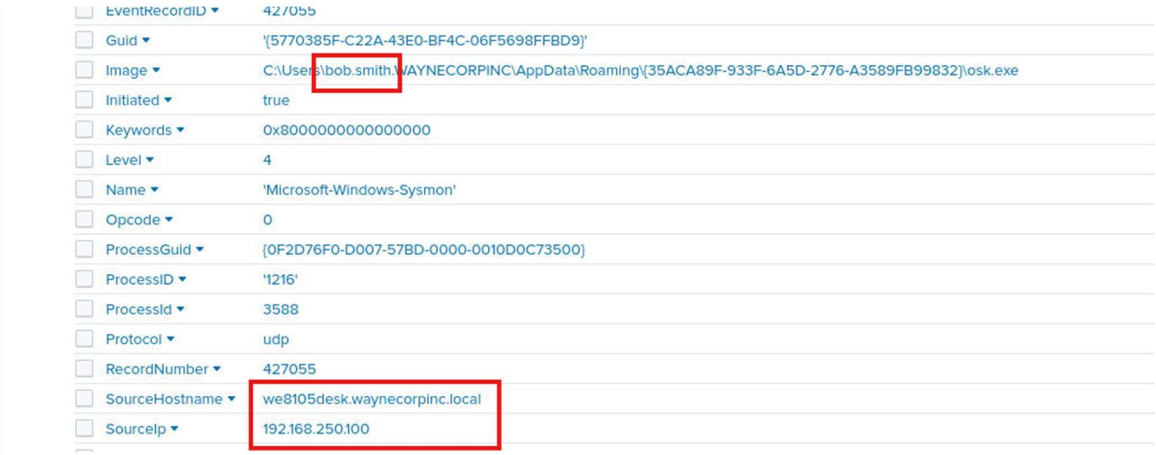
3. Filter on Sysmon events (sourcetype=xmlwineventlog) and search for the suspicious executable name. How many events are returned based on this query?



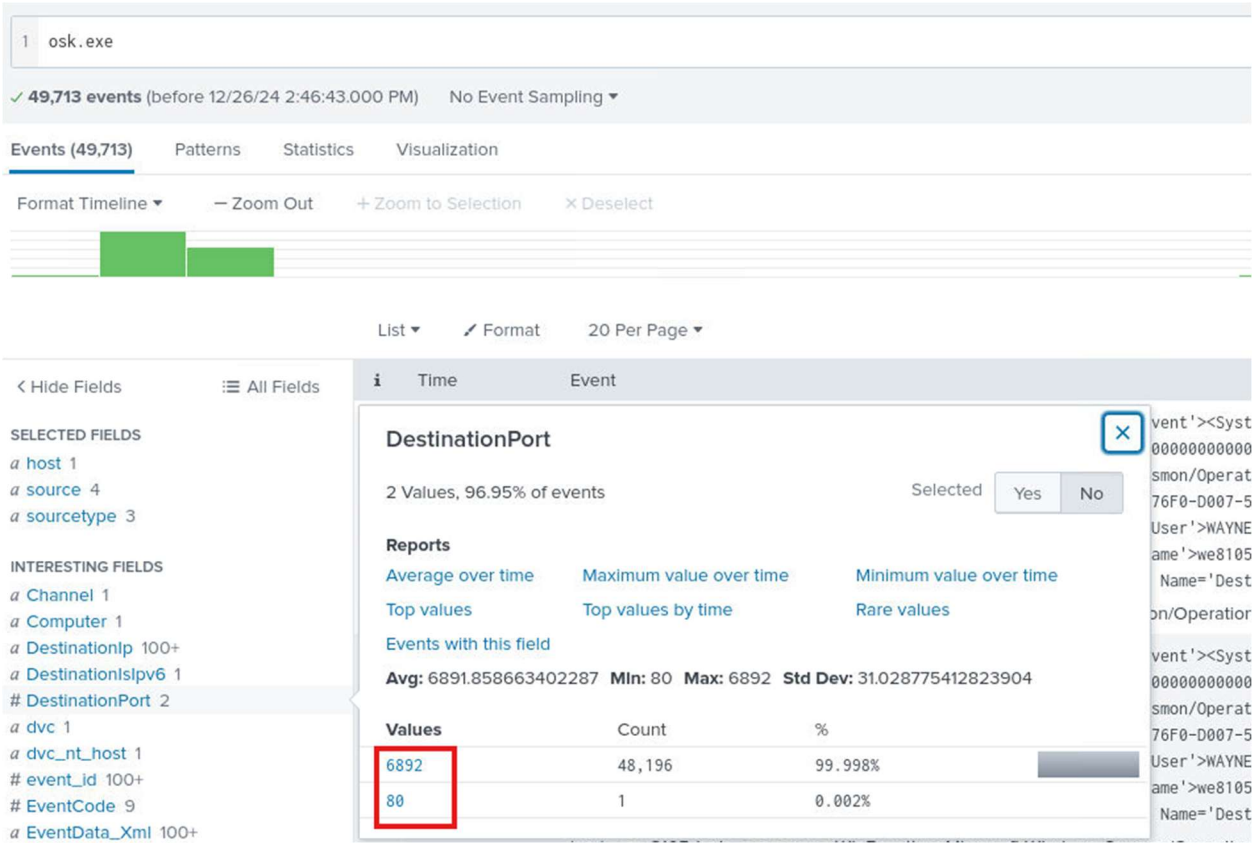
4. What is the full file path of the suspicious executable?



