# 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?   
   They largely targeted the Gaming industry.
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   They largely targeted Financial Services.
3. Which companies are the top phishing targets, according to Akamai?   
   According to Akamai, companies that are the top phishing targets are Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn.
4. What is credential stuffing?   
   According to Wikipedia, credential stuffing is a type of cyberattack in which stolen account credentials, usually consisting of lists of stolen usernames, emails and corresponding passwords, are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   Number one source of credential abuse attacks is the United States. Country number 2 is Russia.
6. Which country is the number one source of web application attacks? Which country is number 2?  
   According to the three sources (Americas, EMEA, APAC) the number one source of web applications is the United States, followed by 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?   
  Akamai has noticed that one of their customers was receiving abnormal amounts of traffic. The amount of traffic was so high that at its peak it almost overflowed Akamai’s database responsible for logging such activities.

Initial investigation and reports suggested a large-scale DDoS attack.  
  
After mitigating over 4 billion requests from 15,582 IP addresses they discovered that the source of the high traffic was a warranty tool gone haywire. This was later confirmed by the customer as well as the vendor responsible for the said tool. A patch was pushed within hours to all affected systems to prevent future incidents.

1. What is an example of a performance issue with bot traffic?   
   An example of a performance issue with bot traffic is a slow website.
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?   
   The main categories of known-good bots are Search Engine Crawlers; Web Archives; Search Engine Optimization, Audience Analytics, and Marketing Service; Site Monitoring Services; Content Aggregators.
3. What are two evasion techniques that malicious bots use?   
   Two evasion techniques mentioned are:

Altering of the User Agent, or other HTTP header values, allowing bots to impersonate widely known and used web browsers, mobile apps or even known-good bots.

Change of the IP address used in order to mask their origin, or use multiple IP addresses.