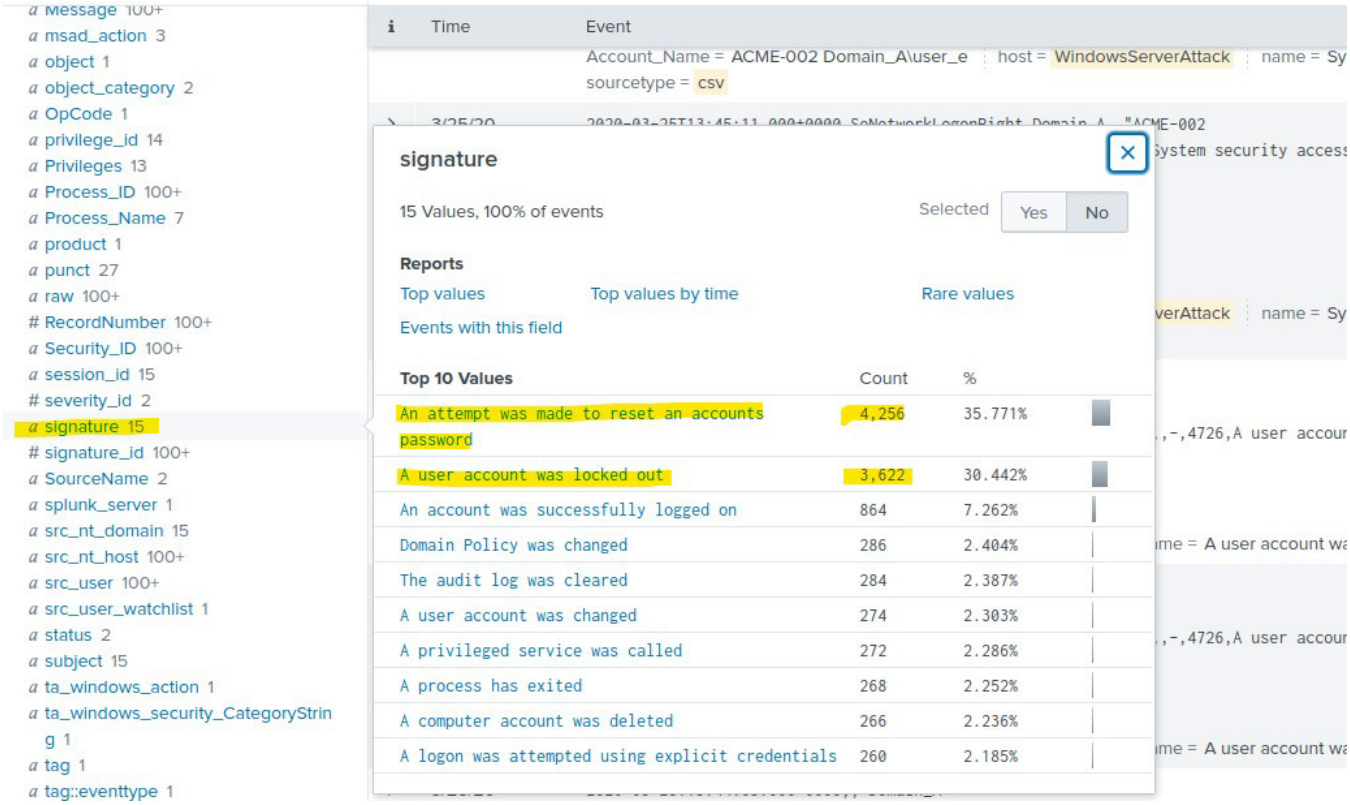
Protecting VSI From Future Attacks

Part 1: Windows Server Attack



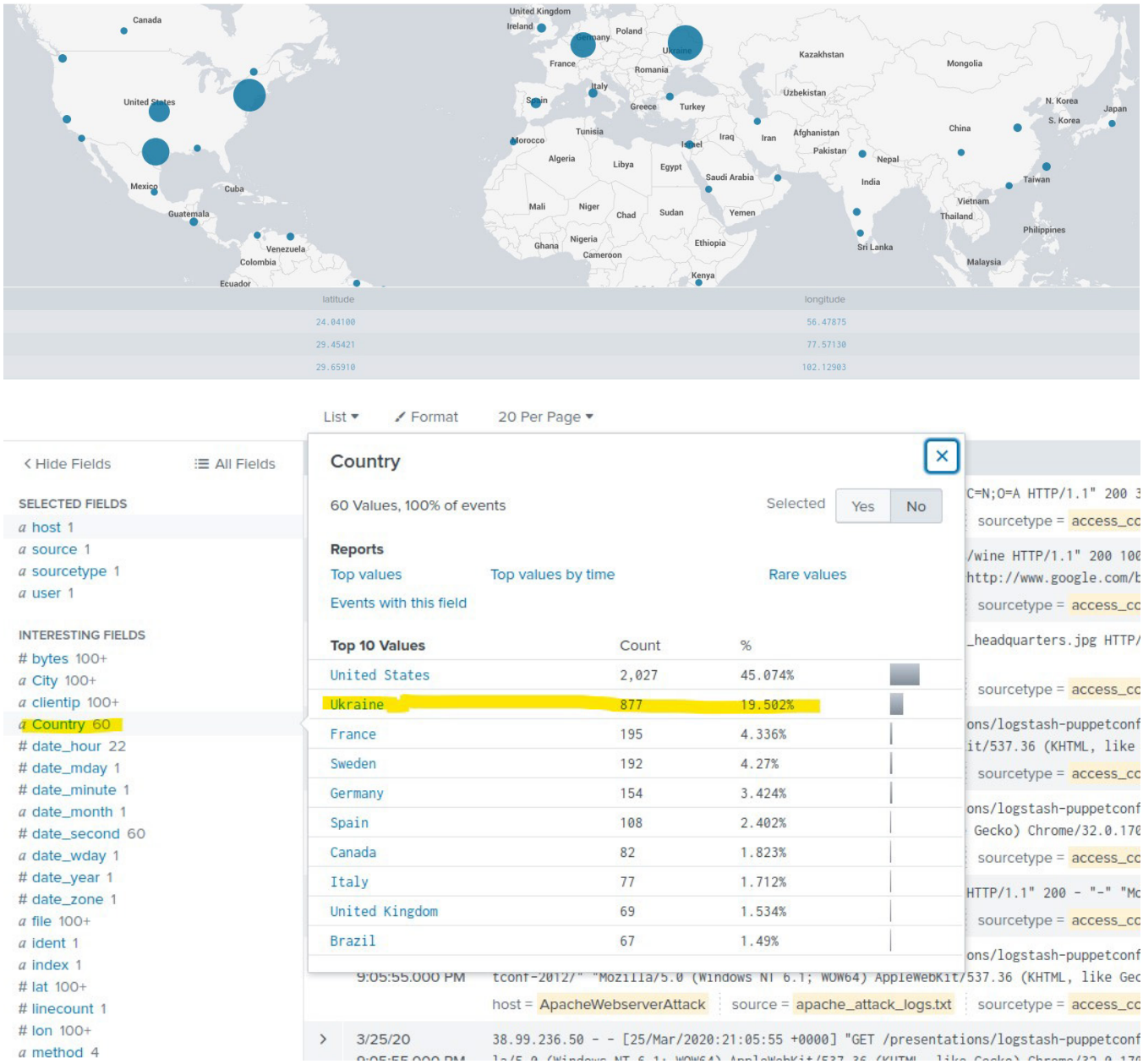
Question 1: One of the primary ways to prevent brute force attacks, or high number of account login attempts, with an end result of also locking out user accounts is to implement 2-factor/ multi-factor authentication as part of the login process. This will slow down the automated or brute force login actions that could cause lock outs to happen.

The other attack signature indicating a high level of account password reset attempts can be mitigated by prompting the user to manually type out the email address associated to the account in order to do a reset, and if the email is correct, a password reset link will be sent to the email on file. The confirmation page should be vague in confirming if the email is correct by showing the same message to the user whether the correct email was typed in or not.

Another thing to implement to the whole company as well is to require regularly scheduled password changes so that even if a password is compromised without knowledge, the duration that it is still applicable will be limited. Mandatory password changes can also be required to a specific user after such attacks occur and a successful login was made for a specific user.

