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?

   The Gaming Industry

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?

   Credential stuffing is basically trying to gain access to other peoples accounts on different websites with stolen usernames and passwords.

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

   1.United States and 2. Russia

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

   1.United States and 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.

Akamai noticed that the URL of a customer located in Asia was receiving an unusually high amount of traffic. It almost overflowed Akamai's database which is responsible for logging this sort of activities.

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

They believed it was a DDoS

What did the team actually discover?

The team discovered that a few days before the "attack'' a same pattern appeared which peaked well over 4 billion requests. Half of the IPs were flagged as NAT gateways and the traffic was generated by a Windows COM Object (WinRequest). Originally the requests types were GET and POST methods but the flagged request contained of 98% of POST requests. Examining all the POST requests hitting the customer's URL showed that the User-Agent fields were not being forged or otherwise altered once blocked.

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

   It can create a high load on your website's servers, slowing down server-side response times. That leads to delays for the customers and it will leave them frustrated.

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**
   - **MARKETING SERVICE**
   - **SITE MONITORING SERVICES**
   - **CONTENT AGGREGATORS**

10. What are two evasion techniques that malicious bots use?
    - **Changing HTTP headers in order to impersonate a popular browser, applications or sometimes even good bots.**
    - **Morphing IP addresses via proxies, VPNs, and Tor.**

- **Cookie tampering in the form of dropping cookies to force timeout.**