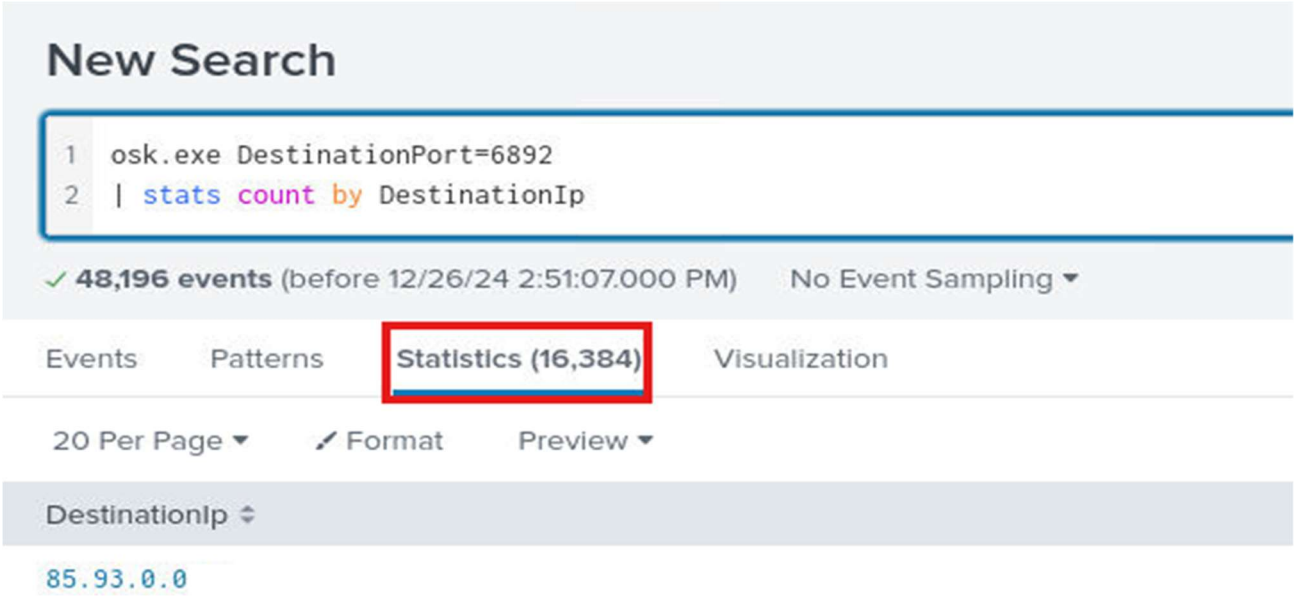
5. What computer is the suspicious file running on, what is the internal IP address, and which user account is running it?



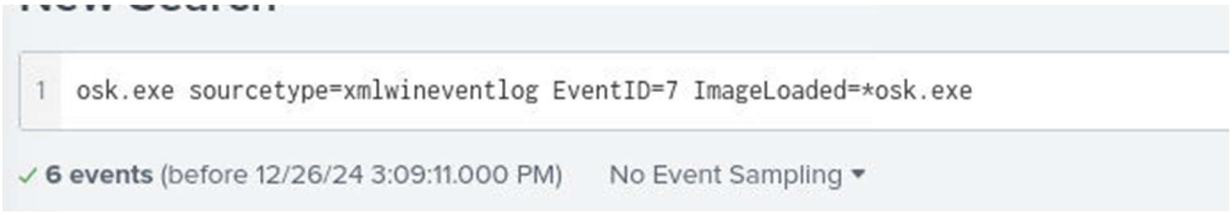
6. To scope our next searches only on this executable, find an appropriate field + value pair to add to your search query. Next it's a good idea to see if there are any network connections - what destination ports is this file connecting to?

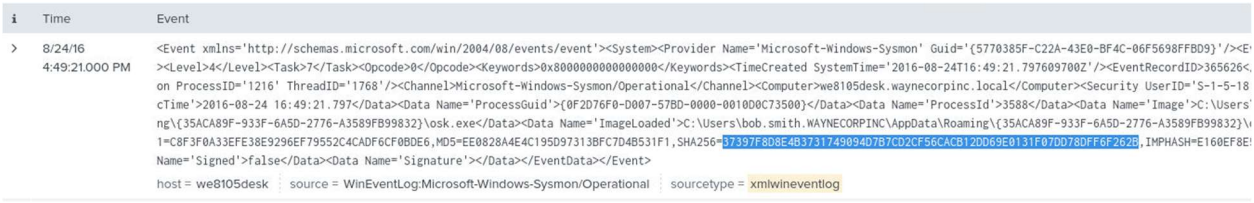


7. Adding the destination port with the highest activity to your query, use 'stats count' functionality to identify the number of unique destination IP addresses this file is connecting to

