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 Industries
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?
   Passwords from a previous attack are automatically entered into a website in an attempt to log in. If one of these passwords match an existing account, the attacker can gain access to sensitive data and systems

5. Which country is the number one source of credential abuse attacks? Which country is number 2?
   USA is one and Russia comes second

6. Which country is the number one source of web application attacks? Which country is number 2?
   USA is one and Russia is two

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?

  The customer was seeing an abnormal amount of traffic specifically HTTP requests to one of its URLs. There were 139 IP addresses approaching the

customer's URL a few days before the peak, with the exact same "attack" features. This URL went from 643 requests to more than 4 billion requests. They believed an attack was occurring, and that it was being requested by a Windows COM Object (WinhttpRequest).

The team found that none of the header fields were being altered. They released that the incident was not an attack. The 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 due to DDoS attacks.

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, SEO services,

10. What are two evasion techniques that malicious bots use?
    -Altering the User Agent, or other HTTP header values.

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