### **Part 1: Windows Server Attack**

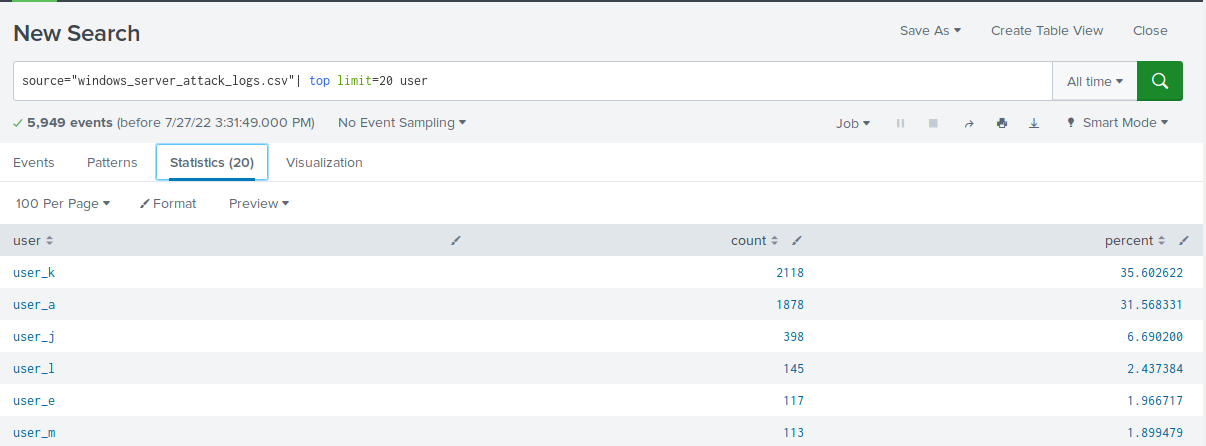
Note: This is a public-facing windows server that VSI employees access.

#### **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.

* Answer: **Based on the screenshots below, users k, a, and j appear to be the most impacted. User\_k had an excessive amount of attempted password resets, user\_a had an excessive amount of account lockouts, and user\_j had a relatively high amount of logins compared to other users. Global mitigation strategies should include implementing complex password policies, as well as limits before account lockouts. Multi-factor authentication should also be implemented for both increased security as well as an early warning system. For each of the users impacted by the attack, passwords should immediately be changed to something more complicated, impose lower limits for attempted logins before lockout, and implement multi-factor authentication.**









#### **Question 2**

VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.

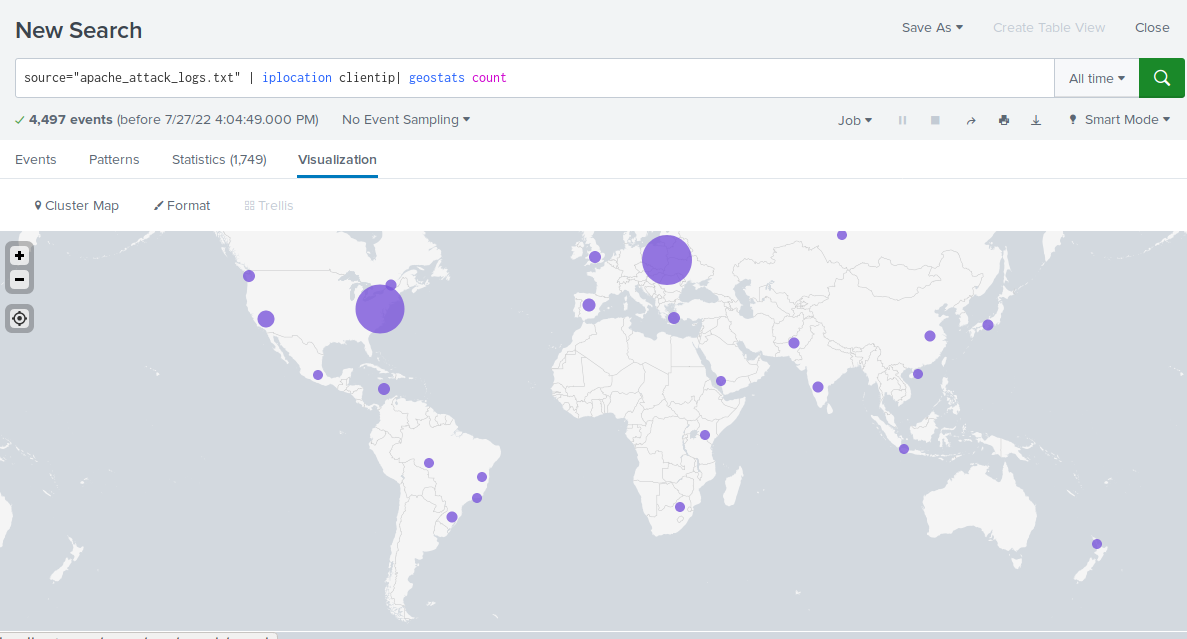
What sort of mitigation could you use to protect against this?

