

## 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?  
Gaming
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?  
Financial services
3. Which companies are the top phishing targets, according to Akamai?  
Microsoft, PayPal, DHL, DropBox, DocuSign, and LinkedIn
4. What is credential stuffing?  
Credential stuffing is when a cyberattacker uses the stolen login credentials of a victim to get into their account, largely through weak and recycled passwords.
5. Which country is the number one source of credential abuse attacks? Which country is number 2?  
United States is first, while Russia is second
6. Which country is the number one source of web application attacks? Which country is number 2?  
United States is first, while Russia is second
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.  
Akamai noticed that a customer in Asia was receiving so much traffic to one of its URLs that at its peak, it almost overflowed the log database that Akamai uses. It

looked just like a DDoS attack. A large amount of HTTP requests were going to the customer's URL.

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

A windows-oriented tool doing a DDoS attack

- What did the team actually discover?

They discovered it was not an attack at all. The heavy traffic on the customer's URL was the result of a warranty tool gone haywire. It was fixed within hours.

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

Slow websites

9. 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, and marketing service, site monitoring services, and content aggregators

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

Altering the user agent and changing the IP address or using multiple of them