# 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 was the most largely targeted industry for DDOS events for the period of January 2019 - September 2019.
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?   
     
   Financial Services comprised almost 50% of the unique targets for DDOS attacks for the period of January 2019 - September 2019.
3. Which companies are the top phishing targets, according to Akamai?   
     
   The companies that are the top phishing targets, according to Akamai’s research and reporting are
4. What is credential stuffing?   
     
   Credential stuffing is a cyberattack in which stolen account credentials are used to gain access to user accounts through large-scale automated login requests on web applications. The credentials, primarily user names and passwords are usually stolen during data breaches.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
     
   The United States and Russia are the number one and number two sources of credential attacks; respectively. The United States had 25,393,327,336 reported malicious logins and Russia had 6,114,186,048 malicious logins.
6. Which country is the number one source of web application attacks? Which country is number 2?  
     
   The United States and Russia are also the number one and number two sources of web application attacks with the US having a total of 1,434,231,212 total attacks and Russia reporting a total of 414,257,266 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.
* What did the team believe the source of the attack was?
* What did the team actually discover?

A company’s website was experiencing a devastatingly high number of URL requests that very quickly ramped up 643 requests to over 4 billion requests within a week. The requests came fro 139 IP addresses that exhibited “attack features”. Earlier site visits contained bot GET and POST methods but during the “attack” the URL was getting inundated with just POST requests.

The team believed the source of the attack was a Windows COM Object (WinhttpRequest).  
  
The team discovered that a code bug caused out-of-control activity by warranty tool consistently visiting the customer’s URL.

1. What is an example of a performance issue with bot traffic?   
     
   Slow websites can be a performance issue with bot traffic.
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?   
     
   The primary categories of known-good bots are:  
   Search engine crawlers  
   Web archives  
   Search engine optimization, audience analytics, and marketing services  
   Site monitoring services  
   Content aggregators
3. What are two evasion techniques that malicious bots use?   
   Malicious bots often use the following evasion techniques:

* Altering the User Agent or other HTTP header values to allow impersonation of trustworthy bots and services.
* Changing IP addresses to shield their origin or use multiple IP addresses.