# 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?

DDOS attack events were mostly target at the **Gaming industry**

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

Almost 50% of unique targets for DDos attacks were targeted at **Financial Services industry**

1. Which companies are the top phishing targets, according to Akamai?

According to Akamai, **Microsoft, PayPal, DHL, Dropbox, DocuSign, and Linked** are the top phishing targets

1. What is credential stuffing?

Credential stuffing is an attack that targets **usernames, passwords, and email addresses** using lists of known compromised credentials

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

The **USA** is the number one source of credential abuse attacks followed by **Russia**

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

Once again the **USA and Russia** are the top two sources of web application attacks

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 SOCC found a report containing a large amount of HTTP requests going to a customers URL making them think a DDoS attack was in progress

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

The SOCC team thought the source of the attack was a **Windows COM Object (WinhttpRequest)**

* What did the team actually discover?

The team found that the cause of the high traffic was actually a **bug in a warranty tool**

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

Bot traffic can cause slow server responses due to bot traffic. This causes delays for end users making the service feel unresponsive or slow

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.

**Search engine crawlers**

**Web archives**

**Search engine optimization, audience analytics, marketing service**

**Site monitoring services**

**Content aggregators**

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

Malicious bots avoid detection by **altering User Agent, or other HTTP headers**; as well as **changing IP addresses**