# Cybersecurity Threat Landscape (Part 2 - Akamai)

In this part, you should primarily use the *Akamai\_Security\_Year\_in\_Review\_2019* and *Akamai State of the Internet/ Security* plus independent research to answer the below questions.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. DDOS attack events from January 2019 to September 2019 largely targeted which industry?   
   **Gaming Industry**
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   **Financial Services Industry**
3. Which companies are the top phishing targets, according to Akamai?   
   **Microsoft, PayPal, DHL, Dropbox, DocuSign, and Linkedin**
4. What is credential stuffing?   
   An attack that targets accounts emails, usernames & passwords
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **USA is #1 and Russia is #2**
6. Which country is the number one source of web application attacks? Which country is number 2?  
   **USA is #1 and Russia is #2**
7. In Akamai’s State of the Internet report, it refers to a possible DDoS team that the company thought was affecting a customer in Asia (starts on page 11).

* Describe what was happening.
* What did the team believe the source of the attack was?
* What did the team actually discover?

1. What is an example of a performance issue with bot traffic?
2. Known-good bots are bots that perform useful or helpful tasks, and not do anything malicious to sites or servers. What are the main categories of known-good bots.
3. What are two evasion techniques that malicious bots use?   
   **Altering the User Agent and changing IP addresses**