

Attacks in the digital age

With the expansion of reliable high-speed internet, the number of computers connected to the internet increased dramatically. Because malware could spread through the internet, threat actors no longer needed to use physical disks to spread viruses.

To better understand attacks in the digital age, we'll discuss two notable attacks that relied on the internet: the LoveLetter attack and the Equifax breach.

In the year 2000, Onel De Guzman created the LoveLetter malware to steal internet login credentials. This attack spread rapidly and took advantage of people who had not developed a healthy suspicion for unsolicited emails. Users received an email with the subject line, "I Love You." Each email contained an attachment labeled, "Love Letter For You." When the attachment was opened, the malware scanned a user's address book. Then, it automatically sent itself to each person on the list and installed a program to collect user information and passwords. Recipients would think they were receiving an email from a friend, but it was actually malware. The LoveLetter ended up infecting 45 million computers globally and is believed to have caused over \$10 billion dollars in damages. The LoveLetter attack is the first example of social engineering.

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

After the LoveLetter, attackers understood the power of social engineering. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Many people are now prioritizing convenience over privacy. The trade-off of this evolving shift is that these tools may lead to increased vulnerability, if people do not use them appropriately.

As a security professional, your role is to identify and manage inappropriate use of technology that may place your organization and all the people associated with it at risk. One way to safeguard your organization is to conduct regular internal trainings, which you as a future security analyst may be asked to lead or participate in.

Today, it's common for employees to receive training on how to identify social engineering attacks. Specifically, phishing through the emails they receive. Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Now, let's discuss the Equifax breach. In 2017, attackers successfully infiltrated the credit reporting agency, Equifax. This resulted in one of the largest known data breaches of sensitive information. Over 143 million customer records were stolen, and the breach affected approximately 40% of all Americans.

The records included personally identifiable information including social security numbers, birth

dates, driver's license numbers, home addresses, and credit card numbers. From a security standpoint, the breach occurred due to multiple failures on Equifax's part. It wasn't just one vulnerability that the attackers took advantage of, there were several. The company failed to take the actions needed to fix multiple known vulnerabilities in the months leading up to the data breach.

In the end, Equifax settled with the U.S. government and paid over \$575 million dollars to resolve customer complaints and cover required fines.

While there have been other data breaches before and after the Equifax breach, the large settlement with the U.S. government alerted companies to the financial impact of a breach and the need to implement preventative measures.

These are just a couple of well-known incidents that have shaped the security industry. Knowing about them will help you in your security career. Understanding different types of malware and social engineering attacks will allow you to communicate about security risks during future job interviews.

As a future security professional, constantly adapting and educating yourself on threat actors' tactics and techniques will be a part of your job. By noticing similar trends, patterns, and methodologies, you may be able to identify a potential breach and limit future damage.

Finally, understanding how security affects people's lives is a good reminder of why the work you will do is so important!

Revision #1

Created 30 May 2023 21:55:58 by naruzkurai

Updated 30 May 2023 21:56:57 by naruzkurai