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? - Think of a security incident as a pesky cold that may sideline you for a couple of days. This could be anything from a misplaced drive to missing paper files. A breach is the nastiest flu bug ever. Source:

https://www.spartantec.com/2016/12/07/whats-the-difference-between-a-breach-and-security-incident/

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors? - Outside: 69%, Internal: 34%

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: is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

   Source:

https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

Command and Control - (found in both security incidents and breaches) (most common functionality - 47% in incidents.) a C&C server is a computer controlled by an attacker of cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network. Many campaigns have been found using cloud-based services, such as webmail and file-sharing services, as C&C servers to blend in with normal traffic and avoid detection.

Source:

https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server

Backdoor - typically a covert method of bypassing normal authentication or encryption in a computer. Most often used for securing remote access to a computer, or obtaining access plaintext in cryptographic systems

Source:

https://en.wikipedia.org/wiki/Backdoor_(computing)

Keylogger - software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored. A type of spyware.

Source:

https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger/

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.

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