# 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?

The financial services has largely been the DDoS attack target between January 2019 to September 2019 **(Akamai’s Security Year In Review Pg. 9)**

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

“Half of all unique organizations impersonated by phishing domains were in the financial services sector, according to Akamai data.” **(Akamai’s Security Year In Review Pg. 10)**

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

According to Akamai, the top phishing targets were, “Microsoft, Paypal, DHL, and Dropbox.”([Akamai Security Research: Cybercriminals Using Enterprise-Based Strategies For Phishing Kit Development And Deployment](https://www.akamai.com/us/en/about/news/press/2019-press/state-of-the-internet-security-phishing-baiting-the-hook.jsp))

1. What is credential stuffing?

“Credential stuffing is a cyber attack in which credentials obtained from a data breach on one service are used to attempt to log in to another unrelated service.” (<https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/>)

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

The United States is #1 in credential abuse attacks and Russia comes in #2. **(Akamai’s Security Year In Review Pg. 16,17)**

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

Again, the United States comes in as #1 for web application attacks, and Russia comes in #2. **(Akamai’s Security Year In Review Pg. 20,21)**

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.
* What did the team believe the source of the attack was?
* What did the team actually discover?

a. In “Early 2018, Akamai noticed a customer in Asia was receiving an abnormal amount of traffic to one of it’s URL’s. The initial spike in traffic was so large - more than 4 billion requests - it almost crashed the logging system.” **(Akamai’s State of the Internet Report Pg. 11 and Figure 11)**

b. Akamai’s “Initial analysis showed that half of the IP’s 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). **(Akamai’s State of the Internet Report Pg. 13)**

c. The SIRT team discovered that it was just bad code that caused a DOS (Denial of Service) on the customers website that was picked up by Akamai. “Earlier analysis backed by additional SIRT research, concluded the high volume of traffic hammering the customers URL was the result of a warranty tool gone haywire.” **(Akamai’s State of the Internet Report Pg. 14)**

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

There are both good and bad bot’s. Here are 2 examples of bad bot’s. The first could be one that is designed to slow down or crash a website, DOS attack. The second could be a bot that is now being used at this time to purchase all of the GPU’s from all vendors on the day they go on sale.

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 bot's?

The main categories for good bot’s are: “Search Engine Crawlers, Web Archives, Search Engine Optimization, Audience Analytics,Marketing, Site Monitoring Services, and Content Aggregators.” **(Akamai’s State of the Internet Report Pg. 16)**

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

Here is an example of two evasion techniques that a malicious bot can use:

First, a bot can “change the IP address used in order to mask their origin.” A second one could be that a “bot that will tamper with browser properties, spoofing known fingerprint characteristics that are often whitelisted.” **(Akamai’s State of the Internet Report Pg. 17, 18)**