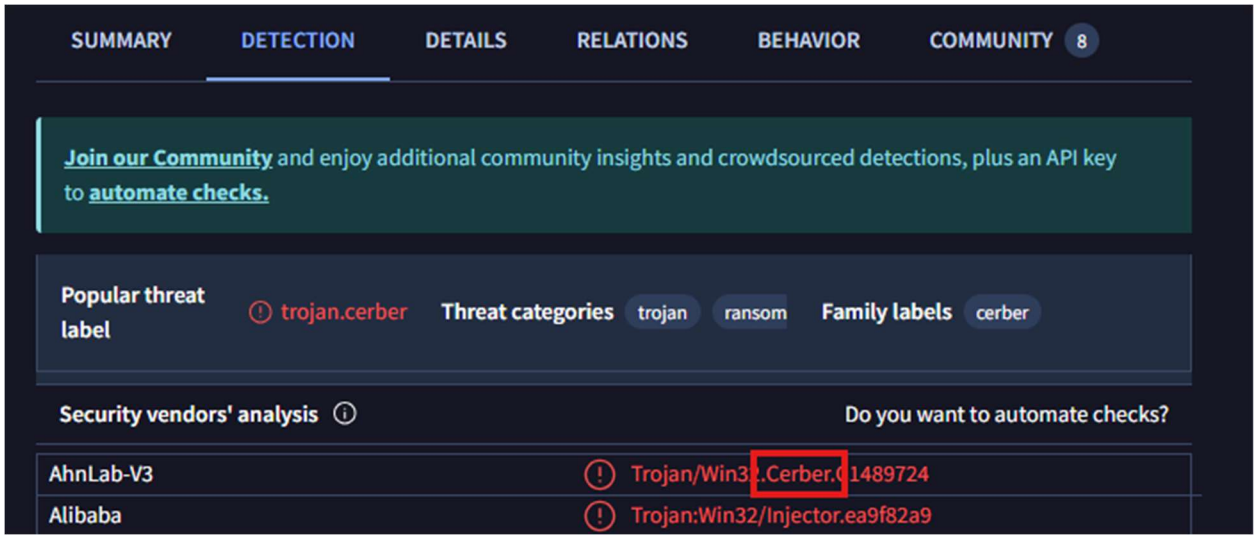


8. Sysmon EventID 7 logs contain the hash values of files (ImageLoaded field) that are executed. Use this to find the SHA256 hash of the suspicious osk.exe and submit it

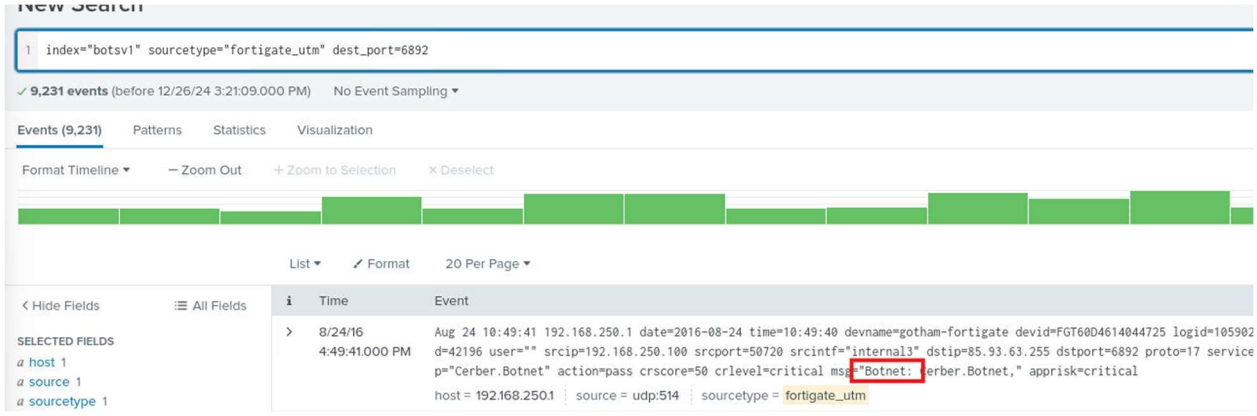




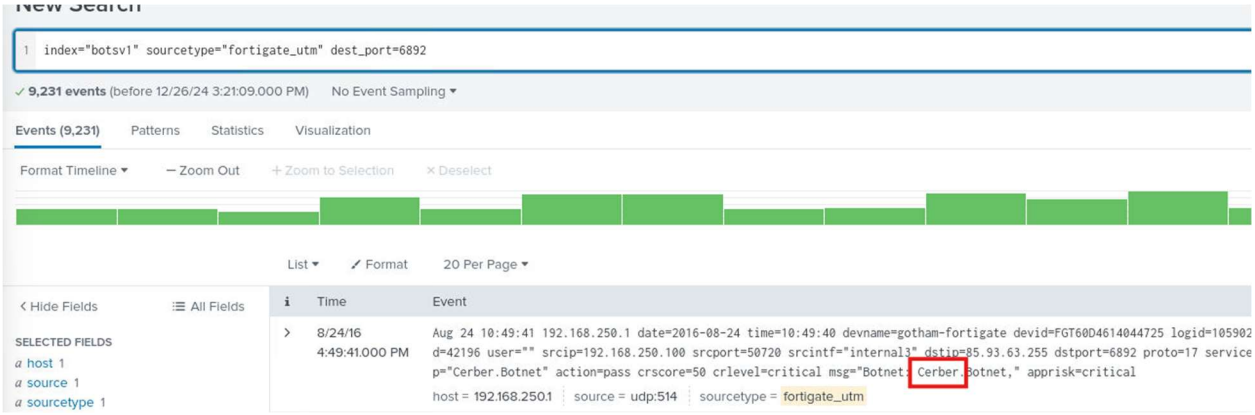
9. Outside of the lab, submit the SHA256 hash to VirusTotal. Based on the results on the Detection page, what is the potential name of this malware?



