Sasha Shahidi

Cybersecurity Threat Landscape (Part 3 - Verizon)

In this part, you should primarily use the *Verizon Data Breaches Investigation Report* plus independent research to answer the below questions.

---

1. What is the difference between an incident and a breach?
   An incident is a security event where an asset's confidentiality, integrity, and availability are compromised, whereas a breach is when the aforementioned incident causes the disclosure of data to its party.

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?
   69% by outside actors and 34% by internal actors

3. What percentage of breaches were perpetrated by organized criminal groups?
   39%

4. What percentage of breaches were financially motivated?
   71%

5. Define the following:

   Denial of Service: A cyber attack in which a cybercriminal works to turn a system unusable by overwhelming a system with requests so that the normal process cannot occur (cloudflare.com)

   Command and Control: A cyber attack in which a cybercriminal puts malware on a system and sends commands to obtain stolen data (trendmicro.com)

   Backdoor: The process of bypassing typical security processes to gain root access on a system to possibly steal data or insert malware (malwarebytes.com)

   Keylogger: A software made to monitor and obtain keystrokes entered by a user, where data typed into a website is obtained and used thereafter (csoonline.com)

6. The time from an attacker's first action to the initial compromise of an asset is typically measured in which one? Seconds, minutes, hours, days?
   Minutes

7. When it comes to phishing, which industry has the highest click rates?
   Education