Malware Attacks

Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge

Cyber attackers create, use and sell malware for many different reasons, but it is most frequently used to steal personal, financial or business information. While their motivations vary, cyber attackers nearly always focus their tactics, techniques and procedures (TTPs) on gaining access to privileged credentials and accounts to carry out their mission.

Types of Malware Attacks

Most malware types can be classified into one of the following categories:

- **Virus:** When a computer virus is executed, it can replicate itself by modifying other programs and inserting its malicious code. It is the only type of malware that can "infect" other files and is one of the most difficult types of malware to remove.
- **Worm:** A worm has the power to self-replicate without end-user involvement and can infect entire networks quickly by moving from one machine to another.
- **Trojan:** Trojan malware disguises itself as a legitimate program, making it one of the most difficult types of malware to detect. This type of malware contains malicious code and instructions that, once executed by the victim, can operate under the radar. It is often used to let other types of malware into the system.
- **Hybrid malware:** Modern malware is often a "hybrid" or combination of malicious software types. For example, "bots" first appear as Trojans then, once executed, act as worms. They are frequently used to target individual users as part of a larger network-wide cyber attack.
- **Adware:** Adware serves unwanted and aggressive advertising (e.g., pop-up ads) to the end-user.
- **Malvertising:** Malvertising uses legitimate ads to deliver malware to end-user machines.
- **Spyware:** Spyware spies on the unsuspecting end-user, collecting credentials and passwords, browsing history and more.
- **Ransomware:** **Ransomware** infects machines, encrypts files and holds the needed decryption key for ransom until the victim pays. Ransomware attacks targeting enterprises and government entities are on the rise,

costing organizations millions as some pay off the attackers to restore vital systems. Cyptolocker, Petya and Loky are some of the most common and notorious families of ransomware.

Examples of Malware Attacks

Here are just a few of the many types of malware cyber attackers use to target sensitive data:

- **Pony malware** is the most commonly used malware for stealing passwords and credentials. It is sometimes referred to as Pony Stealer, Pony Loader or FareIT. Pony malware targets Windows machines and collects information about the system and the users connected to it. It can be used to download other malware or to steal credentials and send them to the command and control server.
- **Loki**, or Loki-Bot, is an information-stealing malware that targets credentials and passwords across approximately 80 programs, including all known browsers, email clients, remote control programs and file sharing programs. It has been used by cyber attackers since 2016 and continues to be a popular method for stealing credentials and accessing personal data.
- **Krypton Stealer** first appeared in early 2019 and is sold on foreign forums as malware-as-a-service (MaaS) for just $100 in cryptocurrency. It targets Windows machines running version 7 and above and steals credentials without the need for admin permissions. The malware also targets credit card numbers and other sensitive data stored in browsers, such as browsing history, auto-completion, download lists, cookies and search history.
- **Triton malware** crippled operations at a critical infrastructure facility in the Middle East in 2017 in one of the first recorded malware attacks of its kind. The malware is named after the system it targets – Triconex safety instrumented system (SIS) controllers. These systems are used to shut down operations in nuclear facilities, oil and gas plants in the event of a problem, such as equipment failure, explosions or fire. The Triton malware is designed to disable these failsafe mechanisms, which could lead to physical attacks on critical infrastructure and potential human harm.

How to Prevent Malware Attacks

To strengthen malware protection and detection without negatively impacting business productivity, organizations often take the following steps:

- ✓ Use anti-virus tools to protect against common and known malware.
- Utilize endpoint detection and response technology to continuously monitor and respond to malware attacks and other cyber threats on end-user machines.
- Follow application and Operating System (OS) patching best practices.
- Implement the **principle of least privilege** and **just-in-time access** to elevate account privileges for specific authorized tasks to keep users productive without providing unnecessary privileges.
- Remove local administrator rights from standard user accounts to reduce the attack surface.
- Apply application greylisting on user endpoints to prevent unknown applications, such as new ransomware instances, from accessing the Internet and gaining the read, write and modify permissions needed to encrypt files.
- Apply application whitelisting on servers to maximize the security of these assets.
- Frequently and automatically backup data from endpoints and servers to allow for effective disaster recovery.

Password attacks

Password cracking is one of the imperative phases of the hacking framework. Password cracking is a way to recuperate recover passwords from the information stored or sent by a PC or mainframe..

Types of Password Attacks :

Password cracking is consistently violated regardless of the legal aspects to secure from unapproved framework access, for instance, recovering a password the customer had forgotten etc.

Non-Electronic Attacks –

This is most likely the hacker's first go-to to acquire the target system password. These sorts of password cracking hacks don't need any specialized ability or information about hacking or misuse of frameworks. Along these lines, this is a non-electronic hack. A few strategies used for actualizing these sorts of hacks are social engineering, shoulder surfing, and so forth.