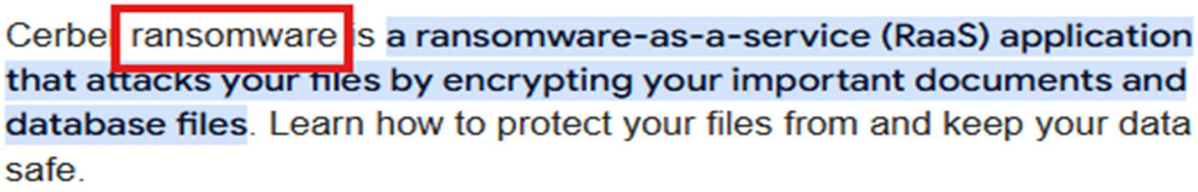
10. Sysmon was useful, but let's investigate the network traffic coming from the suspicious file out to thousands of IP addresses. To do this we'll look at the Fortigate Unified Threat Management logs. Find something all (but one) of the osk.exe sysmon logs have in common regarding network traffic and use this in your search query. What is the category of malware dedicated by Fortigate?



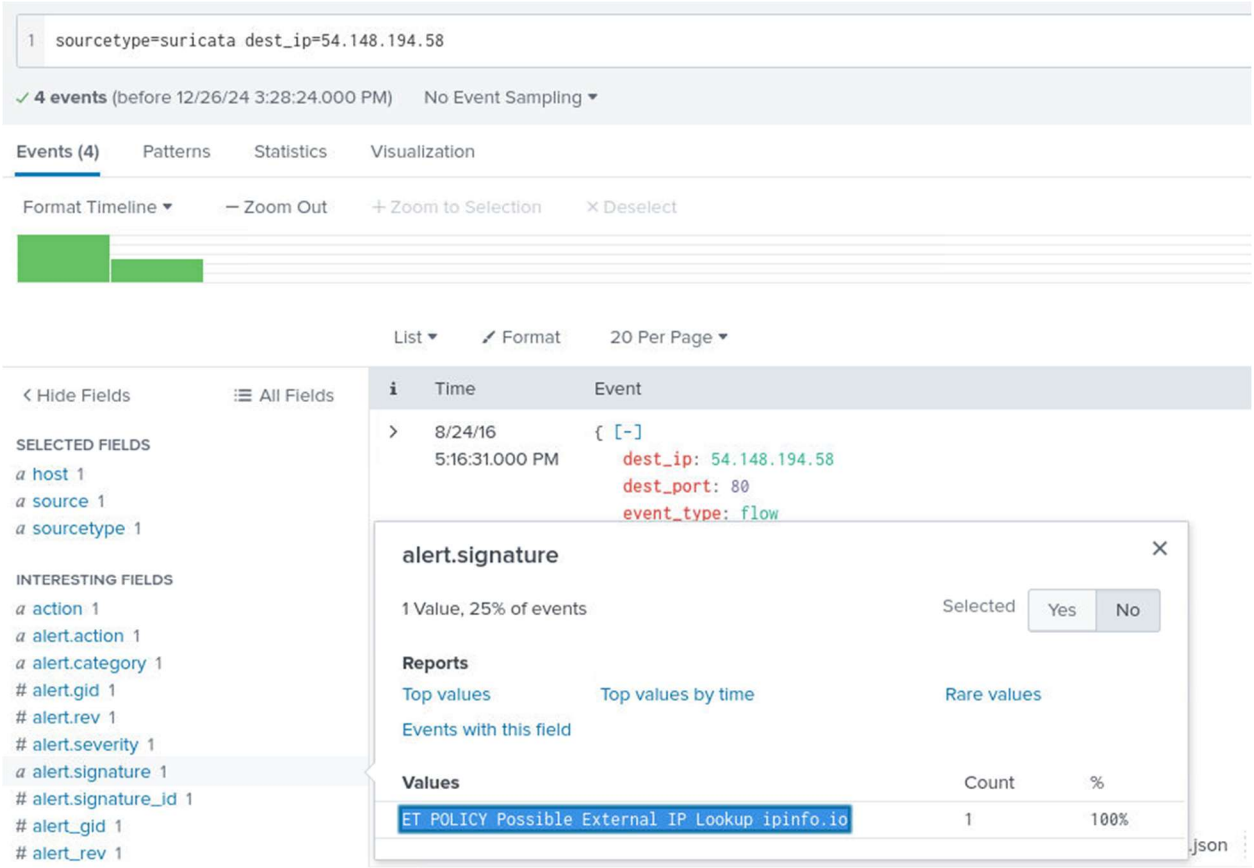
11. What is the name given to this specific malware by Fortigate?



