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? - the automated injection of a breached username/password pairs in order to fraudulently gain access to a user account. This is a subset of the brute force attack category.

   Source:

https://owasp.org/www-community/attacks/Credential_stuffing

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.

  A customer was receiving an abnormal amount of traffic to one of its URLs. The customer was seeing so much traffic that, at its peak, it almost overflowed the database Akamai uses to log such activity

- What did the team believe the source of the attack was? - a major DDoD (Distributed Denial of Service attack)
-
- What did the team actually discover? - The Security Incident Response Team and Security Operations Command Center concluded the high volume of traffic hammering the customer's URL was a result of a warranty tool gone hayware. A fix was pushed within hours to all affected systems.

8. What is an example of a performance issue with bot traffic? - Here are 2: 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, allowing the bot to impersonate widely used browsers, mobile apps, or even known-good bots

    -changing the IP address used in order to mask their origin, or use multiple IP addresses