Protecting VSI From Future Attacks

Windows Server Attack

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.***

One mitigation strategy would be to only allow connections from trusted sources or only accept domestic connections filtering out any foreign connections.

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?***

To protect users from getting completely locked out, some mitigation strategies are:

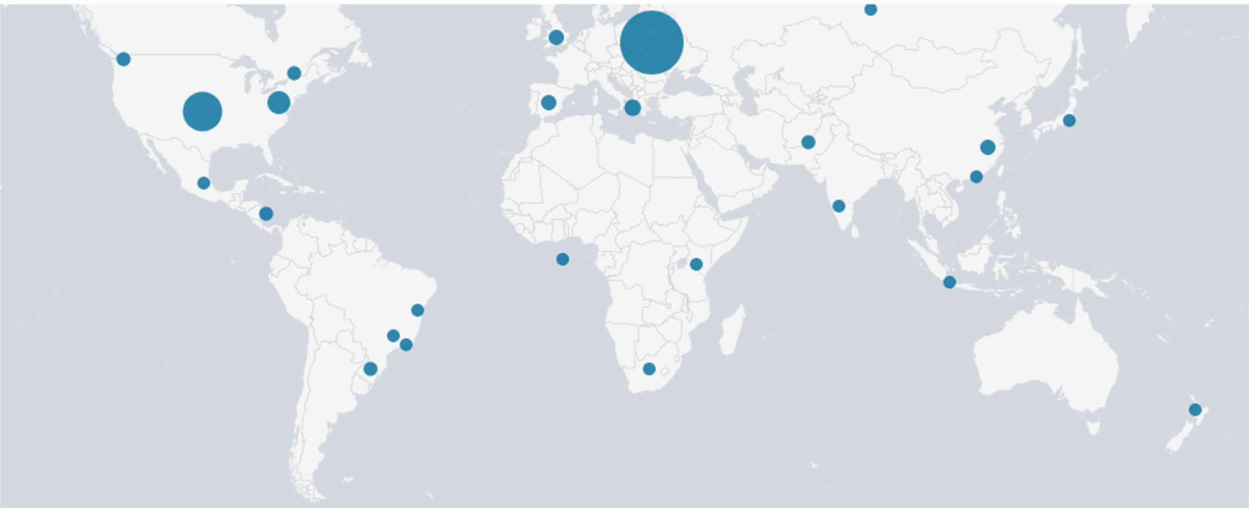
- Utilize multi-factor authentication (MFA).
- Notify users that "several login attempts were made, and the account has been locked. Contact support or reset password" in order to unlock the account.
- Set time constraints on how long the account is locked for. (i.e., account locked for 1 hour).

Apache Web Server 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***

Block all incoming foreign traffic since a significant amount of this traffic is outside of the United States.



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?***

Additional rules that can be created are to circumvent these attacks are:

- A special rule can be created which can block all incoming traffic with bytes over the 6000 threshold.
- Consult and specify server security and protection settings.