12. Conduct another OSINT search for the name of the malware. What is the primary function of this malware? (Submit the malware category, different from Q10)



13. Finally, let's investigate the single connection from osk.exe to a remote IP address on destination port 80 HTTP. Find the IP from the Sysmon logs and use it to search in the suricata logs - these logs have different event types, and we're interested in 'alert'. If Suricata has alerted on this activity, what is the alert.signature value?
Destination IP: 54.148.194.58



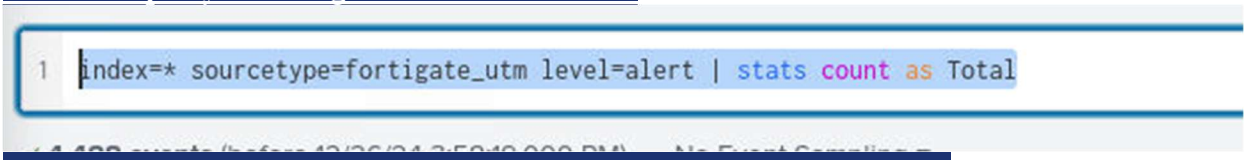
Splunk Investigation 4

PROMPT:

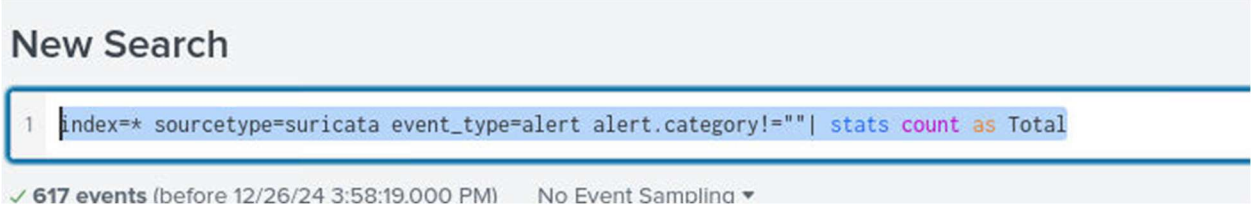
The security team has begun to create an operational dashboard within their SIEM instance to highlight important events. You've been tasked with trying it out to investigate some suspicious activity, and also add some new panels to the dashboard!

1. Click on Dashboards and go to Splunk Investigation 4. How many Suricata alerts are there, and how many Fortigate alerts are there

2. Edit the dashboard and look at the search query for the Fortigate Alerts counter. What is the full query used to generate this number?

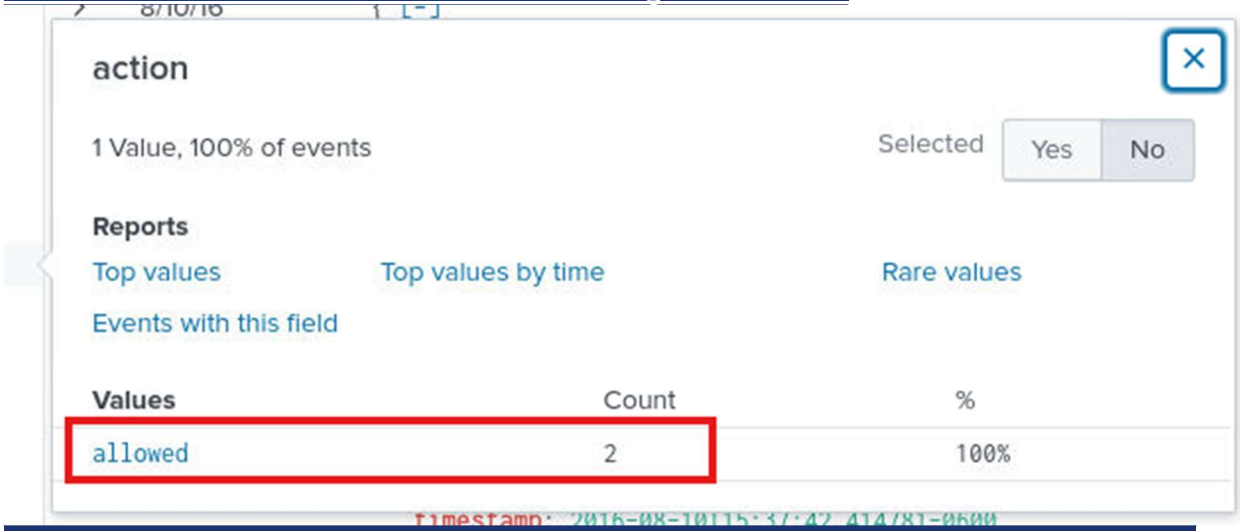


3.What is the full query used to generate the Suricata Alerts counter?

