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?

   It was the gaming industry that was targeted.

2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?

   It was against the financial services industry

3. Which companies are the top phishing targets, according to Akamai?

   Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn are all top phishing targets, according to Akamai's monitoring.

4. What is credential stuffing?

   Credential stuffing is a cybercrime technique where an attacker uses automated scripts to try each credential against a target website. The reason this works is the majority of users reuse the same credentials on multiple accounts.

5. Which country is the number one source of credential abuse attacks? Which country is number 2?

    a. **United States of America**
    b. **Russia**

6. Which country is the number one source of web application attacks? Which country is number 2?

    a. **United States of America**
    b. **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.
        - **In early August, Black Hat, DEF CON, and BSides Las Vegas were taking place, and many of the early headlines were part of what journalist Violet Blue calls "Infosec Clickbait Season." But the news item that got the most buzz wasn't even security-related — it was about a man wearing a TV on his head, who was observed on camera leaving TVs on porches in Virginia. After narrowly avoiding a plague of locusts in Las Vegas, those who attended Black Hat were told they might have been exposed to measles if they were in the area between August 3 and 5.**
    - What did the team believe the source of the attack was?
        - **The team believed the source of the attack was 94% of the attacks against the financial sector came from SQLi attacks, LFI, Cross-Site Scripting (XSS), and OGNL Java Injections.**
    - What did the team actually discover?
        - **The team discovered a new DDoS vector that can hit 35/Gbps. The vector, which leverages a UDP amplification technique known as WS-Discovery (WSD), can be used to get amplification rates of up to 15,300%.**

8. What is an example of a performance issue with bot traffic?

   Bots can be programmed to click on your ads, leaving chaos in their wake: for example, by draining your Adwords account, by causing Google to rate your ad's performance as poor, by stopping your ad being displayed while competitors' ads are featured prominently, and by impacting conversion rates and rendering your analytics meaningless.

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?

   Good bots are the ones that are beneficial to the business as well as the individuals. Examples of Search engines as Googlebot, Bingbot, and Baidu Spider to name a few. There are other bots that are used in various categories, such as Slackbot for partner bot, Facebook Bot for social networking to name a few.

10. What are two evasion techniques that malicious bots use?

    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.