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?
   High Technology

4. What is credential stuffing?
   Credential stuffing leverages people's tendency to re-use passwords. An attacker will gain passwords from one source and use it in another source.

5. Which country is the number one source of credential abuse attacks? Which country is number 2?
   United States and Russia respectively

6. Which country is the number one source of web application attacks? Which country is number 2?
   United States (#1) and Brazil (#2)

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 team noticed a large amount of web traffic to one of Akamai's customer's URLs. The number of HTTP requests was so large that Akamai's logging server almost crashed.
- What did the team believe the source of the attack was?

    - The document doesn’t actually state what the SOCC or SIRT team actually thought the source of the attack was. It only states that those teams thought that the traffic was the result of a malicious attack.
- What did the team actually discover?
    - The massive amount of network traffic was the result of a faulty application warranty tool.

8. What is an example of a performance issue with bot traffic?
   A lot of bot traffic occurs over the web. This can cause websites to load slower.

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

10. What are two evasion techniques that malicious bots use?
    From the report:
    - “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.”