# 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?  **Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.**

**Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party (pg 2)**

1. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?   
   **- 69% Outside actors**

**-34% Internal Actors (pg 5)**

1. What percentage of breaches were perpetrated by organized criminal groups?   
   **-39% by organized Criminal Groups (pg 5)**
2. What percentage of breaches were financially motivated?   
   **- 71% of breaches were financially motivated (pg 5)**
3. Define the following:   
     
   Denial of Service: **A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.**

<https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/>

Command and Control**: A command-and-control [C&C] server is a computer controlled by an**[**attacker**](https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf)**or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network. It can be used to disseminate commands that can steal data, spread malware, disrupt web services, and more.**

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

Backdoor: **A backdoor is a**[**malware type**](https://www.imperva.com/learn/application-security/malware-detection-and-removal/)**that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.**

**Backdoor installation is achieved by taking advantage of**[**vulnerable**](https://www.imperva.com/learn/application-security/vulnerability-management/)**components in a web application. Once installed, detection is difficult as files tend to be highly obfuscated.**

<https://www.imperva.com/learn/application-security/backdoor-shell-attack/>

Keylogger: **A keylogger is an insidious form of**[**spyware**](https://home.sophos.com/en-us/content/best-spyware-removal.aspx)**. You enter sensitive data onto your keyboard, believing nobody is watching. In fact, keylogging software is hard at work logging everything that you type.**

**Keyloggers are activity-monitoring software programs that give hackers access to your personal data. The passwords and credit card numbers you type, the webpages you visit – all by logging your keyboard strokes. The software is installed on your computer, and records everything you type. Then it sends this log file to a server, where cybercriminals wait to make use of all this sensitive information.**

<https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger.aspx>

1. 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?   
   **However, the time from the attacker’s first action in an event chain to the initial compromise of an asset is typically measured in minutes. Conversely, the time to discovery is more likely to be months. (pg 19)**
2. When it comes to phishing, which industry has the highest click rates?  
   **Education-4.93%**