# 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. More on it was explain that the game industry suffered from just under 9,000 attacks between 2017-11 to 2019-04.**
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?   
   **Utilizing stolen usernames and passwords to test on a website. The list of stolen usernames can come from a corporate breach or darknet. The testing is done by bots interacting with websites.**
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **United States of America is the number one source of credential abuse attacks followed by the number two being Canada.**
6. Which country is the number one source of web application attacks? Which country is number 2?  
   **United States of America is the number one source of web application attacks followed by the number two being Brazil.**
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?

* **A customer in Asia was receiving abnormal amount of traffic to one of its URLs.**
* **Another department also flagged the traffic as something to investigate because it seemed like a major DDOS attack.**
* **The high volume of traffic hammering this customer's URL was the result of a warranty tool gone haywire.**

1. What is an example of a performance issue with bot traffic?

**Slow websites, frustrated customers, increase in IT expenses.**

1. 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 - google.com**
* **web archives - scanning the web periodically and recording its content to searchable indexed data**
* **SEO, Audience analytics and marketing service.**
* **Site monitoring services**
* **Content Aggregators.**

1. What are two evasion techniques that malicious bots use?

* **The most basic evasion technique is to alter the User Agent or change HTTP header values. This allows the bot to impersonate widely used browsers, mobile applications, or even known-good bots.**
* **Bots will also change the IP addresses used in order to cover up their origin or use multiple IP addresses for the same purpose. The IP address change-out is also used to bypass rate limitations, as the bot will use a “low and slow” method where multiple IP addresses send a low number of requests each hour.**