# 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?   
   Credential stuffing is a cyber attack in which credentials obtained from a [data breach](https://www.cloudflare.com/learning/security/what-is-a-data-breach/) on one service are used to attempt to log in to another unrelated service.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   United States of America and Russia
6. Which country is the number one source of web application attacks? Which country is number 2?  
   United States of America and 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 large amount of HTTP requests going to a customer’s URL , traffic volume reached 875,000 requests per second at one point. There were 139 IP addresses approaching the customer’s URL a few days before the peak, with the exact same “attack” features. This URL went from 643 requests, to well over 4 billion, in less than a week.
* What did the team believe the source of the attack was? - A DDoS attack from a Windows-oriented tool.
* What did the team actually discover? - They concluded 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 and frustrated customers.

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, Web Archives, (Search Engine Optimization, Audience Analytics, And Marketing Service), Site Monitering Services, Content Aggregators

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

- The most basic evasion technique is altering the User Agent, or other HTTP header values, allowing 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 mask their origin, or use multiple IP addresses. 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.