Part 1: Windows Server Attack

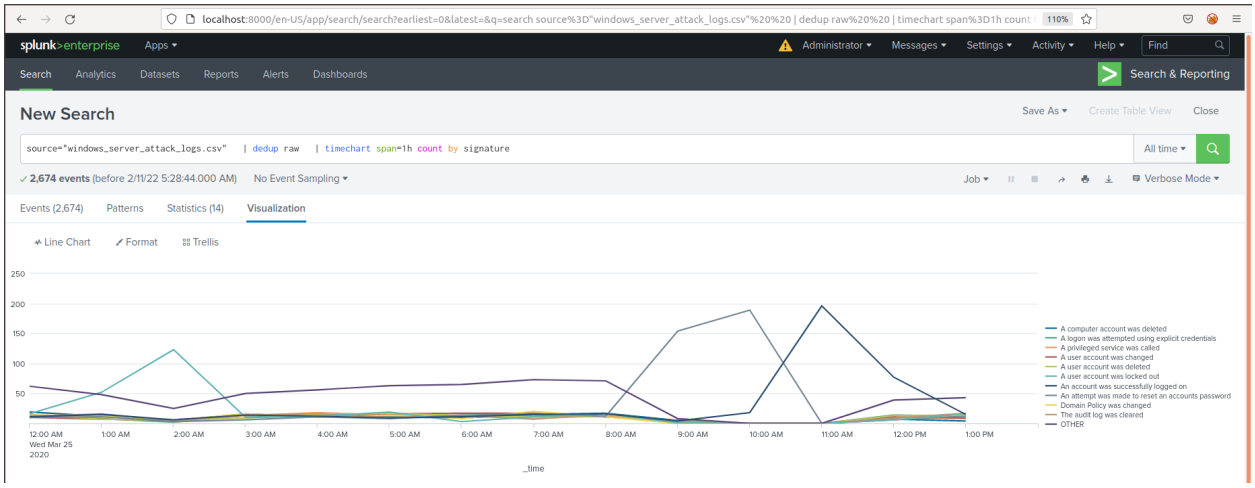
Note: This is a public-facing windows server that VSI employees access.

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.

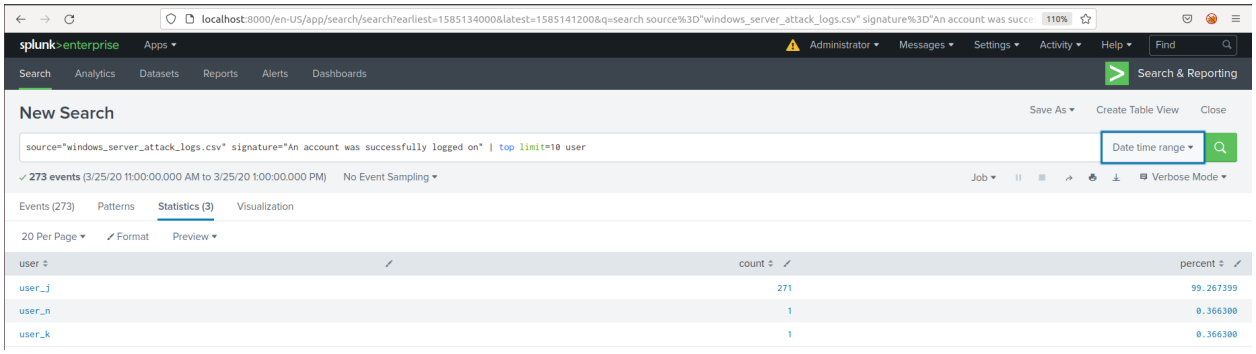
Global solution:

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.

