

Part 1: Windows Server Attack

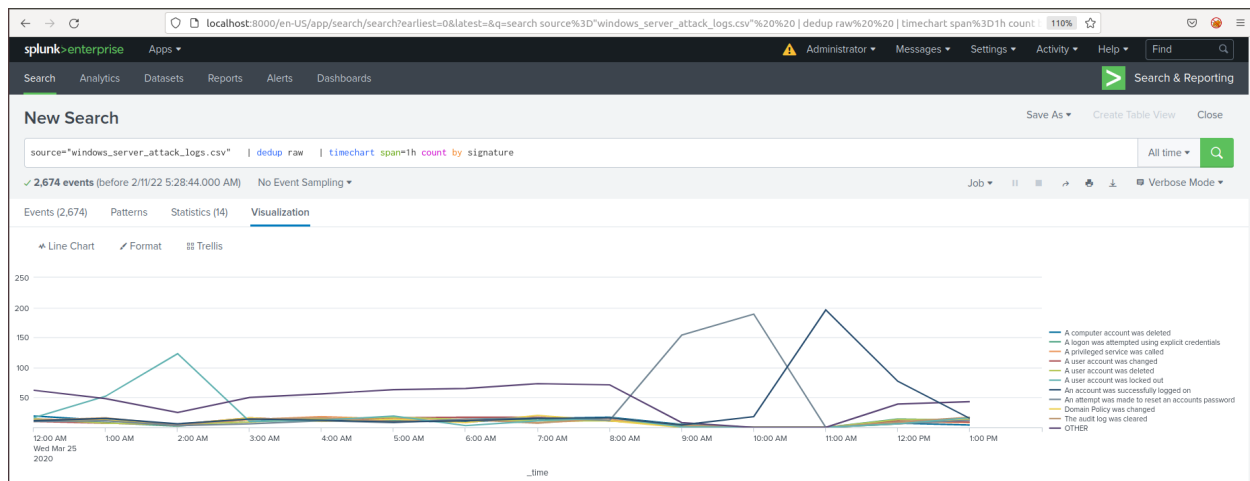
Note: This is a public-facing windows server that VSI employees access.

Question 1

- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.

Global solution:

The best overall (global) mitigation strategies are to secure individual user accounts across company systems. Implementing multi-factor authentication is a company-wide safety implementation that can reduce the chances of success for an attacker, especially on user accounts.



Individual solutions for specific users:

- **User_J: An Account was successfully logged on**
 - The log for this user shows that the attacker was successful in obtaining the user's password
 - An admin can easily change the password for the User_J
 - User specific alerts can also be made to monitor uncharacteristic activity more closely.

The screenshot shows a Splunk Enterprise search interface. The search bar contains the query: `source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | top limit=10 user`. The results show 273 events. The 'Statistics' tab is selected, displaying a table with columns: user, count, and percent.

user	count	percent
user_j	271	99.267399
user_n	1	0.366300
user_k	1	0.366300

- **User_A: A user account was locked out**
 - This user was subject to a successful brute force attack. This user should change their passwords immediately and increase the complexity to mitigate brute-force attacks.

The screenshot shows a Splunk Enterprise search interface. The search bar contains the query: `source="windows_server_attack_logs.csv" signature="A user account was locked out" | top limit=10 user`. The results show 1,701 events. The 'Statistics' tab is selected, displaying a table with columns: user, count, and percent.

user	count	percent
user_a	1686	99.118166
user_k	3	0.176367
user_b	3	0.176367
user_e	2	0.117578
user_n	1	0.058789
user_l	1	0.058789
user_j	1	0.058789
user_i	1	0.058789
user_h	1	0.058789
user_f	1	0.058789

- **User_K: An attempt was made to reset an account password**
 - Logs do not show evidence of a successful login into this user's account or to successfully reset the password
 - User specific alerts can be employed here as well to analyze users password changes and the frequency at which they occur

The screenshot shows a Splunk Enterprise search interface. The search bar contains the query: `source="windows_server_attack_logs.csv" signature="An attempt was made to reset an accounts password" | top limit=10 user`. The results show 2,019 events. The 'Statistics' tab is selected, displaying a table with columns: user, count, and percent.

user	count	percent
user_k	2016	99.851412
user_c	3	0.148588

- The remaining users had accounts created or changed

Question 2

- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

One solution to this would be to add a group policy to unlock user accounts after a certain period of time so that users could access their own accounts again. Employees should also be educated and taught to be vigilant regarding who they accept or send information to and what type of information is being sent.

