# 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?

**During Jan 2019 - Sept 2019 Gaming Industry was largely target**

1. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?

Financial Services

1. Which companies are the top phishing targets, according to Akamai?   
   **• Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn**
2. What is credential stuffing?

**Credential stuffing** is a type of [cyberattack](https://en.wikipedia.org/wiki/Cyberattack) in which stolen account [credentials](https://en.wikipedia.org/wiki/Credentials), typically consisting of lists of [usernames](https://en.wikipedia.org/wiki/Username) and/or [email addresses](https://en.wikipedia.org/wiki/Email_addresses) and the corresponding [passwords](https://en.wikipedia.org/wiki/Password) (often from a [data breach](https://en.wikipedia.org/wiki/Data_breach)), are used to gain unauthorized access to [user accounts](https://en.wikipedia.org/wiki/User_account) through large-scale automated login requests directed against a [web application](https://en.wikipedia.org/wiki/Web_application).[[1]](https://en.wikipedia.org/wiki/Credential_stuffing#cite_note-1)

1. Which country is the number one source of credential abuse attacks? Which country is number 2?

**United States   
Russia**

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

United States and Russia

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. - 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 believe the source of the attack was? Warranty tool gone haywire
* What did the team actually discover?   
  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.

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

Page Load Speed, An abnormal decrease in bounce rate

1. 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.

Chat bots, Transactional bots and Informational bots

1. What are two evasion techniques that malicious bots use?

SQLi attacks, LFI, Cross-Site Scripting (XSS), and OGNL Java Injections