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.

To try and protect users overall, enacting a policy of 2 factor authentication could help mitigate potential for attacks such as the type that occurred. This 2 factor authentication could also be required to even send the reset password command to prevent a flood of reset password requests as happened in the attack. Making sure individuals have strong passwords to prevent potential brute force attacks would be an effective method as well. A company-wide training on social engineering and the risks of giving away information about one's company account to unknown or suspicious parties could also help mitigate risk.

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?

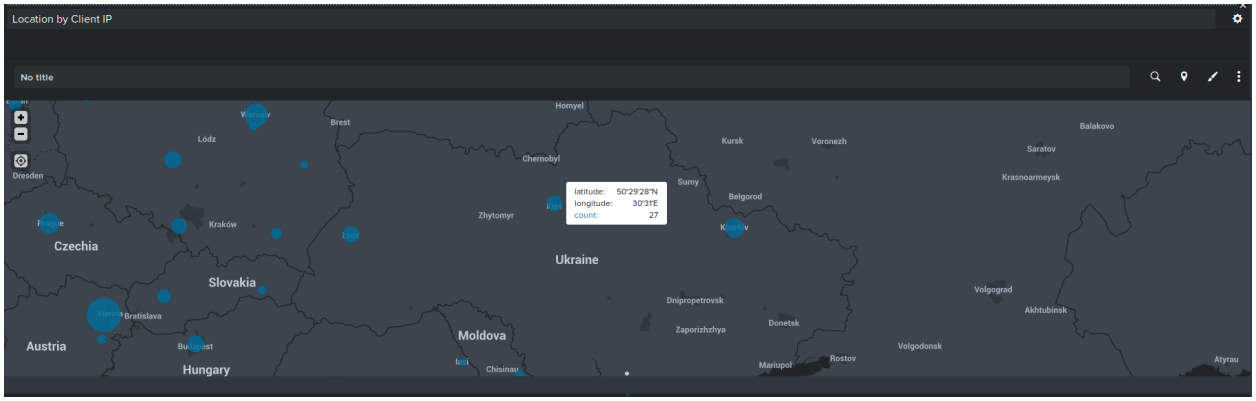
There are several ways to try and mitigate this attack. Locking out users after a certain number of attempts is good to stop a brute force attack but as we see from this attack that method can be used to lock out a mass of users quickly and easily. One method of mitigation is to only accept log-in attempts from a known device or IP for a specific account, that way if log-in attempts are made from another unknown device that device could be locked out but the actual owner of the account would still be able to log-in. Another method is to have a specific security image associated with an account, so say Account A's security image is a lamp. That user will know if he goes to log in and the image is not a lamp that he needs to find his security image. The hacker wouldnt know and many attempts on the wrong image could lock out that account but logging on with the correct image could still work.

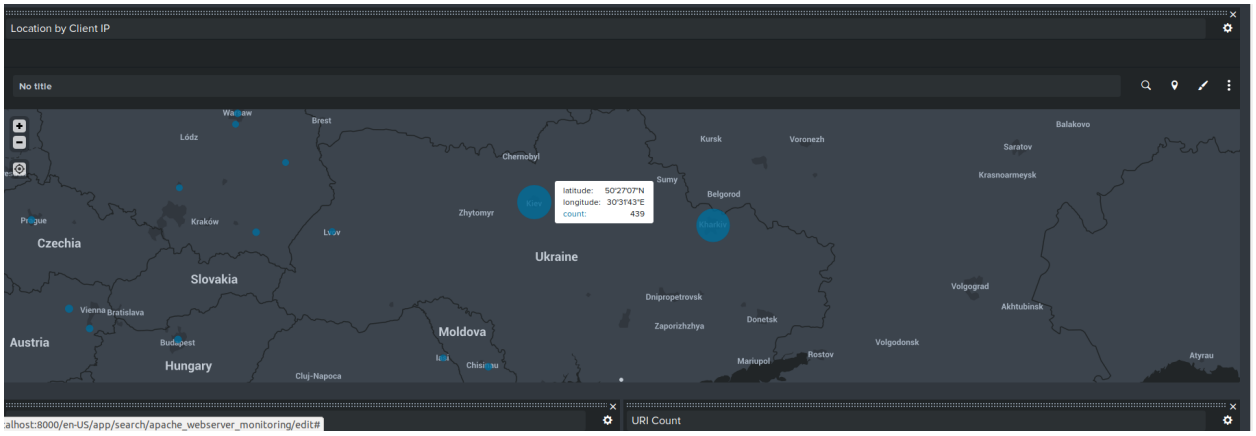
Part 2: Apache Webserver Attack:

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 screen shot of the geographic map that justifies why you created this rule.

I would recommend either blocking all incoming traffic from Ukraine or very closely monitoring and potentially filtering out some traffic from Ukraine. As shown in the screenshots below the activity from Ukraine ballooned after the attack, which means that most of the traffic came from that area. It would be a good idea to get a handle of the traffic from Ukraine to prevent the same thing from happening again.





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".

There are a few things to try and prevent a similar attack. One way is that the attacker used the same user agent to conduct the attack. Watching closely for/blocking traffic from that particular user agent could help prevent the attack. They also targeted the account logon page for the attack so making a rule that limits the amount of traffic to that page within a particular time limit could also help prevent the attack, especially considering the traffic to the log-on page went from 100 to over 1200 there is a threshold that could be established to alert and shut down traffic after a certain amount.