# 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 the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
   United States is number one

Russia is number 2

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

Russia is number 2

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.

Early in 2018, 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.

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

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. Notes from early in the incident record the flood of traffic as highly distributed, with early log grabs recording 5.5 Gbps

* What did the team actually discover?   
  Analysis by additional SIRT research concluded the high volume of traffic hammering the 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.

1. What is an example of a performance issue with bot traffic?   
   Slow websites
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

SEO, Audience analytics, Marketing Service

Site Monitoring Services

Content Aggregators

1. What are two evasion techniques that malicious bots use?   
   Alter User Agent or other HTTP header values to impersonate

Change the IP addresses to mask their origin (or use multiple IP addresses to bypass rate limitations)