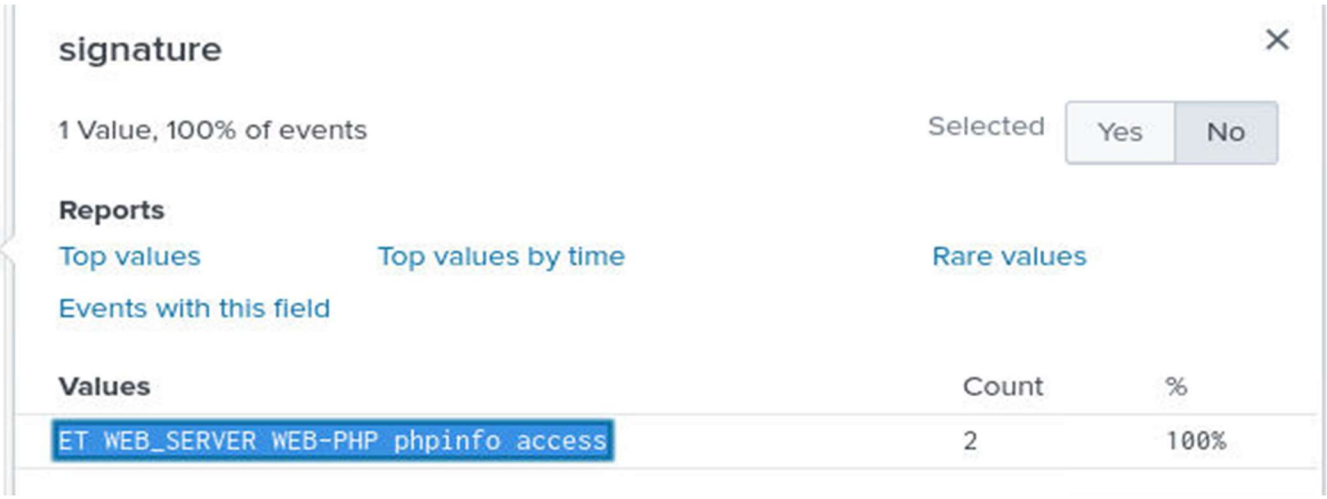


4. Click on the Suricata alert titled 'Information Leak' to see the associated events. What is the source IP address, and what is the destination IP address?

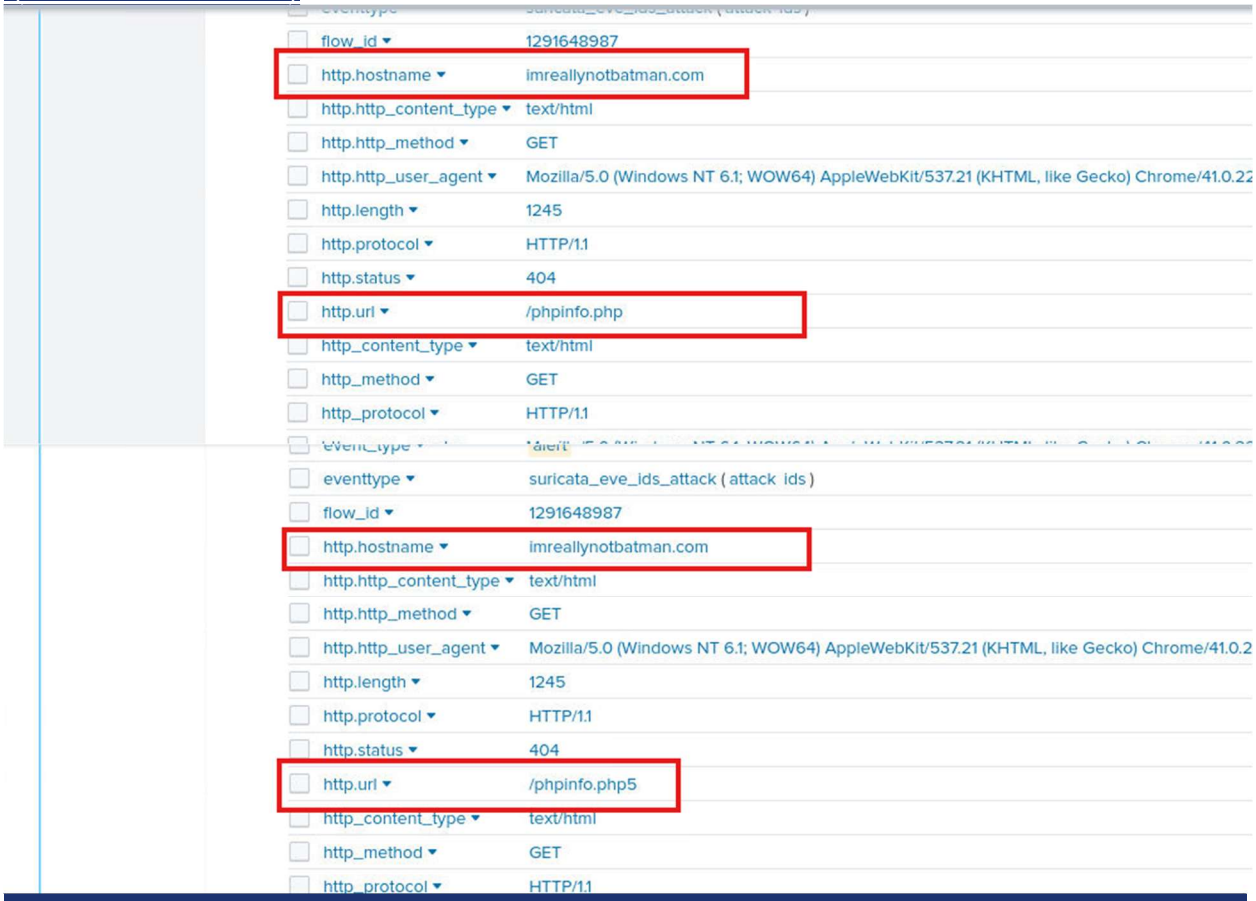
5. What action did Suricata take after observing these events?