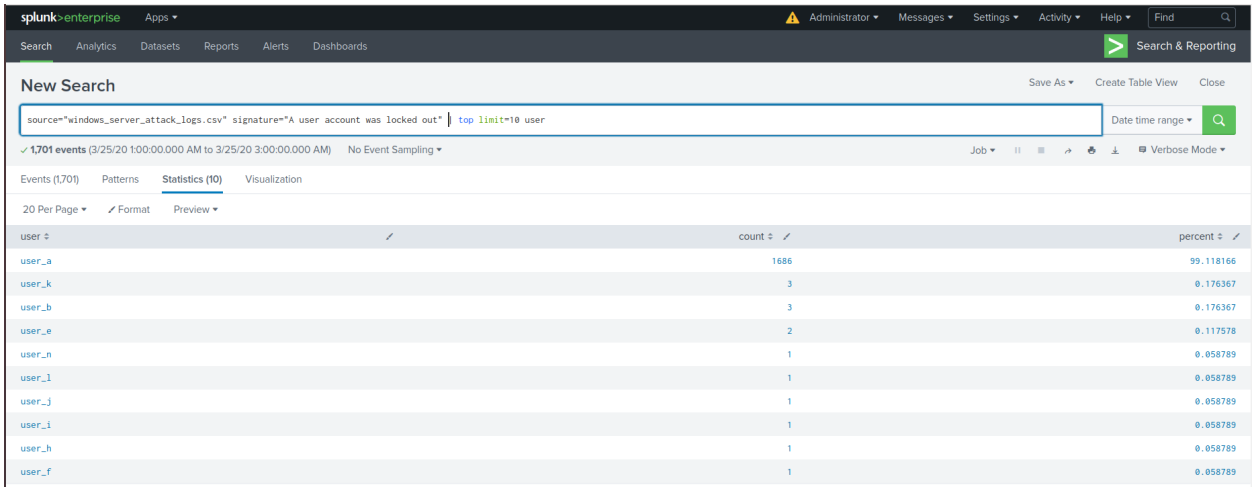


Individual solutions for specific users:

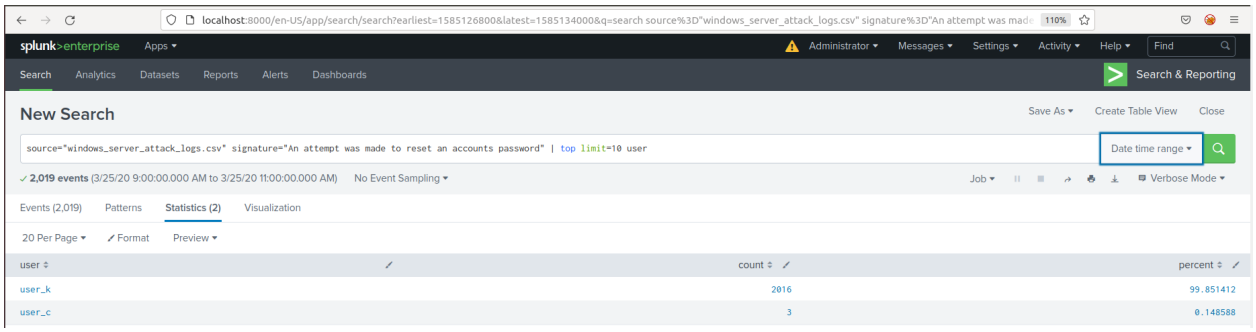
- User_J: *An Account was successfully logged on*
  - The log for this user shows that the attacker was successful in obtaining the user's password
  - An admin can easily change the password for the User_J
  - User specific alerts can also be made to monitor uncharacteristic activity more closely.



- 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.



- 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 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

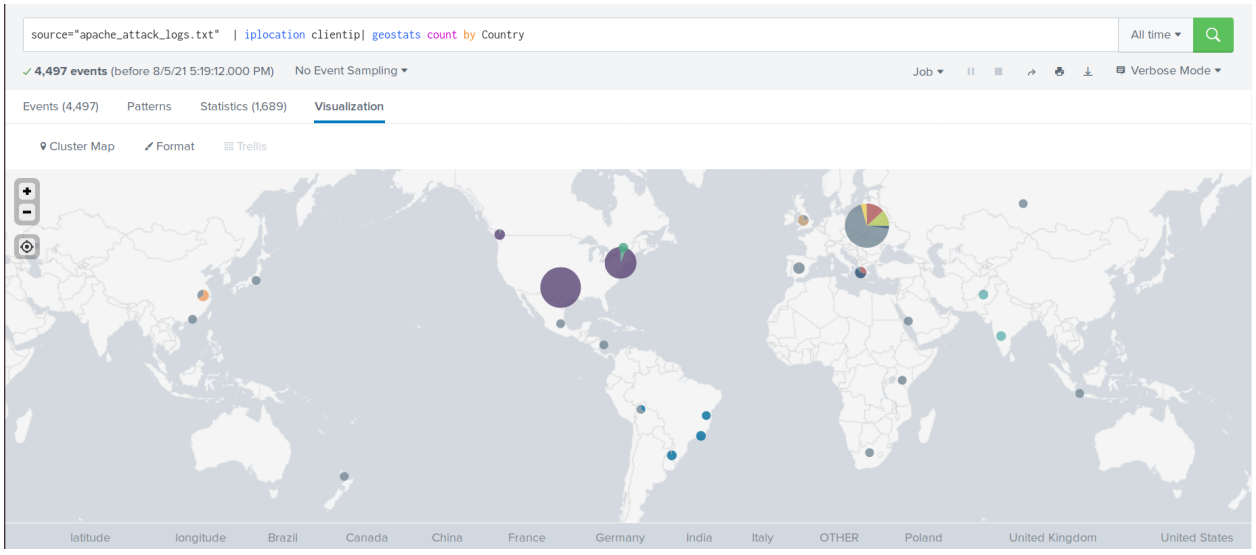
Selected: Yes / No

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.”*