# 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 is the largely targetting industry in 2019 accounting to close to 3,500 DDoS attack events.
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   Financial Services industry is the largely targeted industry in 2019 with almost 50% of the unique targets for DDoS attacks.
3. Which companies are the top phishing targets, according to Akamai?   
   Microsoft, Paypal, DHL, Dropbox, Docusign, and LinkedIn are the top phishing targets, according to Akamai.
4. What is credential stuffing?   
   Credential Stuffing is a methodology where the attacker uses a known/breached pair of username & password to fraudulently access the resources.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   United States is the number one source of credential abuse attacks in the Americas as well as in the world whereas Russia takes the 2nd place.
6. Which country is the number one source of web application attacks? Which country is number 2?  
   United States is the number one source of web application attacks while Russia takes the 2nd place.
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. - In Early 2018, Akamai noticed abnormal traffic to one of the URLs that belongs to a customer in Asia.
* What did the team believe the source of the attack was? DDos
* What did the team actually discover? Large amount of HTTP requests going to the customer’s URLs.

1. What is an example of a performance issue with bot traffic?   
   Slow website response is 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.   
   Search Engine Crawlers, Web Archives, Search Engine Optimisation, Audience Analytics, Marketing service. Site Monitoring Services, Content Aggregators are the main categories of known-good bots.
3. What are two evasion techniques that malicious bots use?   
   Altering User Agent or other HTTP header values, IP address change-out are two most common evasion techniques that malicious bots use.