# 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 was the number one services targeted by DDOS attacks, by a large margin. Over 3,000 attacks on the gaming industry occurred between January and September of 2019, vs fewer than 1,000 in telecom and Internet.
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
   Financial Services were the largest industry targeted by DDoS attacks. Over 40% of unique attacks targeted financial services, whereas gaming, the next-largest industry targeted, accounted for just over 10% of all unique attacks between January and September of 2019.
3. Which companies are the top phishing targets, according to Akamai?   
   Some of the top targets of phishing scams were Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn.
4. What is credential stuffing?   
   Credential Stuffing is a cyberattack in which attackers are able to use data such as usernames and passwords, obtained in a previous data breach to gain access to other accounts. Credential Stuffing is only possible because many targets use the same credentials for multiple accounts.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   When accounting for all credential abuse attacks, the United States is the number one source, followed by Russia, but when only looking at data from gaming attacks, Russia is the number one source.
6. Which country is the number one source of web application attacks? Which country is number 2?

Again, the United States is the top source for Web Application attacks with 1,434,231,212 attacks occurring between November 2017 and September 2019, and Russia is number 2, with 1,093,219,355 attacks.

1. 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 in Asia was receiving a high volume of traffic to one of its URL’s. The data showed what resembled a DDoS Attack (a distributed denial-of-service attack, which occurs when multiple systems flood the bandwidth or resources of a targeted system). At one point the traffic was so high it reached 875,000 requests per second at one point.
* What did the team believe the source of the attack was?
  + The team believed the source was a DDoS attack.
* What did the team actually discover?
  + There was no attack. The high volume of traffic was the result of a faulty warranty tool that kept visiting the same URL.

1. What is an example of a performance issue with bot traffic?   
   Slow websites is one example of performance issues with bots.
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.   
   There are five main categories used when considering 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?   
   Malicious bots will sometimes change their IP address to mask their location or even use multiple IP addresses to send a low number of requests, or they might alter the User Agent to impersonate other browsers or even other known-good bots to avoid detection.