Cybersecurity threat

A Lethal Challenge ahead…

AUGUST 2019

Vittal Siddaiah
CEO

Genie Systems

Impossible is Nothing we are Only Limited by our Imagination and Perceptions

Cyber Threat

In early days the word cyber was used to refer to cybernetics – the science of knowing the control and drive of machines. Then it was followed by cyber positioned for computerized. The term cyberspace emerged to redefine an invented physical space that a few wanted to believe existed behind the electronic activities of computing devices.

Key ***terminologies*** referred in cybersecurity

1. Ransomware

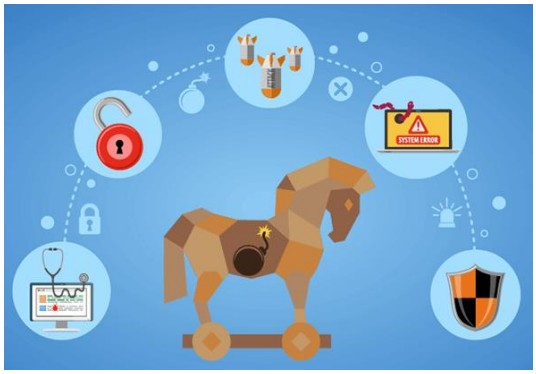
Ransomware is a type of malicious software which encrypts files on your computer or completely locks you out. It's spread by hackers who then demand a ransom, claiming that, if you pay, you'll receive the decryption key to recover your files.

Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 percent, indicating the established criminal groups are still quite productive, the number of ransomware families dropped, suggesting they are innovating less and may have shifted their focus to new, higher-value targets.

2. Spear Phishing

Spear phishing relies on tricking the recipient into opening an attachment or following a malicious link. The approach is typically termed Spray and Pray, targeting broad and automated. The victims could be a specific employee of a company or a company itself.

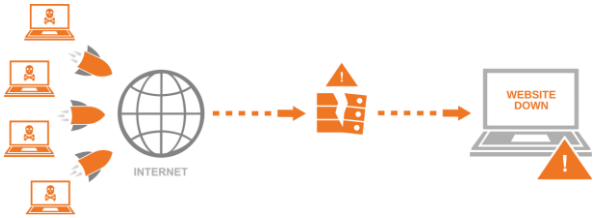
Spearfishing is one of the most common infection vectors; in other words, this is how the attacker manages to get to the victim's network in the first place. Its popularity shows how often the person sitting behind a computer can be the weakest link in an organization's security.



3. Trojan

A Trojan acts as an authentic application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designated. An attack directed at a specific target or targets as opposed to widescale indiscriminate campaigns. The work of individuals usually isn't classed as a targeted attack.

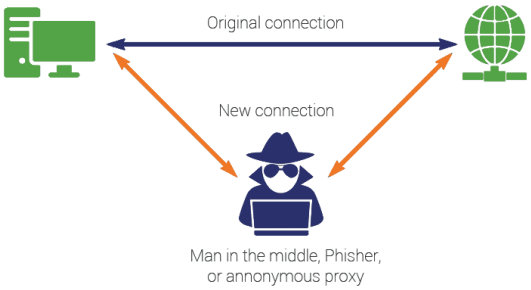
The motivation for a targeted attack is primarily an intelligence gathering. Other motives include disruption, sabotage, and financial gain.



4. DDoS Attacks

DDos, or distributed denial of service attack, This is a malware first creates a network of bots commonly termed as botnets, it then uses all the botnets to ping a single server at the same time.

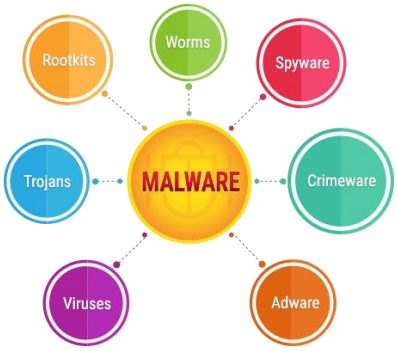
DDoS attacks can be a decoy for other more targeted attacks. Because admins will be busy trying to stem the DDoS attack, they may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway.



5.Man in the Middle Attack

An attack when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, and intercepts the communication without the knowledge of the victim.
The goal of an attack is to steal personal information, such as login credentials, account details, and credit card numbers.

If an attacker has control over a targeted network, for example by creating a rogue Wi-Fi access point, then they can attempt to swap any requested file update using a man-in-the-middle (MitM) attack



6. Malware

Malware is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions, and monitoring users' computer activity without their permission.

There has been a considerable rise in mobile malware as well as malware injection into supply chain attacks. It also continues to be one of the most essential tools used by targeted attack groups although many groups rely on it less than before malware is still generally used at the "pointy end" of any attack, to achieve the ultimate goal of the attack, whether it's information stealing, spying, sabotage, or any other kind of compromise.

7. Watering hole Attacks

Phishing is like giving random people poisoned candy and hoping they eat it, but a Watering Hole attack is like poisoning the village water supply and just waiting for them to drink from it.
A Watering Hole attack is a method in which the attacker seeks to compromise a specific group of end-users by infecting websites that members of that group are known to visit. The attacks are adopted by criminals, APT groups, and nation-states alike, and we see the amounts rising. The goal is to infect a victim's computer and gain access to the network within the victims' place of employment. Many conclude that these attacks are an alternative to Spear Phishing but are quite different.

Cybersecurity ***agent*** terminology

- *A **breach** is an incident that results in a confirmed disclosure. It is not just potential exposure of data to an unauthorized party.*
- *An **incident** is a security event that compromises the integrity, confidentiality, or availability of an information asset.*
- *An **incident report** is a report on the incident that occurred; the Incident report could be qualitative based on the authors' knowledge and perception.*
- *A **vulnerability** is a weakness in your security. Vulnerabilities expose the organization's assets. They exist in operating systems, applications, or hardware you use. How you configure software, hardware, and even email or social media accounts can also create vulnerabilities.*
- *An **exploit** commonly used to describe a software program that has been developed to attack a system by taking advantage of a vulnerability. The objective of many exploits is to gain control over the system. For example, a successful exploit of a database vulnerability can provide an attacker with the means to collect or exfiltrate all the records from that database.*