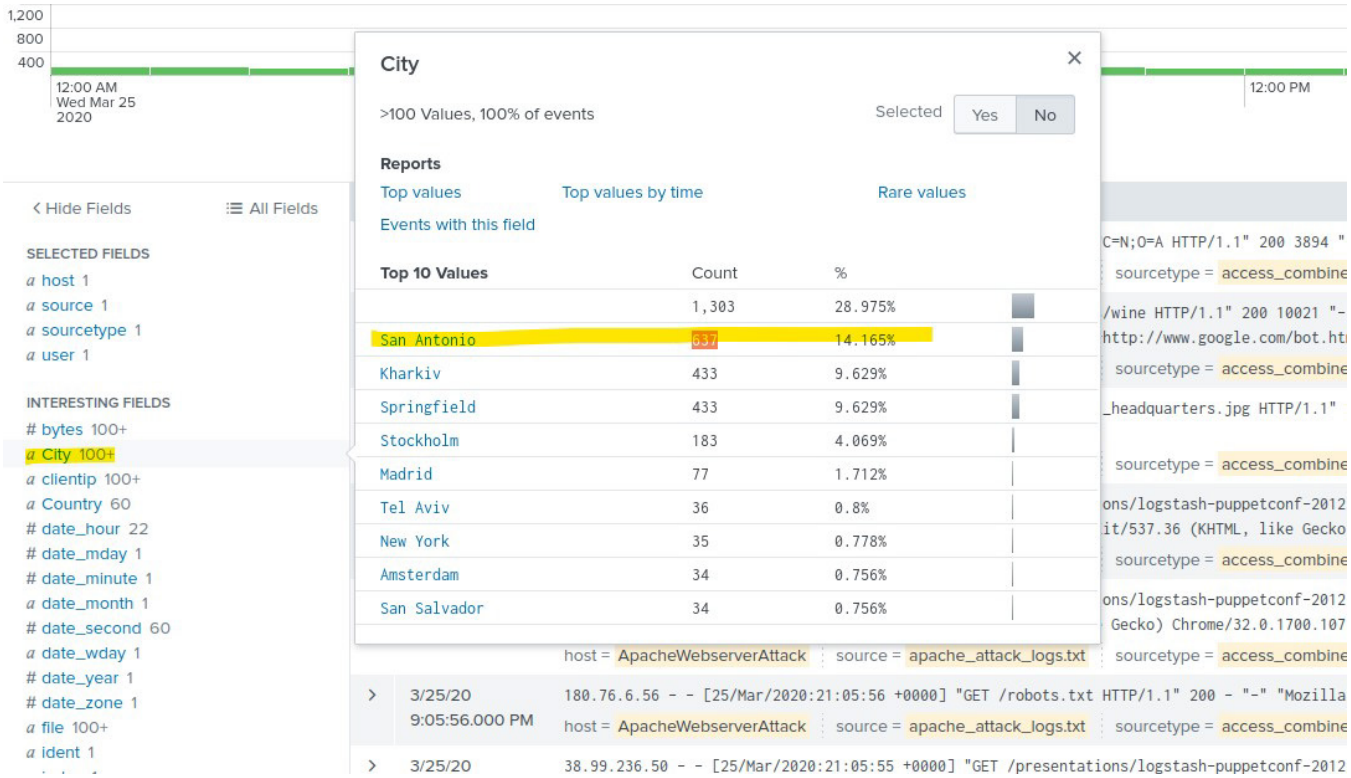
Question 2: For VSI to protect against JobeCorp or another bad actor from trying to lock out every user, CAPTCHAs can also be implemented in addition to the above policies and mitigations so that locking any accounts is a highly time-consuming and laborous task. If anyone does try to persistently attempt any accounts to do a lock out, accounts should also be set to lock only for a set limited amount of time, for example 5-10 minutes, per lockout period before returning to normal, or incrementally time-out for longer and longer durations to not make sense to persist, yet allow the real user to login regularly at a later time.