1. **Active Online Attacks –**

   This is perhaps the most straightforward approach to acquire unapproved manager-level mainframe access. To crack the passwords, a hacker needs to have correspondence with the objective machines as it is obligatory for password access. A few techniques used for actualizing these sorts of hacks are word reference, brute-forcing, password speculating, hash infusion, phishing, LLMNR/NBT-NS Poisoning, utilizing Trojan/spyware/keyloggers, and so forth.

2. **Passive Online Attacks** –
   An uninvolved hack is a deliberate attack that doesn't bring about a change to the framework in any capacity. In these sorts of hacks, the hacker doesn't have to deal with the framework. In light of everything, he/she idly screens or records the data ignoring the correspondence channel to and from the mainframe. The attacker then uses the critical data to break into the system. Techniques used to perform passive online hacks incorporate replay attacks, wire-sniffing, man-in-the-middle attack, and so on.
3. **Offline Attacks** –
   Disconnected hacks allude to password attacks where an aggressor attempts to recuperate clear content passwords from a password hash dump. These sorts of hacks are habitually dreary yet can be viable, as password hashes can be changed due to their more modest keyspace and more restricted length. Aggressors utilize preprocessed hashes from rainbow tables to perform disconnected and conveyed network hacks.

Some of the best practices protecting against password cracking include :

1. Perform data security reviews to screen and track password assaults.
2. Try not to utilize a similar password during the password change.
3. Try not to share passwords.
4. Do whatever it takes not to use passwords that can be found in a word reference.
5. Make an effort not to use clear content shows and shows with weak encryption.
6. Set the password change technique to 30 days.
7. Try not to store passwords in an unstable area.
8. Try not to utilize any mainframe's or PC's default passwords.
9. Unpatched computers can reset passwords during cradle flood or Denial of Service assaults. Try to refresh the framework.
10. Empower account lockout with a specific number of endeavors, counter time, and lockout span. One of the best approaches to

oversee passwords in associations is to set a computerized password reset.

11. Ensure that the computer or server’s BIOS is scrambled with a password, particularly on devices that are unprotected from real perils, for instance, centralized servers and PCs.

There are various ways cybercriminals conduct illicit activities. With the advancement in security technology, it has become challenging for them to deceive the security programs and attack the device. So, they are using the traditional technique in modern ways to infiltrate the system. This technique is known as the Social Engineering attack.

In this post, we would discuss what Social Engineering attack is, how it is planned and performed, and how to prevent it from happening to you.

What is Social Engineering Attack

The Social Engineering attack is one of the oldest and traditional forms of attack in which the cybercriminals take advantage of human psychology and deceive the targeted victims into providing the sensitive information required for infiltrating their devices and accounts. It can also be called "human hacking."

Generally, cybercriminals take advantage of the security vulnerabilities of the system to infiltrate it and release malicious code. This may or may not require any human intervention. On the other hand, the Social Engineering attack needs human interaction to happen successfully.

Cybercriminals use various illicit techniques to get inside of the victims' heads and force them into revealing sensitive information. They create a sense of fear or urgency so that the victims do not get time to think about their actions.

A typical example of a Social Engineering attack is the fake jackpot offers or fake virus alerts sent through email. Almost every internet or email user might have encountered email titles **"Congratulations! You have won a lottery of $1 Miliion,"** or something similar. Such emails offer the unreal jackpot to the users, and for sending that jackpot, they ask for sensitive information in return. In anticipation and greed of getting the jackpot, many users provide all their info to the fraudster behind the fake email and thus become a victim of a Social Engineering attack.

How Does Social Engineering Work

Social Engineering is conducted by analyzing what victims would react if a fake alert or offer is presented before them. Conducting a Social Engineering attack is not a straightforward task. The attackers need to do extensive research on the company or the individual for knowing their psych.

Here is the lifecycle of the Social Engineering attack;

- The first step is to identify the victims and do background research to know how they can be psychologically exploited, and then plan a suitable attack.
- Now the attacker would try to engage the victim in conversation or send him some small genuine offers. This is done to gain the trust of the victim.
- After gaining the trust of the victim, the intruder would now gain the sensitive information of the victims by promising them more rewards or similar thing. The victims would willingly provide their information in the sense of greed, urgency, or fear, depending on the situation.
- In this stage, the cyber attacker would finally perform the Social Engineering attack using the information gathered in the previous step.
- Finally, after fulfilling the attack, the cybercriminals would remove all their traces and discontinue their interactions with the victims.

How to Prevent Social Engineering Attack

As it is clear by now, a Social Engineering attack can be pretty dangerous. However, by being attentive and not getting into the tricks of cyberattackers, you can easily stay away from it. Here are some preventive tips –

- **Never share your confidential information with anyone:** No genuine or reputed organization would ask for your personal information on the call or email.
- **Verify the tempting offers:** Maximum users become victims of a Social Engineering attack because they are tempted to unreal offers and go for them without verifying their authenticity.
- **Use Multifactor Authentication on all your accounts:** If MFA is enabled, then even if the attackers get their hand on your credentials, your account would be secure.
- **Keep installed a robust security solution:** A security solution would prevent you from spam emails, phishing attacks, and other similar social engineering attacks.