6. We know the alert category is 'Information Leak', however the specific signature can provide us with more information about this activity. What is the signature shared by both events?

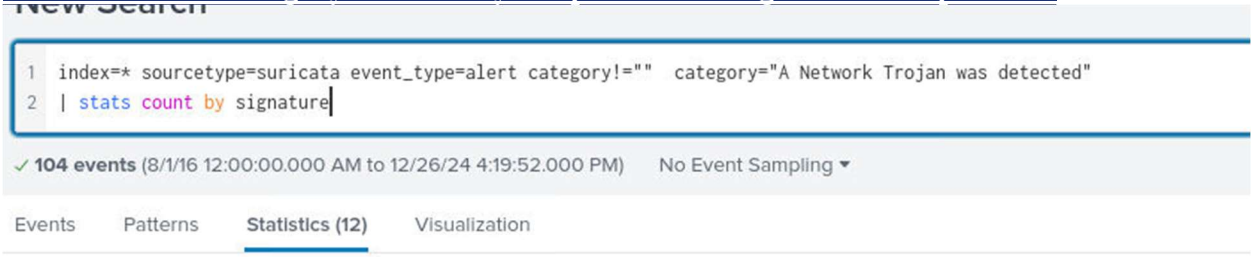


7.Based on the logs, combine two fields to understand the full website addresses being accessed by the attacker (Remember, in some logs a "/" character must be escaped by putting a "\" in front of it. You should not reference the "\") (hostname and URL)



8. What HTTP status code is returned to both of these requests, that tells us this attack was not successful?

9. Return to the Dashboard and click on the Suricata alert titled 'A Network Trojan was detected' to load this search. Modify the search query to show count of every signature field within this alert category. How many unique suricata signatures are present?



10. Search manually through Suricata logs where the HTTP status code is 200, then perform a count of each signature field to find two signatures that reference a vulnerability

CVE identifier. Search this CVE on the National Vulnerability Database.- what is the CVSS Version 3 Score?

```
1 index=* sourcetype=suricata event_type=alert category!="" status=200
2 | stats count by signature
```

✓ **193 events** (8/1/16 12:00:00.000 AM to 12/26/24 4:22:38.000 PM) No Event Sampling

Events Patterns **Statistics (15)** Visualization

20 Per Page Format Preview

signature
ET POLICY Possible External IP Lookup ipinfo.io
ET SCAN Acunetix Version 6 (Free Edition) Scan Detected
ET WEB_SERVER IIS 8.3 Filename With Wildcard (Possible File/Dir Bruteforce)
ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt
ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt
ET WEB_SERVER Possible CVE-2014-6271 Attempt
ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access
ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM
ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
ET WEB_SERVER Possible SQLi Attempt in User Agent (Inbound)
ET WEB_SERVER SQL Injection Select Sleep Time Delay

issue affects Lockech. before 15.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information c

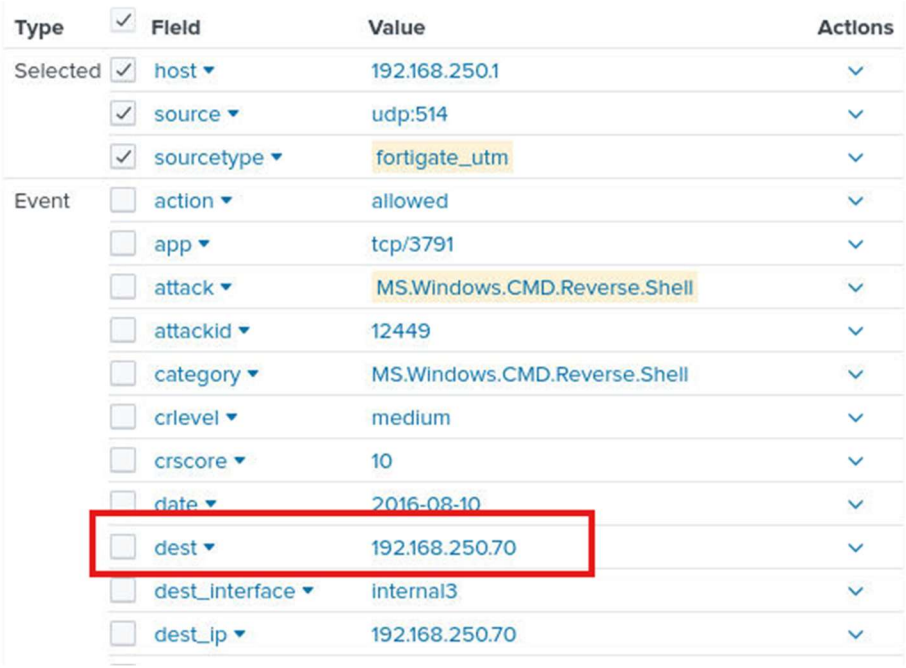
CVSS 3.x Severity and Vector Strings:

