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?

Multi-factor authentication and credential stuffing were themes Akamai followed throughout 2019.

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

   In 2019, Financial Services counted for more than 50 percent of unique targets for DDoS attacks.
3. Which companies are the top phishing targets, according to Akamai?

   In 2019, Gaming companies were the top phishing targets according to Akamai.
4. What is credential stuffing?

   Credential stuffing is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?

   The USA is the top source for credential stuffing, followed by Russia.
6. Which country is the number one source of web application attacks? Which country is number 2?

   The country with the number one source of web app attacks is USA and Russia is number 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.

  In 2018, Akamai noticed a customer in Asia was receiving an abnormal amount of traffic to one of its URLs. The customer had observed no traffic that, at its peak, it almost overflowed the Akamai used to log suck activity.

- What did the team believe the source of the attack was?

  When flagged this trafic as something to investigate, the initial report and associated data showed all the hallmarks of a major DDoS attack.

- What did the team actually discover?
  It was concluded that high volume of traffic hammering this customer's URL was the result of a warranty tool gone haywire.

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

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?

   The main categories of known-good bots are; Search engine crawlers, Web archives, Search engine optimization, Audience Analytics and Marketing services, Site Monitoring services, and content aggregators.

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

    Two evasion techniques that malicious bots use are; altering the User Agent, or other HTTP header values, and Bots will also change the IP addresses used in order to mask their origin, or use multiple IP addresses.