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 that compromises the integrity, confidentiality or availability of an information asset. An Breach is an incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party.

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?

   80 percent of breaches were perpetrated by outside actors from 2011 to 2018.

   35 percent of the breaches were perpetrated by internal actors from 2011 to 2018.

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

   In 2011, 75 percent of breaches were perpetrated by organized criminal groups, then decreasing thereafter, only to reach its peak at 80 percent in 2015 then falling off again.
4. What percentage of breaches were financially motivated?

   Financially motivation accounted for 85 percent of the breaches in 2011, then fell off only to reach a peck in 2015 at 80 percent.

5. Define the following:

   Denial of Service: Threat seeks to make a machine or network resource unavailable to its internet users by temporarily or indefinitely disrupting services of hosts connected to the internet.

Command and Control:

A server computer controlled by an attack or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.

Backdoor:

A backdoor is a malware type that negates normal authentication procedures to access a system.

Keylogger:

Is an action of recording the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

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?

   The time from the attacker’s first action in an event chain to the initial compromise of an asset is typically measured in minutes.

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

   The industry that has the highest click rates is education.