# 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**
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   **Financial Services**
3. Which companies are the top phishing targets, according to Akamai?   
   **Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn**
4. What is credential stuffing?   
   **Stolen account credentials are used to gain unauthorized access to user accounts through large-scale automated login request directed against a web application.**
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **United States is number 1 and Russia is number 2**
6. Which country is the number one source of web application attacks? Which country is number 2?  
   **United States is number 1 and Russia is number 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.- **customer in Asia was receiving an abnormal amount of traffic to one of its URLs. they saw so much traffic that at its peak it almost overflowed the database akamai uses to log such activity. Traffic reached 875000 requests per second. This was a DDOS Attack**
* What did the team believe the source of the attack was?

**They thought it was a DDoS attack**

* What did the team actually discover?   
  **The importance of developing a strong defensive posture.**

1. What is an example of a performance issue with bot traffic?   
   **Slow websites and frustrated customers**
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.   
   **Search engine crawlers, web archives, search engine optimization, audience analytics and marketing service, site monitoring services, content aggregators**
3. What are two evasion techniques that malicious bots use?   
   **Altering the user agent or other http header values, allowing the bot to impersonate widely used browsers. Change the ip addresses used in order to mask their origin.**