CNA: Computer Emergency Response Team of the Republic of Turkey

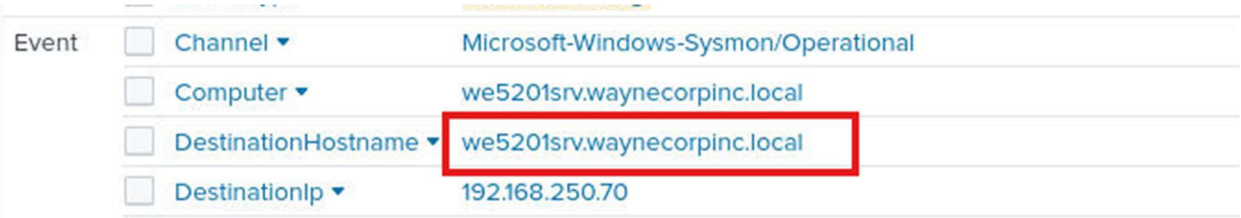
Base Score: 9.8 CRITICAL

Vector: CVSS:3.1/AV:N

11. On the Fortigate Security Alerts dashboard table click on 'MS.Windows.CMD.Reverse.Shell'. Identify the internal IP within this event, and use your SIEM skills to identify the name of this system.

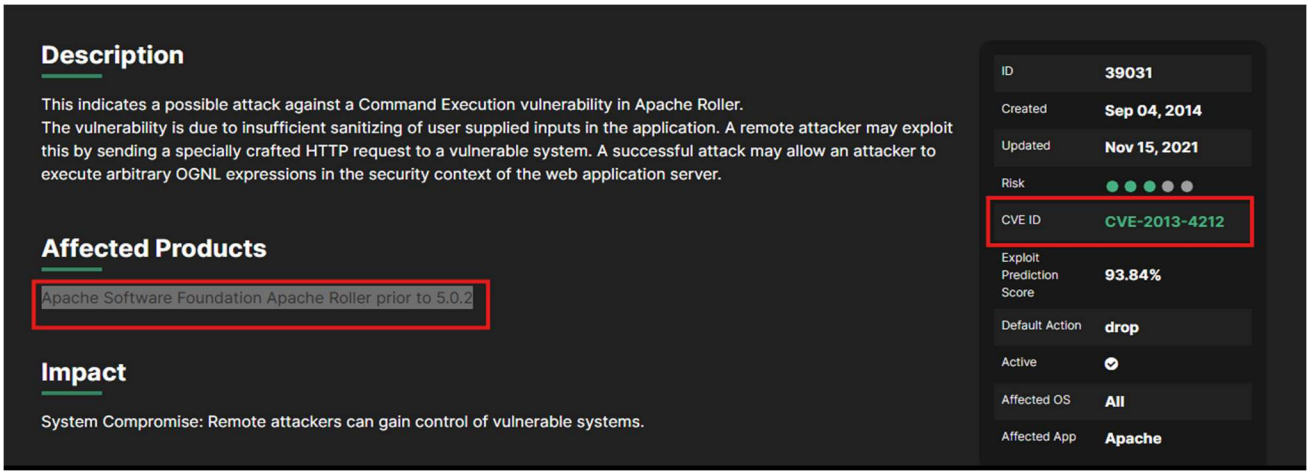


Type	Field	Value	Actions
Selected	host	192.168.250.1	
	source	udp:514	
	sourcetype	fortigate_utm	
Event	action	allowed	
	app	tcp/3791	
	attack	MS.Windows.CMD.Reverse.Shell	
	attackid	12449	
	category	MS.Windows.CMD.Reverse.Shell	
	crlevel	medium	
	crscore	10	
	date	2016-08-10	
	dest	192.168.250.70	
	dest_interface	internal3	
	dest_ip	192.168.250.70	



Event	Channel	Microsoft-Windows-Sysmon/Operational
	Computer	we5201srv.waynecorpinc.local
	DestinationHostname	we5201srv.waynecorpinc.local
	DestinationIp	192.168.250.70

12. Go back to the Fortigate Security Events table and click on 'Apache.Roller.OGNL.Injection.Remote.Code.Execution'. Find the reference field in the log and open the URL on your host machine. What is the Affected Products text, and the CVE identifier?



13. On the dashboard consider the Fortigate category with the highest number of events. Try to find the version of the scanning tool being used, looking at Fortigate logs then Suricata logs.
Had to go to Suricata and search Acunetix