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? An attack that attempts to gain access by using automated login requests with stolen credentials like usernames and their corresponding passwords.

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. An absurd amount of traffic was flooding one of its URLs, as much as 875,000 requests per second at one point. The flooding was coming from HTTP requests.

- What did the team believe the source of the attack was? They believed it was a DDoS attack.
- What did the team actually discover? They discovered it was an issue with a warranty tool gone wrong. Once the SOCC started filtering traffic, the warranty tool kept visiting the URL and it wasnt changing anything in the headers.

8. What is an example of a performance issue with bot traffic? Slow websites and frustrated customers

9. 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

10. What are two evasion techniques that malicious bots use? Altering the user agent or other HTTP header values which allows them to impersonate widely used browsers, mobile applications and even known-good bots. They will also change the IP addresses to hide their origin and will even use multiple IP addresses.