# 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?**According to Akamai (A year in Review, 2019, pg.12) the industry that was mostly targeted by DDOS attacks was Gaming.
2. **Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?**According to Akamai (A year in Review, 2019, pg.12) the industry targeted the most for unique DDOS attacks was financial services.
3. **Which companies are the top phishing targets, according to Akamai?**According to Akamai (A year in Review, 2019, pg.14) the top companies targeted for Phishing attacks are; Microsoft, Paypal, DHL, Dropbox, DocuSign, and LinkedIn.
4. **What is credential stuffing?**Credential stuffing is a new form of attack that automates the injection of breached username and password pairs to gain fraudulent access to an account. It is a subset of a brute force attack where large numbers of leaked credentials are entered into a website until a match is found and the attacker gains control of the account.  
   (Credential stuffing Software Attack | OWASP Foundation, 2021)
5. **Which country is the number one source of credential abuse attacks? Which country is number 2?**According to Akamai (A year in Review, 2019, pg.18,19) the United states was the number 1 country for credential abuse at 25,393,327,336 malicious logins and Russia was the number 2 country sitting at 6,114,186,048 malicious logins.
6. **Which country is the number one source of web application attacks? Which country is number 2?**According to Akamai (A year in Review, 2019, pg.22,23) the United States was the number 1 for web application attacks at 1,434,231,212 attacks, the number 2 was Russia at 1,093,219,355 attacks
7. **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?**In 2018 Akamai noticed a customer originating in Asia was receiving an abnormal amount of traffic to one of the URLs, so much so that it almost overflowed the Akamai database used to log such activity. Traffic volume had reached 875000 requests per second at one point and was showing all the signs of a DDoS attack.  
    
  Initially Akamai thought the Source of the attack was a targeted DDoS attack targeted at the customer in asia, after viewing the logs they could see that many IPs that approached the customers URL a few days prior to the event with similar “attack” features, the URL went from 643 requests to over 4 billion in less than a week.  
    
  The team in the SOCC, over the course of 28 hours, mitigated over 4 billion requests from 15,582 IP addresses. Once the SOCC had things under control they had realized that the event wasn’t an attack at all but in fact a warranty tool going haywire, the tool in question tool kept visiting the URL but the subsequent visits didn’t alter anything that could’ve assisted in bypassing the mitigations thus proving it wasn’t a malicious attack.  
  (The state of the Internet, 2019, pg.11-14)

1. **What is an example of a performance issue with bot traffic?**An example of bot traffic performance issues is slow websites that invariably result in frustrated customers.  
   (The state of the Internet, 2019, pg.16)
2. **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.**According to Akamai (The state of the Internet, 2019, pg.16) the main categories of Good Bots are as follows;
   1. Search engine crawlers.
   2. Web archives.
   3. Search engine optimization, audience analytics and marketing service.
   4. Site monitoring services.
   5. Content aggregators.
3. **What are two evasion techniques that malicious bots use?**   
   According to Akamai (The state of the Internet, 2019, pg.17,18) Two examples of evasion techniques that bots use are altering the user agent or other HTTP header values allowing the bot to impersonate other applications or good bots, Bots will also change the IP used to mask their origin and can even use multiple IPs, this can also be used to bypass rate limitations.

**Bibliography**

2019. *A year in Review*. Akamai, pg.12,14,18,19,22,23.

Owasp.org. 2021. *Credential stuffing Software Attack | OWASP Foundation*. [online] Available at: <<https://owasp.org/www-community/attacks/Credential_stuffing>>.

2019. *The state of the Internet*. Akamai, pg. 11-14,16-18.