# 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?   
   **The attack events from Jan 2019 to Sept 2019 largely targeted the gaming industry.**
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   **Almost 50% of unique targets largely targeted the Financial Services industry.**
3. Which companies are the top phishing targets, according to Akamai?   
   **Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn are the top phishing targets.**
4. What is credential stuffing?   
   **“Credential stuffing is a cyberattack method in which attackers use lists of compromised user credentials to breach into a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.”** (**imperva**)
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **United States then Russia**
6. Which country is the number one source of web application attacks? Which country is number 2?  
   **United States then Russia**
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?   
  **In 2018, Akamai was informed by another department who flagged excess traffic overflowing a customer’s database. When the security team noticed a large number of HTTP requests going to the URL, they knew they had to stop it.**

**The team believed that a Windows-oriented tool was responsible for the uptick in URL visits.**

**The team discovered that there was no attack but instead, a warranty tool was having issues. The tool kept visiting the URL so once a fix was pushed, everything eventually went back to normal.**

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, and content aggregators.**
3. What are two evasion techniques that malicious bots use?   
   **Altering the User Agent and change the IP addresses used.**