Part 2: Apache Webserver Attack:

Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
 - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screenshot of the geographic map that justifies why you created this rule.

According to the the data, it appears that Ukraine was the source of most of the attacks. It would be prudent to set a firewall rule to block incoming HTTP traffic coming from Ukraine.

The Firewall Rule: **"Block all incoming HTTP traffic of source IP's coming from country Ukraine"**

Country



60 Values, 100% of events

Selected

Yes

No

Reports

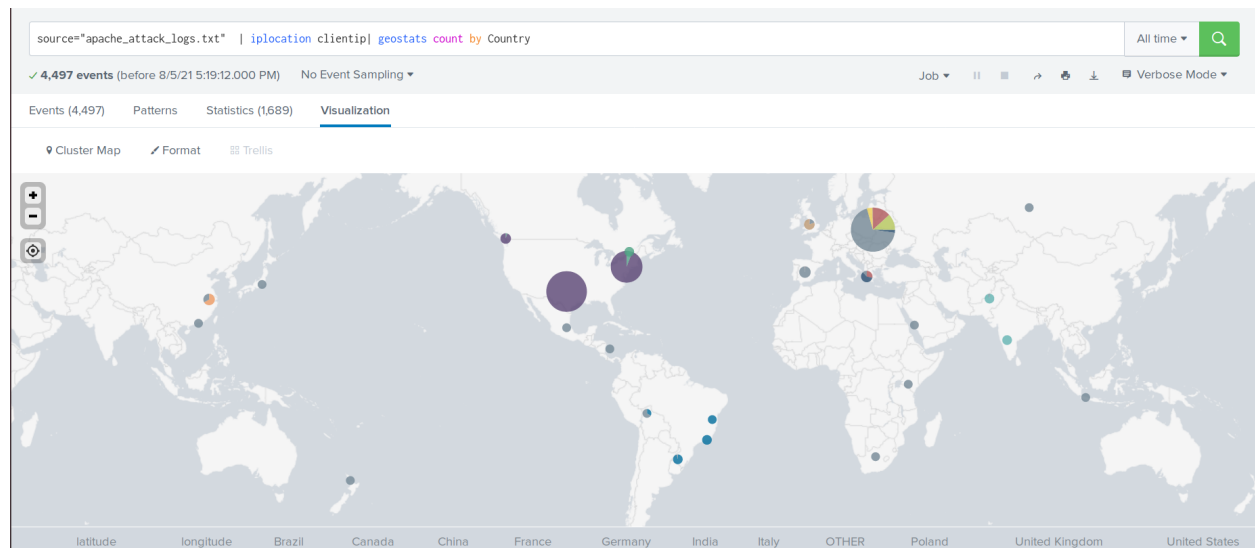
Top values

Top values by time

Rare values

Events with this field

Top 10 Values	Count	%	
United States	2,027	45.074%	
Ukraine	877	19.502%	
France	195	4.336%	
Sweden	192	4.27%	
Germany	154	3.424%	
Spain	108	2.402%	
Canada	82	1.823%	
Italy	77	1.712%	
United Kingdom	69	1.534%	
Brazil	67	1.49%	



Question 2

- VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.
- What other rules can you create to protect VSI from attacks against your webserver?
 - Conceive of two more rules in "plain english".
 - Hint: Look for other fields that indicate the attacker.

If the IP is changed, then subsequent rules can be based of the fields of “user_agent” and “bytes”. If “user_agent” is used look for *“Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1).”* If “bytes” is used look for the byte amount of 65748

You can write the firewall rules as such:

- “Block all incoming HTTP traffic if user_agent is *“Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1).”*”
- “Block all incoming HTTP traffic is bytes amount is 65748.”

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search bar contains the query: `source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States" | top limit=10 Country`. Below the search bar, it shows '2,470 events' for the time range '3/25/20 12:00:00.000 AM to 3/26/20 12:00:00.000 AM'. The results are displayed in a table with columns 'Country', 'count', and 'percent'.

Country	count	percent
Ukraine	877	35.506073
France	195	7.894737
Sweden	192	7.773279
Germany	154	6.234818
Spain	108	4.372470
Canada	82	3.319838
Italy	77	3.117409
United Kingdom	69	2.793522
Brazil	67	2.712551
China	64	2.591093