* Answer: **I would ensure all employees are properly trained in avoiding phishing attacks and clicking unknown links.**

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

#### **Question 1**

* Based on the geographic map, recommend a firewall rule that the networking team should implement.
  + Answer: **Since most of the attacks originated from Ukraine, I would implement a firewall rule to block traffic from that region**
* Provide a "plain English" description of the rule.
  + Answer: **Block all incoming HTTP traffic where the source IP comes from Ukraine**
* Provide a screen shot of the geographic map that justifies why you created this rule.



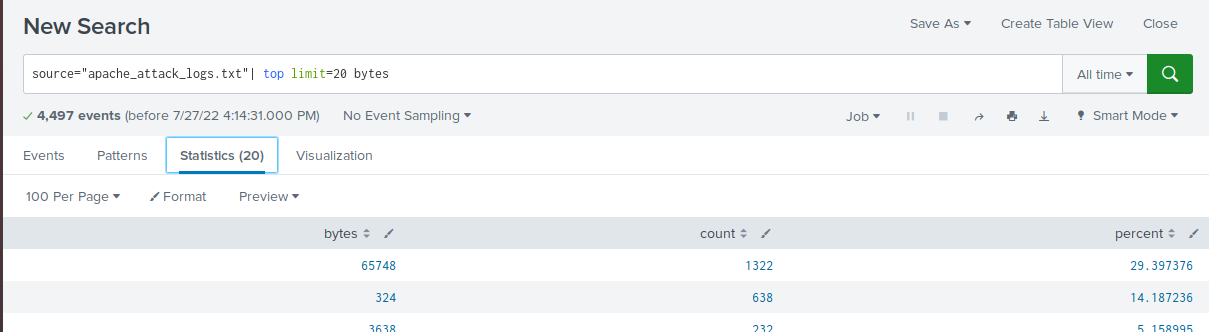
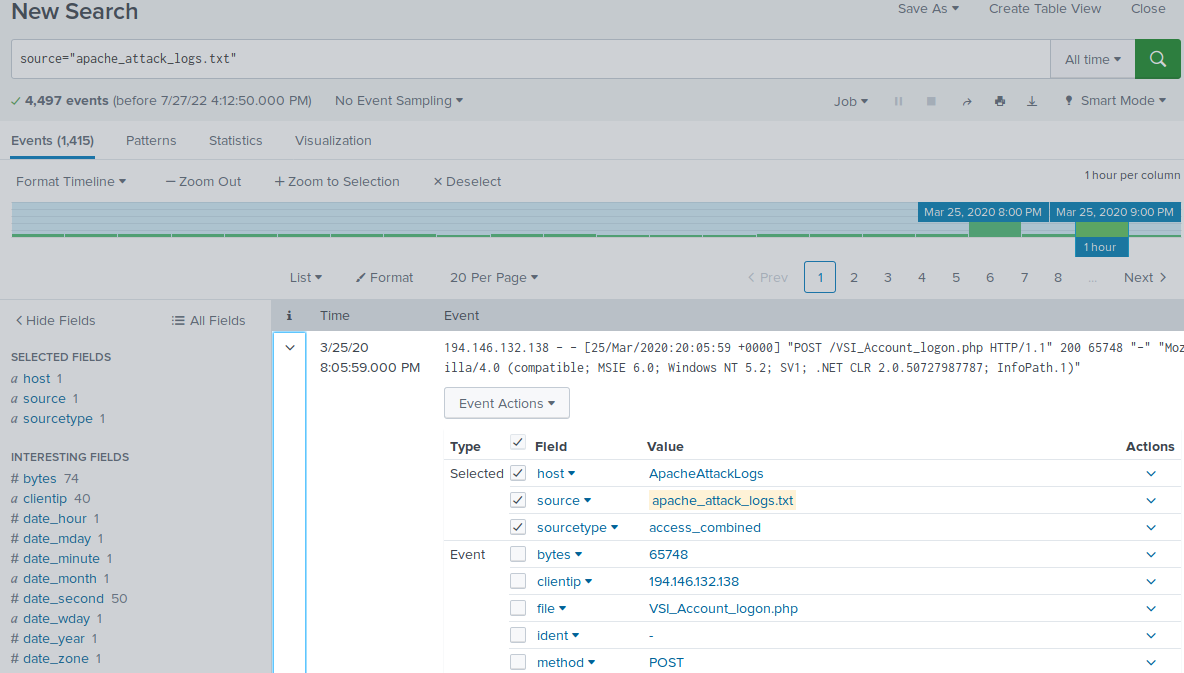
#### **Question 2**

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?

Answer:

* **Block all incoming HTTP traffic where the useragent 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 where the bytes amount is 65748**





****

### 