# Security 101 Homework: Cybersecurity Threat Landscape

# Part 3: *Verizon Data Breaches Investigation Report*

In this part, 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.

1. What percentage of breaches were perpetrated by outside actors? - 80% What percentage were perpetrated by internal actors? - 20%

1. What percentage of breaches were perpetrated by organized crime? - 80%
2. What percentage of breaches were financially motivated? - Over 75%

1. Define the following (Additional research may be required outside of the report):   
     
   Denial of Service:   
    **An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.** "a recent spate of denial of services attacks against e-commerce sites"

Command and Control:

**Malicious network attacks have been on the rise in the last decade. One of the most damaging attacks, often executed over DNS, is accomplished through command and control, also called C2 or C&C.**

The attacker starts by infecting a computer, which may sit behind a firewall. This can be done in a variety of ways:

* Via a phishing email that tricks the user into following a link to a malicious website or opening an attachment that executes malicious code.
* Through security holes in browser plugins.
* Via other infected software.

Once communication is established, the infected machine sends a signal to the attacker’s server looking for its next instruction. The infected computer will carry out the commands from the attacker’s C2 server and may install additional software. The attacker now has complete control of the victim’s computer and can execute any code. The malicious code will typically spread to more computers, creating a botnet – a network of infected machines. In this way, an attacker who is not authorized to access a company’s network can obtain full control of that network.

**What Can Hackers Accomplish Through Command and Control?**

1. **Data theft.** Sensitive company data, such as financial documents, can be copied or transferred to an attacker’s server.
2. **Shutdown.** An attacker can shut down one or several machines, or even bring down a company’s network.
3. **Reboot.** Infected computers may suddenly and repeatedly shutdown and reboot, which can disrupt normal business operations.
4. **Distributed denial of service.** DDoS attacks overwhelm server or networks by flooding them with internet traffic. Once a botnet is established, an attacker can instruct each bot to send a request to the targeted IP address, creating a jam of requests for the targeted server. The result is like traffic clogging a highway – legitimate traffic to the attacked IP address is denied access. This type of attack can be used take a website down.

Backdoor:

What is a backdoor attack? In general terms, a backdoor attack is a type of breach where hackers install malware that can surpass a network's normal security requirements and authentication by deceit and proper hiding.  
Keylogger:

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program.

1. What remains one of the most sought-after data types for hackers? - Credentials
2. What was the percentage of breaches involving phishing? - 35%