# 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?   
   **It is a cyberattack that uses stolen usernames and passwords from one organization to gain access to other organizations. Stolen information can be acquired via data breaches or purchased off the dark web.**
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **#1 United States #2 Russia**
6. Which country is the number one source of web application attacks? Which country is number 2?  
   **#1 United States #2 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. **A customer was receiving an abnormal amount of traffic to one of its URLs. Traffic volume reached 875,000 requests per second at one point.**
* What did the team believe the source of the attack was? **The initial report and associated data showed all the hallmarks of a major DDoS attack.**
* What did the team actually discover? **They concluded the high volume of traffic was the result of a warranty tool gone haywire.**

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**

1. What are two evasion techniques that malicious bots use?   
   **1. Altering the User Agent or other HTTP header values to impersonate widely used browsers, mobile applications, or known-good bots.**

**2. Change the IP addresses used in order to mask their origin or use multiple IP addresses.**