Common Types of Attack

Brought to you by Assemble You.

It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

Nowadays, most of our work involves the Internet, making us vulnerable to bad actors and invisible enemies.

These enemies conduct cyberattacks – sometimes on networks and systems,but adversaries have discovered it's much easier to hack a human. Today, we'll discuss some of those attacks, as well as how to protect ourselves against them.

PurpleSec researchers discovered that in the United States alone in **2019**, **164.68 million** sensitive records were exposed through **1473 attacks**. The average cost of a data breach resulting from these attacks was **$3.92 million**. Hacking is big business, and - directly or indirectly - we're all potential victims.

There's a very high chance your passwords have been compromised in data breaches. Hackers sell this data, use it to conduct social engineering attacks, and even use it for identity theft. In fact, in 2020, consumers lost over 56 BILLION dollars to identity theft.

Hackers conduct cyber attacks to steal information, sabotage one or more systems, or bring down a working network. They can also attack several systems at once, gain control, and use these systems to initiate another attack on a different network altogether. Hackers conduct various types of attacks, but today we'll focus on:

- social engineering
- malware
- ransomware
- distributed denial of service
- Man-in-the-middle (MITM) attacks

- insider threats
- credential reuse
- And mobile attacks

So, let's begin with social engineering attacks. Cybersecurity expert Bruce Schneier once said, ***"Amateurs hack systems; professionals hack people."*** You may feel that your data is safe once you've activated firewalls and downloaded antivirus software, but you'd be wrong. Hackers can bypass your defenses by taking a non-digital approach. In his book *Secrets and Lies: Digital Security in a Networked World,* Schneier says

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."

Hackers use diverse methods to trick subjects into acting. Once the action is performed, they have a way into a system or a network. From there, they are free to steal confidential and sensitive information.

Phishing utilizes email and is the most common social engineering attack. For example, it involves an attacker, masquerading as a trusted entity, duping a victim into opening an email, instant message, or text message. The email often contains links to trick the recipient into providing personal information, such as a password, credit card number, or social security number.

Then, the next attack is **malware**.
Malware is a portmanteau, a combination of the words – "malicious" and "software." It's malicious software that is designed to cause harm to a system. It could be simply deleting data or, even more perniciously, hiding like a spy in the system, monitoring our activities. It can capture your keystrokes and send them to the hacker who planted the malware in our system. This means that if we are entering a password somewhere, let's say in our online bank account, that person controlling the malware also gets to know it. Almost everything is visible to the hacker, including our data, confidential files, photographs.

After **malware**, the next one is **ransomware**.
Hackers can encrypt our files using ransomware and demand a ransom. They encrypt the files, which then can only be decrypted with a decryption key. Even if the ransom is paid, the hacker may not decrypt the files.

This type of attack is more common on individuals but still happens to organizations. According to heimdalsecurity.com, 37% of the organizations were hit by ransomware. Of those, 32% paid the ransom to get their data back, but they only retrieved 65% of the data.

The next one on the list is **Denial-of-Service**, commonly known as **DoS**.

DoS typically targets the webservers hosting a website. A webserver, by definition, is a server that hosts a website or a web application. Users connect to the website, such

as google.com, and access information. The hackers target the webserver, sending an enormous volume of malformed requests. The webserver attempts to handle these requests, but eventually, the load becomes too high. The webserver then runs out of processing power and memory and crashes. Legitimate users now can't access the site because the webserver is unavailable.

A single system conducts the DoS attack. It can be amplified when several hundred, thousands, or even millions of systems perform the attack against one or more web servers. This type of attack is known as Distributed Denial-of-Service (DDoS) attack. In 2007, a massive DDoS attack on Estonia was reported by ccdcoe.org. Around a million systems were used to conduct this attack.

The obvious question is: how did the hackers get a million systems to do this? The answer is malware - these were malware-infected systems controlled by hackers, these machines are collectively known at 'botnets'.

One type of attack you may not have heard of is **the man-in-the-middle (MITM) attack**. A **man-in-the-middle** attack is a general term for when a perpetrator positions themself in a conversation between a user and an application. They do it either to eavesdrop or to impersonate one of the parties.

