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 attacks from January 2019 to September 2019 largely targeted the gaming industry

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

Financial Services accounted for almost 50% of unique targets for DDoS attacks.

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

The top phishing targeted companies are: Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn.

1. **What is credential stuffing?**

Credential stuffing is a type of cyberattack where stolen usernames and passwords are used to access user accounts at another organization.

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

The United States is the number one source of credential abuse attacks. Russia is number two.

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

The United States is the number one source of web application attacks. Russia is number two.

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.**

Akami noticed a customer in Asia was receiving an abnormal amount of traffic to on if its URL. They were seeing so much traffic that, it almost overflowed the database Akamai uses to log such activity.

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

At first, they believed it was a major DDoS attack.

* **What did the team actually discover?**

The team discovered that it wasn’t a DDoS attack but was the result of a watrranty tool gone haywire.

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

An example of a performance issue with bot traffic is that websites or the computer will run slower and increases IT expenses.

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.**

The main categories of known good bots is:

Search engine crawlers

Web archives

Search engine optimization, audience analytics, and marketing service

Site monitoring services

Content aggregators

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

The most common evasion technique malicious bots use is altering the User Agent header values, allowing the bot to impersonate widely used browsers, mobile applications, or even known-good bots. Another technique is that bots will also change the IP addresses used in order to mask their origin, or use multiple IPs.