# 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 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 where various amounts of compromised usernames and passwords are automatically used on a website in order to gain access to an unauthorized account.**
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
    **The United States is the number 1 source of credential abuse attacks with over 25 billion malicious logins, while Russa is number 2 with just over 6 billion malicious logins.**
6. Which country is the number one source of web application attacks? Which country is number 2?  
    **The United States is the number one source of web application attacks with 1.4 billion attacks, while Russia is number 2 with just under 1.1 billion attacks.**
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.

**A customer of Akamai was getting an insanely high amount of network traffic to their URL which led Akamai to believe this user was getting attacked.**

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

**The team believed the source of the attack was from a Windows COM Object (otherwise known as WinhttpRequest).**

* What did the team actually discover?

**The team realized that the customer wasn’t actually getting attacked. Instead, it turned out to be a bug in a warranty tool that the customer used.**

1. What is an example of a performance issue with bot traffic?   
    **Bot traffic can slow down your website.**
2. 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), and (Content aggregators).**
3. What are two evasion techniques that malicious bots use?   
    **Malicious bots will change its User-Agent Header in order to act as if its a Good Bot, mobile application, or a widely used browser.**

**Malicious bots can also change its IP address or use multiple IP addresses in order to hide its origin and/or bypass rate limitations.**