The aim is to reveal personal information, such as usernames, passwords, credit card numbers, etc.
This does not have to be a person literally eavesdropping on a conversation, simply using an open Wi-Fi network would allow anyone on that network to perform an MITM attack. However, this is less frequent today due to the adoption of secure web standards such as HTTPS, the green padlock you see next to supported sites on your browsers.

Broadly speaking, a **man-in-the-middle** attack is the equivalent of a mailman opening your bank statement, writing down your account details, and then resealing the envelope and delivering it to your door.

Moving on, let's talk about **credential reuse**.
We all access several websites in a day. Some of them require us to log in. To do that, we must remember our usernames and passwords. Many of us are guilty of a particular mistake: we keep repeating the passwords from one website to another. When hackers hack one website or web application, they gain access to credentials. They then try the same credentials with other websites and web applications. In many cases, the hackers can match the usernames and passwords. It only takes one database breach and there are openly available tools for testing email/username password combinations against hundreds of sites to check for password reuse. While it only takes a few minutes to set up and properly configure a secure password manager across your devices, it takes hackers seconds to check if you've reused a password against many common sites.

Next up is the **insider threat**.

Once you've nailed your outward security, it's essential to remain aware of internal threats. These are often people who are either unhappy with the organization or are frustrated with their work. They can initiate the attack themselves or provide information to the people who initiate it. Tessian reports an increase of 47% insider threats between 2018 and 2020.

Last but not least is the **mobile attack**.
With the popularity of mobile devices, attacks have become equally common. Hackers target vulnerable mobile apps, and when they are used, they gain access to mobile devices to steal information. Hackers also post malicious fake apps into the app stores. Once users download and start using them, the hackers can access their mobile devices, allowing them access with more control than the end user of the device. One standard method is sending malicious links through SMS messages and letting the curious users click on those links. Once that happens, malware can be downloaded onto a mobile device.

Protecting Yourself
So, we have learned about several types of common attacks. But how do we safeguard ourselves?

The first method is **training**.
Everyone in an organization should undergo a basic level of security training. The user should be informed about social engineering, specifically phishing attacks. We don't need to make everyone a security expert, but fundamental knowledge can prevent many security breaches. For example, the users should never click on a link in an email or an SMS message sent by an anonymous person. This training should be refreshed on a schedule and as the threat landscape and you or your organization's exposure widens.

The next method involves **restricted access privileges**.
The users within an organization must be assigned permissions on a need-to-know basis. The users should never be allocated more access privileges than they need to have, as this minimizes the scope of any potential breach.

Another tactic you may be familiar with is **multi-factor authentication.**
In most cases, hackers obtain the user credentials, which they later use to steal information. With multi-factor authentication in place, even if hackers get ahold of user credentials, they still require a PIN, One-time Password, or even a smart card, adding an extra layer of protection. Enable it wherever possible!

The penultimate list entry is called **Defense-in-Depth**.
This just refers to the principle of having multiple layers of security implemented. A solid example might be the combination of a firewall, an anti-malware application, and restricted privileges.

Finally, let's discuss **security policies**.

Organizations need well-designed IT security policies to ensure the success of their cyber-security strategies and efforts. Security policies should focus on passwords, training, and infrastructure. For example, a password policy should drive the users to use complex passwords and change them after a certain number of days. Other important policies involve the protection of data, such as storing/exchanging confidential information on portable drives and ensuring the security of your workstations and laptops.

Equally as important as the policies are their actual enforcement and verification. An IT security policy is worth nothing if it's not followed.

So, that's a lot to mull over. The threat of bad actors online is genuine. Still, thankfully - with the help of the techniques outlined today - you can significantly reduce risk.

This week, update your accounts to make use of multi-factor authentication and consider getting a password manager such as LastPass. It can feel like too much extra effort, but it's certainly worth doing to protect sensitive personal and professional data.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] Top Cyber Attacks In History | Biggest Cyber Attacks Of All Time | Cyber Security | Simplilearn
- [Video] 5 Most Devastating Cyber Attacks | Cybersecurity Insights #18
- [Video] How could cyber attacks affect you?
- [Article] Common Types of Cybersecurity Attacks
- [Article] More and More Companies Are Getting Hit with Ransomware [2021-2022]
- [Article] Man-in-the-middle (MITM) Attack, Imperva
- [Article] Consumers lost $56 billion to identity fraud last year—here's what to look out for, M. Leonhart