# 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?   
   **Answer: -** Gaming industry most affected by DDOS attacks in 2019.
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   **Answer: -** It was financial industry got targeted almost 50% of unique targets by DDoS attacks in 2019.
3. Which companies are the top phishing targets, according to Akamai?   
   **Answer: -** Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn are all top phishing targets, according to Akamai’s monitoring.
4. What is credential stuffing?   
   **Answer: -** Credential stuffing is a cybercrime technique in which attackers use lists of compromised user credentials to breach into a system or website, and an attacker uses automated scripts to try each credential against a target website, and reason this works is the majority of users reuse the same credentials on multiple accounts.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **Answer: -** United States is a top source for credential abuse attacks and Russia is on number two position for credential abuse attacks.
6. Which country is the number one source of web application attacks? Which country is number 2?  
   **Answer: -** United States is a top source for web application attacks and Russia is on number two position for web application attacks.
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?   
  **Answer: -**

1. Early in 2018, Akamai noticed a customer in Asia was receiving an abnormal amount of traffic to one of its URLs. The customer was seeing so much traffic that, at its peak, it almost overflowed the database Akamai uses to log such activity.
2. The data showed all the hallmarks of a major DDoS attack.
3. They discover it was a Windows-oriented tool that was responsible for this massive flood of requests.
4. What is an example of a performance issue with bot traffic?   
   **Answer: -** Slow websites is an example of a performance issue with bot traffic.
5. 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.  
   **Answer: -** Below are following main categories when considering known-good bots.
6. Search Engine Crawlers.
7. Web Archives.
8. Search Engine Optimization.
9. Audience Analytics.
10. Marketing Service.
11. Site Monitoring Services.
12. Content Aggregators.
13. What are two evasion techniques that malicious bots use?   
    **Answer: -**
14. First evasion technique is altering the User Agent, or other HTTP header values.
15. Second evasion technique is change the IP addresses used in order to mask their origin, or use multiple IP addresses.