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?**

* High Technology

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?**

* Media and Tech Companies

1. **What is credential stuffing?**

* Credential stuffing is similar to a brute force attack, but there are several important differences:
* Brute force attacks try to guess credentials with no context, using random strings, commonly used password patterns or dictionaries of common phrases
* Brute force attacks succeed if users choose simple, guessable passwords
* Brute force attacks lack context and data from previous breaches, and so their login success rate is much lower

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

* Number one country is: The United States
* Number two Country is: Russia

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

* The number one country is: The United States
* The number two country is: 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.**
  + A large amount of HTTP requests going to a customer’s URL led to the presumption that there was a possible attack.
* **What did the team believe the source of the attack was?**
  + A Windows Oriented Tool was responsible for the massive flood of requests
* **What did the team actually discover?**
  + SRIT concluded that the high amount of volume was not actually an attack

But the result of a warranty tool gone bad

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

* Examples are: Slow websites, frustrated customers and IT costs

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

What are two evasion techniques that malicious bots use?

* Altering the user agent or HTTP header values allowing the bot to impersonate widely used browsers, mobile applications or known “good bots”.
* Another technique is to change the IP Address or use multiple IP Addresses in order to mask their origin