### **C Spencer**

HW 19

2/2/2021

### 

### **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.

Whitelisting of certain users based on their source IP addresses could serve as a global mitigation

User Specific Mitigations

* User\_a - User account was locked out
  + This is indicative of a brute force attack and failing to guess the password results in the account being locked.
  + This user should change their password to something that is securely long and complex to ensure their account is robust against brute force attacks.
* User\_k - account password reset attempts
  + There were attempts made to reset user\_k’s password but they were not successful.
  + Setting up alerts with a lower thresholds could provide early warning if similar attacks happen again.
* User\_j - successful log on
  + It appears the hacker was able to obtain or guess the correct password for user\_j.
  + User\_j should change their password and lower thresholds could be applied to user\_j’s account to provide early warning unauthorized log in attempts happen again.

#### **Question 2**

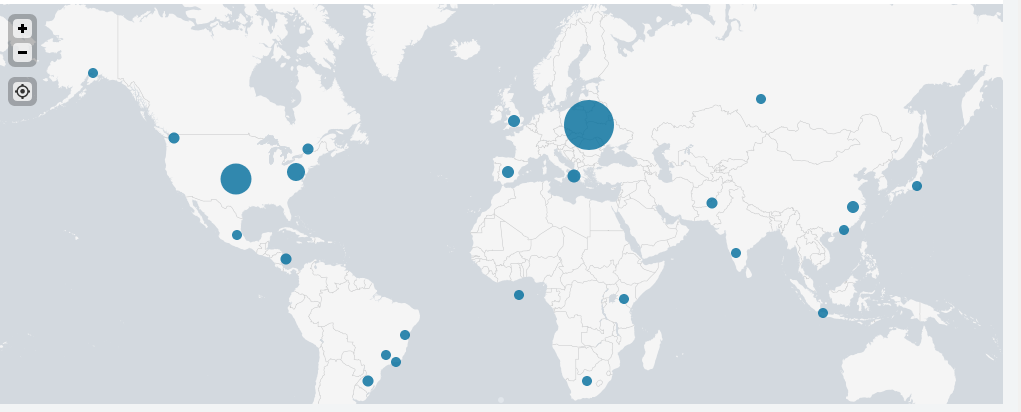
* VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
* What sort of mitigation could you use to protect against this?

The best mitigation would be to use time-based lockouts to thwart attempts to lock a user’s account while allowing users to access their accounts again once a certain amount of time has passed to make it safe to do so.

### **Part 2: Apache Webserver Attack:**

#### **Question 1**

* Based on the geographic map, recommend a firewall rule that the networking team should implement.
  + Block incoming HTTP traffic with an origin of Ukraine





#### 

#### 

#### **Question 2**

* VSI has insider information that JobeCorp will launch the same web server 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?  
  + Block incoming HTTP traffic for usergeant Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
  + Block incoming traffic with bytes greater than 60000

