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 aFittacks 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?
   Credential stuffing is a cybercrime technique where an attacker uses automated scripts to try each credential against a target web site.

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

6. Which country is the number one source of web application attacks? Which country is number 2?
   United States and 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.
- What did the team believe the source of the attack was?
- What did the team actually discover?
  Akamai noticed that one of their customers was receiving an abnormal amount of traffic going to one of it's URL's. It almost overflowed their database. They thought it was a DDoS attack. Early log grabs were up to 5.5 Gbps. The initial spike was so large they thought it had to be a DDoS

attack. The SIRT worked on determining the root cause of the surge in traffic, while the SOCC worked on getting customer's operations back to normal. Before this, the traffic to the customer's URL was seeing GET and POST request methods. Now, it was primarily a large number of POST requests. The SIRT thought it was a Windows-oriented tool. It was actually a warranty tool gone haywire. It wasn't a malicious attack because it didn't alter anything in the headers, such as the User Agent. They learned of the importance of developing a strong defensive posture. Prevent the problem before it exists!

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, allowing the bot to impersonate widely used browsers, mobile applications, or even known-good bots.
    Changing the IP addresses used in order to mask their origin, or use multiple IP addresses.