# 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 talks about an event that compromises the CIA of an asset  
   -A Breach is an incident that results in the confirmed disclosure (as opposed to potential exposure) of data to an unauthorized party. (Verizon, 2019, pg.2)
2. **What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?**   
   According to the summary of findings of the Data breach investigations report (Verizon, 2019, pg.5) 69% of all breaches are perpetrated by outsiders and 39% by internal actors.
3. **What percentage of breaches were perpetrated by organized criminal groups?**   
   According to the summary of findings of the Data breach investigations report (Verizon, 2019, pg.5) organized criminal groups were behind 39% of breaches.
4. **What percentage of breaches were financially motivated?**   
   According to the summary of findings of the Data breach investigations report (Verizon, 2019, pg.5) 71% of breaches were financially motivated.
5. **Define the following:**   
     
   **Denial of Service:** An attack that is intended to compromise the availability of any network or system. Designed to overwhelm systems which results in performance degradation or interruption of service. Can include both network and application attacks. (Data Breach Investigations Report, 2019, pg.25)  
    **Command and Control:** A type of Crimeware that may not fit into a specific pattern and is most likely opportunistic in nature and financially motivated (Data Breach Investigations Report, 2019, pg.25)  
   Command and control (or C2) is a set of tools that is used to maintain communication to a compromised machine after initial attack, it will keep one or more channels of secret communication to a device in which the attacker controls.  
   (What is C2? Command and Control Infrastructure Explained | Varonis, 2021) **Backdoor:** A backdoor is a method for a hacker to attack a system remotely without your knowledge. This is done by malware being installed onto your device to create the backdoor, nobody is safe from this kind of attack since new forms of malware are constantly being made.  
   (What Is a Backdoor & How to Prevent Backdoor Virus Attacks in 2021, 2021) **Keylogger:** A keylogger is a type of surveillance technology, either hardware or software, used to steal PII (Personally Identifiable Information) by monitoring and recording keystrokes.  
   (What is a Keylogger? How Do Keystroke Loggers Work?, 2021)
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?**According to theData breach investigations report (Verizon, 2019, pg.19) the first action 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?**  
   According to theData breach investigations report (Verizon, 2019, pg.32) the industry that has the highest click rates in regards to phishing is Education sitting at 4.93%.

**Bibliography**

2019. *Data Breach Investigations Report*. Verizon, pg.2, 5, 19, 25, 32.

SafetyDetectives. 2021. *What Is a Backdoor & How to Prevent Backdoor Virus Attacks in 2021*. [online] Available at: <<https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/>>.

SearchSecurity. 2021. *What is a Keylogger? How Do Keystroke Loggers Work?*. [online] Available at: <<https://searchsecurity.techtarget.com/definition/keylogger>>.

Inside Out Security. 2021. *What is C2? Command and Control Infrastructure Explained | Varonis*. [online] Available at: <<https://www.varonis.com/blog/what-is-c2/>>.