Types of Cyber Attacks

A cyber attack is a type of attack that targets computer systems, infrastructures, networks or personal computer devices using various methods at hands.

There are many types of Cyber Attacks each capable of targeting a specific computer system for a variety of purposes. The type of Cyber Attacks currently known will be highlighted in this article.

The information in this article will be useful in the Science and Technology segment of the UPSC 2021.

Overview of Cyber Attacks

Depending on the context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society, or organizations, and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyberweapon.

A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system.

Methods of Cyber Attacks

There are many ways hackers can exploit, infiltrate or attack a computer system. Some of the well known techniques are given in the data below:

1. Malware

Malware is a form of application that performs nefarious activities. Some types of malware are designed to create access to networks, some to spy on credentials while others are simply used to cause disruption

Malwares can be used for extortion as well. An example of it can be found in Ransomware attacks of 2017 where a program was designed to encrypt the victim's files and then ask them to pay a ransom in order to get the decryption key.

Latest Update about Malware Attacks in India

- Mobile Security Report 2021 asserted that mobile malware attacks in India are on rise (845 percent increase) since October 2020.

2. Phishing

In Phishing, an attacker tricks an unsuspecting target into handing over valuable information, such as passwords, credit card details, etc.

An example of this is a message regarding One-Time Passwords (OTP). A hacker using a phishing method will send a clickable link where a user can submit their OTPs. Once the link is clicked a hacker will have access to the users personal information.

Phishing is the common form of cyber attack due to its effectiveness and simplistic execution pattern.

Latest Update about Phishing in India

- Indian Computer Emergency Response Team (CERT-In) released a public advisory to alert citizens against all attempts of phishing through fake domains, emails and text messages that promise registration for a jab against the pandemic.

3. Man-in-the-middle attack (MITM)

A man-in-the-middle attack (MITM) consists of a message interception between two parties in an attempt to spy on the targets.

Due to the advent of end-to-end encryption, MITM attacks have taken a dip in frequency of attacks. Such encryptions prevent third parties in intercepting or tampering data transmitted in the network. Whether the network is secure or not is hardly a factor.

4. Distributed Denial-of-Service (DDoS) attack

In a DDoS attack, an attacker floods a target server with traffic that will disrupt it. Since most servers cannot handle it, it may lead to services slowing down on the website and if it eventually crashes.

Unlike standard denial-of-service attacks, DDoS uses multiple compromised devices to bombard the target server, which sophisticated firewalls cannot respond to or are unable to.

Update about Distributed Denial-of-Service attack in India

In August 2020 the number of Distributed Denial of Service (DDoS) incidents in India hit a record high in terms of total DDOS packets, which were well in excess of 10 billion as per a study by global cyber security firm Radware

5. SQL Injection

This type of cyber attack targets specific SQL databases. These databases use SQL statements for data query. In case permissions are not set properly, a hacker can manipulate SQL queries into changing the data if not deleting them altogether.

6. Zero-day exploit

When cyber-criminals learn of a vulnerability in a frequently used software application they target users and organizations using the software to exploit it until a fix is available. This is called a Zero-day exploit.

7. DNS Tunnelling

A DNS Tunnelling provides attackers with a stable and consistent line of communication to the given target. The malware used will gather information as long as the DNS tunnelling is active. Chances are that firewalls won't be able detect such an attack.

Update about DNS Tunneling in India

India saw the highest number of domain name system or DNS attacks in 2020 with 12.13 attacks per organisation, even though the cost of attacks in the country decreased by 6.08% to ₹5.97 crores, said International Data Corporation or IDC's DNS Threat Report.

8. Business Email Compromise (BEC)

In a BEC attack, hackers target employees who have specific authority to finalize business transactions. They trick them into transferring money into an account belonging to the hacker.

BEC attacks are the most common, if not one of the most damaging attacks for a business firm.

9. Cryptojacking

Cryptojacking is used to target a computer in order to mine cryptocurrencies such as bitcoin. The hackers will be able to get all the cryptocurrency they can instead of the original owners. Cryptojacking is not so widely known but its severity cannot be underestimated.

10. Drive-by Attack

A website is loaded with a malware, and when a visitor happens to come across such a website their device is infected with the malware. The malware will steal valuable data or crash the system.