# 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_good work overall

1. **DDOS attack events from January 2019 to September 2019 largely targeted which industry?**   
   Gaming companies suffered the most DDoS attacks in this period.
2. **Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?**   
   The industry which suffered the most uniquely targeted attacks was Financial Services
3. **Which companies are the top phishing targets, according to Akamai?**   
   DHL, Docusign, Dropbox, LinkedIn, Microsoft and PayPal were seen to be the top phishing targets.
4. **What is credential stuffing?**   
   Utilising an extensive source of login credentials; typically harvested from a data breach; the attackers attempt logon for each credential at an unrelated entity. The concept is that many users reuse credentials and so the same logon may provide access to other accounts. The success rate is estimated to be up to 2%, which is considerably high when taking into account the relative ease with which the attack can be performed.
5. **Which country is the number one source of credential abuse attacks? Which country is number 2?**  
   According to the Akamai review, the US was the top source, followed by Russia.
6. **Which country is the number one source of web application attacks? Which country is number 2?**  
   Again, the US sits as the number 1 source of web application attacks, with Russia coming in second.
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.**  
  The customer’s URL was being absolutely hammered by requests, reflective of a DDoS attack.
* **What did the team believe the source of the attack was?**   
  Packet analysis lead the team to suspect a Windows COM Object was generating the requests, suggesting that a Windows platform tool or feature was causing the ‘attack’.
* **What did the team actually discover?**   
  Once the dust has somewhat settled, the source of the ‘attack’ was identified as a warranty tool that had malfunctioned.

1. **What is an example of a performance issue with bot traffic?**   
   Increased bot traffic can lead to congestion thus slowing access to online businesses. This can in turn lead to higher costs as resources ramp up to compete with the extra load.
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.**   
   As listed in the Akamai report, the main categories of known-good bots are Search Engine Crawlers, Web Archives, SEO/Analytics/Marketings, Site Monitoring and Content Aggregators.
3. **What are two evasion techniques that malicious bots use?**   
   The most basic is altering the User Agent, making the bot appear to be a legitimate user by impersonating a specific browser or mobile application.  
   Another method is cookie tampering whereby the bots may play back harvested good cookies.