By: Zabien McKee

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?**

An incident is anything that is beyond normal operations, such as a Two Factor Authentication notice for a signin that you did not perform. A breach is an incident that results in a loss, such as a phishing attempt leading to the exposure of User Data.

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

From reading the graph, it seems about 80% of all breaches occur by outside actors, while internal actors make up only 20%.

3. **What percentage of breaches were perpetrated by organized crime?**

About 85% of all breaches are performed by organized crime gangs.

4. **What percentage of breaches were financially motivated?**

   The graph displays roughly 90% of all breaches are motivated by financial gain, though it is a little tricky to read

5. **Define the following (Additional research may be required outside of the report):**

   Denial of Service:

   An attack that involves using millions of virtualized users to use a service at once in an attempt to make said service incredibly slow as it's now dealing with significantly more users, or more likely than not, take down the entire system.

   Command and Control:

   A kind of cyber attack that is often performed by a cyber criminal. The attack starts with a hacker or scammer infecting a computer, often via phishing or malicious plugins. The infected computer will then continue to perform cyber attacks against other machines on the network and try to create a bot-net. This kind of attack can bring down entire systems if not properly quarantined.

   Backdoor:

   Essentially a kind of "gateway" into a system that can either be found by a hacker or be purposely planted by one, often by leaving specific ports open on a computer which they can later access.

   Keylogger:

   A piece of malicious software that logs every single key stroke that is made on the computer. Often used by Social Engineering scammers acting as technical support to swipe login credentials, credit card numbers, and Personal Identifiable Information.

6. **What remains one of the most sought-after data types for hackers?**

Banking information. Most other assets require some sort of conversion before they turn into money by either selling or ransoming. Banking information is just money, no conversion required!

7. **What was the percentage of breaches involving phishing?**

Around 37% of all breaches are initially caused by phishing. It is one of the easiest ways to get into many systems, as it is essentially just playing a numbers game, you only need one user to click the link.