Part 2: Apache Webserver Attack



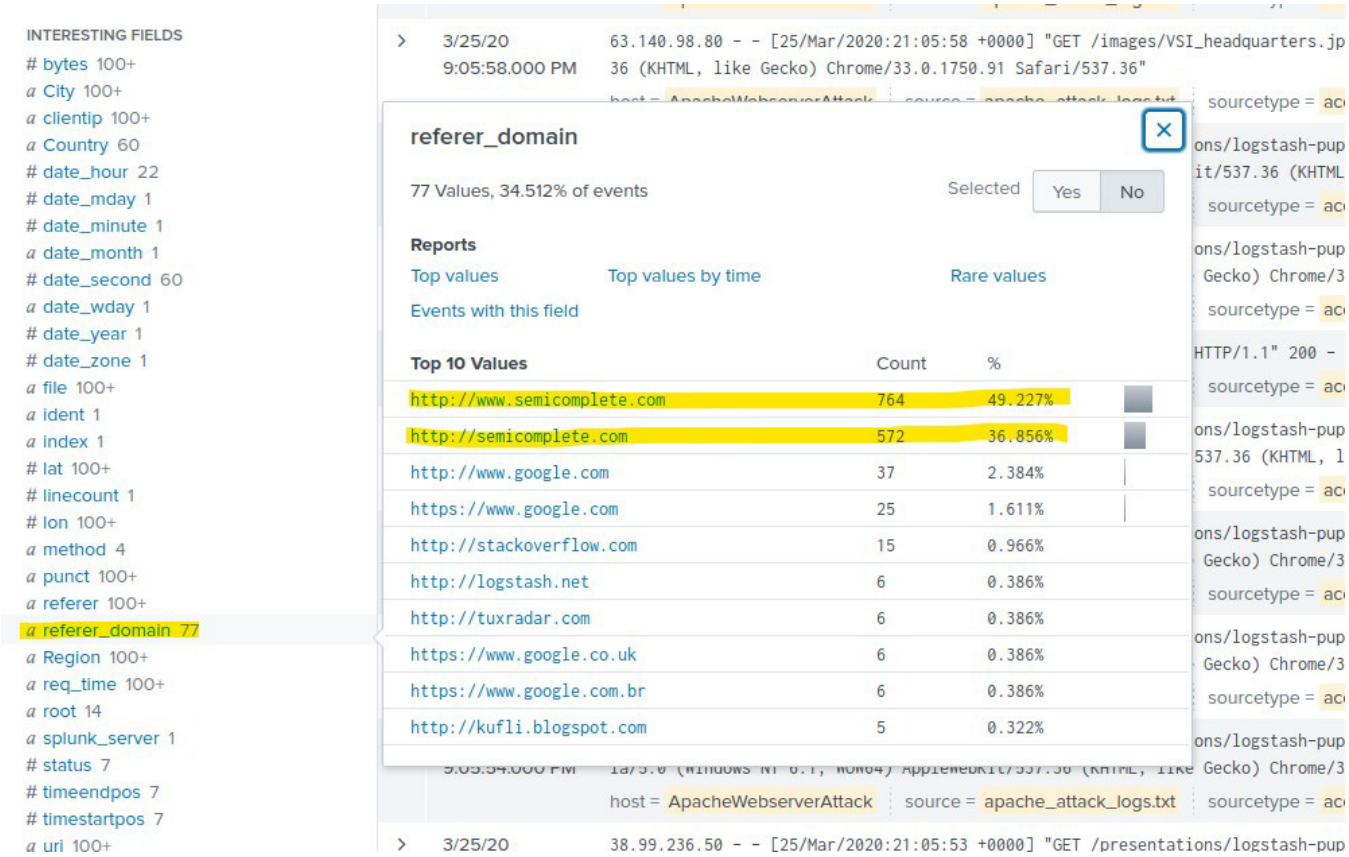
Question 1: One of the countries that has a high concentration of attacks originating is Ukraine. As a result, we will implement a firewall rule to block all traffic from them.

"Block all incoming HTTP traffic where the source IP comes from the country Ukraine"



There is also a lot of activity from specific cities where VSI does not do business, so these attacks are also safe to block.

