# 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 from January 2019 to September 2019 largely targeted the Gaming industry with over 3000 attacks in the stretch of time.

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

* Unique targets for DDoS attacks from January 2019- to September 2019 largely targeted the Financial Services industry.

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

* Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn are all top phishing targets, according to Akamai’s monitoring.

1. What is credential stuffing?

* Type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames and/or email addresses

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

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

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

* The number one source of credential abuse attacks is the United States and number two 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.
* 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?
* Initial analysis showed that half of the IPs were flagged by Akamai as NAT gateways. Additional packet and header analysis confirmed the traffic in question was generated by a Windows COM Object (WinhttpRequest).
* What did the team actually discover?
* By the time SIRT had finished their work, and the SOCC had things under control, everyone involved realized the incident wasn’t an attack at all. Earlier analysis, backed by additional SIRT research, concluded the high volume of traffic hammering this customer’s URL was the result of a warranty tool gone haywire.

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

* slow websites and frustrated customers

1. Known-good bots are bots that perform useful or helpful tasks and do not do anything malicious to sites or servers. What are the main categories of known-good bots?

* Chatbots
* Crawlers
* Transactional bots
* Informational bots
* Entertainment bots: Art bots, Game bots

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

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