# 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 are all top phishing targets, according to Akamai’s monitoring.** (Pg 14)
4. What is credential stuffing?   
   **-Credential stuffing is a cyberattack method in which attackers use lists of compromised user credentials to breach into a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.**

(<https://www.imperva.com/learn/application-security/credential-stuffing/#:~:text=Credential%20stuffing%20is%20a%20cyberattack,and%20passwords%20across%20multiple%20services>.)

1. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   **- Num1: U.S. (25,393,327,336)**

**-Num2: Russia (6,114,186,048)**

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

* **Num1: U.S. (1,434,231,212)**
* **Num 2: Russia (1,093,219,355)**

1. 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?   
  **-Akamai noticed a customer in Asia was receiving an abnormal amount of traffic to one of its URLs. The customer was seeing so much traffic that, at its peak, it almost overflowed the database Akamai uses to log such activity. When another department flagged this traffic as something to investigate, the initial report and associated data showed all the hallmarks of a major DDoS attack. Traffic volume reached 875,000 requests per second at one point. (pg 11)**
* **Once the SOCC started digging into the report, they observed a large amount of HTTP requests going to a customer’s URL — leading to an immediate presumption of attack, as seen in Figure 1. (Pg 12)**
* **Earlier analysis, backed by additional SIRT research, concluded the high volume of traffic hammering this customer’s URL was the result of a warranty tool gone haywire. Once the SOCC started filtering traffic, the warranty tool kept visiting the URL. However, the subsequent visits didn’t alter anything in the headers (such as the UserAgent) that could’ve assisted in bypassing mitigations, proving that this incident wasn’t a malicious attack. This conclusion was later confirmed by the customer, as well as the vendor responsible for the tool. A fix was pushed within hours to all of the affected systems. (pg 14)**

1. What is an example of a performance issue with bot traffic?   
   **-Slow websites and frustrated customers (pg 16)**
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; Content Aggregators (pg 16)**

1. What are two evasion techniques that malicious bots use?   
   **- Altering the User Agent, or other HTTP header values, allowing the bot to impersonate widely used browsers, mobile applications, or even known-good bots.**

**-Bots will also change the IP addresses used in order to mask their origin, or use multiple IP addresses. The IP address change-out is also used to bypass rate limitations, as the bot will use a “low and slow” method where multiple IP addresses send a low number of requests each hour. (pg 17)**