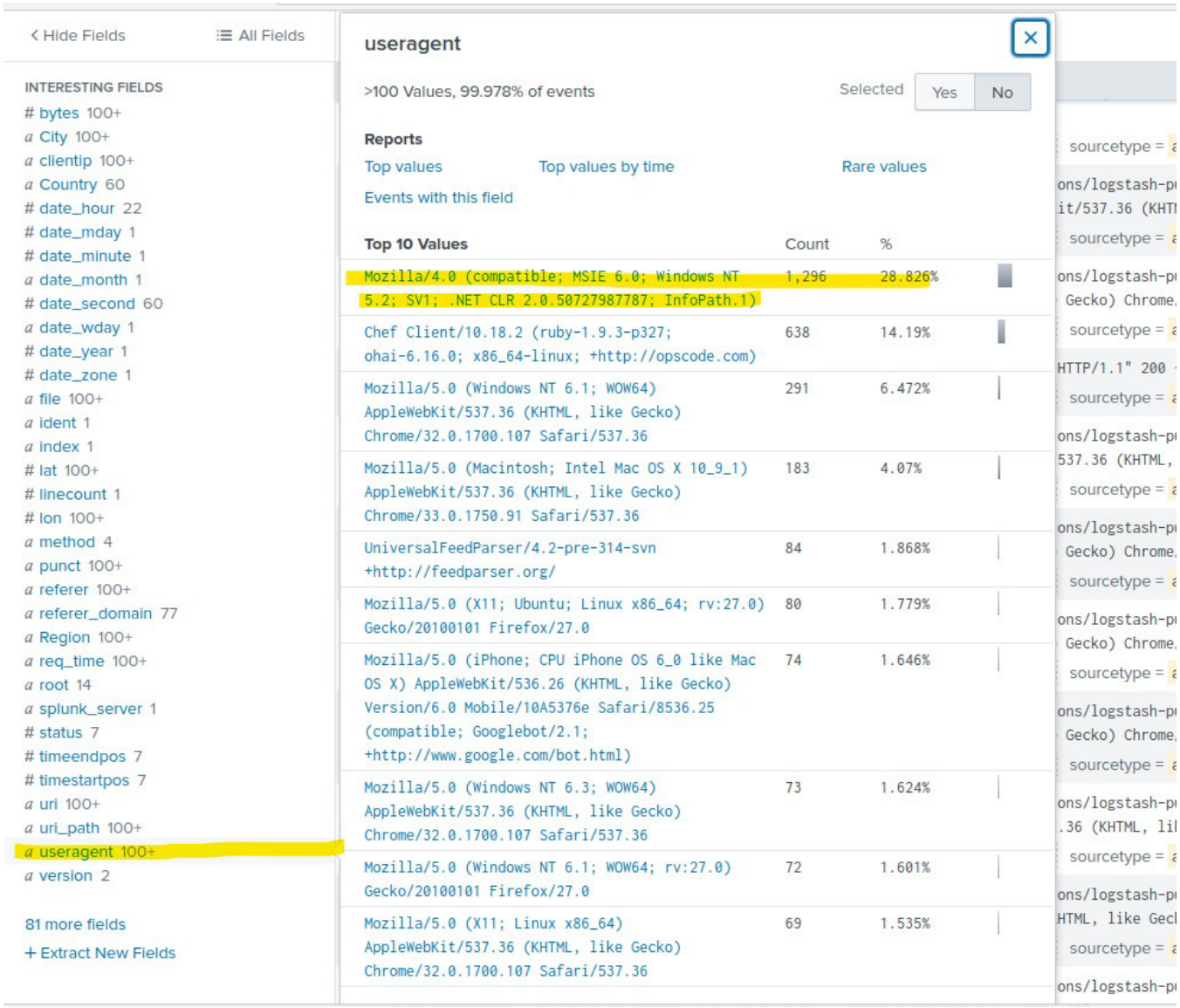
“Block all incoming HTTP traffic from the cities San Antonio, Kharkiv, Springfield, and Stockholm”



Question 2: There is a high percentage of attack traffic coming from 2 variations of the same domain, www.semicomplete.com. There is a good chance that this webserver was compromised as a zombie computer or bot and being used in the brute force and denial of service attacks against VSI. About 85% of all attack traffic originates from this domain.

By blocking traffic coming from this referer domain, we should be able to also mitigate more attack traffic regardless of location to VSI's server.

"Block all incoming HTTP traffic from the from the referer_domain 'www.semicomplete.com' and 'semicomplete.com'"



There is also a very high amount of the attack traffic coming from an older outdated version of the Mozilla/4.0 client. This seems to have a known association with a HTTP DDoS tool that is being used for attacks. Adding this to the firewall block rules would be beneficial for limiting the exposure to known attack tools.

“Block all incoming HTTP traffic from the from the user agent ‘Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)’”