# 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 most DDOS attacks were found to be in the gaming industry from January to September of 2019.
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry? The unique targets that valued at almost 50% of the unique DDOS attacks were in Financial services from January to September of 2019.
3. Which companies are the top phishing targets, according to Akamai? The top companies that were targeted for phishing were Microsoft, Paypal, DHL, Dropbox, Docusign, and LinkedIn.
4. What is credential stuffing?   
   The attack known as credential stuffing is when an attacker uses a bot to stuff multiple credentials form by form to overwhelm a system.
5. Which country is the number one source of credential abuse attacks? Which country is number 2? The number one slot for the biggest source of credential abuse attacks was by far America in the year of 2019.
6. Which country is the number one source of web application attacks? Which country is number 2? The number one slot for the most web application attacks was also America in the year of 2019.
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.` The customer was receiving a large amount of traffic to one of it’s URLs.
* What did the team believe the source of the attack was? The team thought originally that it was a DDoS attack via the 875,000 requests per a second.
* What did the team actually discover? The team discovered that it wasn’t an attack at all it was just a warranty tool gone haywire.

1. What is an example of a performance issue with bot traffic? When there is too much bot traffic this can overwhelm a server and cause a DDoS attack.
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.Here are a couple of the well known good bots are Search Engine Crawlers, Web Archives, Search Engine optimization, Audience Analytics, and Marketing Services, Site monitoring services, and content Aggregators.
3. What are two evasion techniques that malicious bots use? The two big evasion techniques that the bad bots use are changing the User header to a well known website such as google and also changing their IP addresses to not trigger any alarms by sending too many form requests from one IP address.