### Part 1: Windows Webserver 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.

**Mitigation in regards to each user account:**

**1. Limit the number of incorrect password attempts.**

**2. Secondary authentication measures like pins, token codes, and secret questions.**

**3. Enforce strong password standards.**

**Mitigation on a global scale:**

**1. Again, implement lockouts and limit the number of password attempts.**

**2. Whitelist IP addresses for employees.**

**3. Secondary authentification.**

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?

**Mitigation could include something like a captcha to prevent automated logins. You can have a delayed lock out, an account is only locked for a certain period of time.**

### Part 2: Apache Webserver Attack:

Question 1

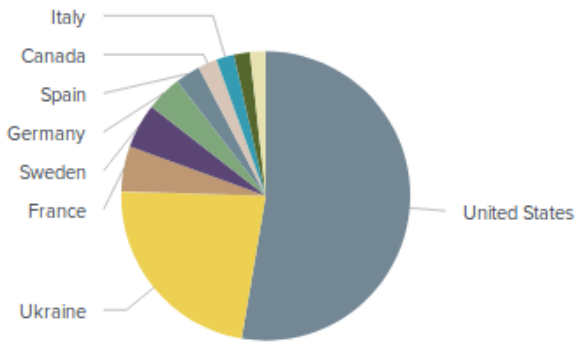
- Based on the geographic map, recommend a firewall rule that the networking team should implement.

- 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.

**There is a large influx of traffic from the Urkraine. We are going to want to block HHTP traffic from  IP's located in the Urkraine.**



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".

  - Hint: Look for other fields that indicate the attacker.

**We can change and hide the port numbers.**

**Establish private networks and VPNs so only the private IPs have access.**