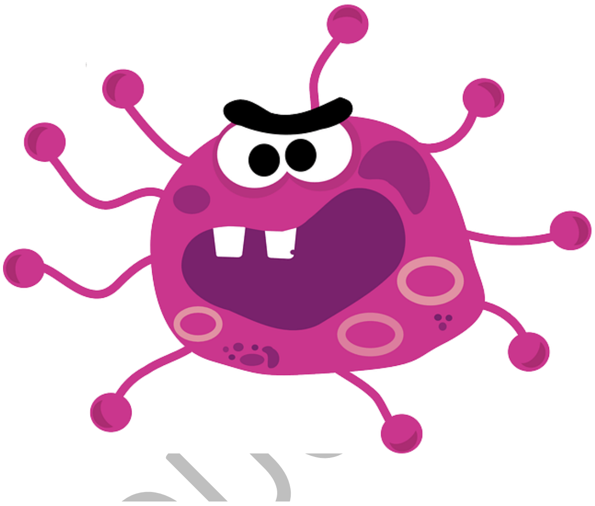
Unit 23. Malware Types- Virus, Worm, Trojan, Ransomware etc

Almost everyone is familiar with the term computer virus, but only a few might have heard about the term malware. A computer virus is a type of malware. Malware includes computer viruses, worms, Trojan horses, spyware, ransomware and many others. In this post, we analyse the different types of malware including the Wannacry, which is a form of ransomware.

What is a Malware?



- Malware is the shortened form of **malicious software**.
- Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software including Ransom wares, Computer Viruses, Worms, Trojan Horses, Spyware, Adware, Scareware etc.
- This is any program or file that is harmful to a computer user.
- The term refers to software that is deployed with malicious intent.
- Malware can be deployed even remotely, and tracking the source of malware is hard.
- It can take the form of executable code, scripts, active content, and other software.

- 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.
- This combination has enabled commercial malware providers to supply sophisticated black markets for both malware and the information that it collects.

Evolution of Malware

- Computer-enabled fraud and service theft evolved in parallel with the information technology that enabled it.
- The term malware was first used by computer scientist and security research **YisraelRadai in 1990**.
- Before the term malware, malicious software was referred to as computer viruses.
- One of the first known examples of malware was the **Creeper virus in 1971**, which was created as an experiment by BBN Technologies engineer Robert Thomas.

What is the purpose of creating a Malware?

- Initially, it started as a prank among software developers. However, later on, malware converted into a full-fledged industry of black and white market.
- It may be used by black hat hackers or even some governments for monitoring their targets.
- Demand for sophisticated malware is created primarily by organised crime syndicates and state-sponsored espionage agents.

Malware is typically used:

1. To steal information that can be readily monetized, such as login credentials, credit card and bank account numbers,
2. And intellectual property such as computer software, financial algorithms, and trade secrets.
3. To ransom money in Bitcoin, for example, Wannacry Ransomware.
4. Spy on computer users for an extended period without their knowledge, for example, Reign Malware.
5. It may be designed to cause harm, often as sabotage for example Stuxnet.
6. Extort payment for example Cryptolocker.

List of Common Malware types:

- **Adware**: The least dangerous and most lucrative Malware. Adware displays ads on your computer.
- **Spyware**: Spyware is software that spies on you, tracking your internet activities in order to send advertising (Adware) back to your system.
- **Virus:** A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers.
- **Spam:** Spamming is a method of flooding the Internet with copies of the same message. Most spams are commercial advertisements which are sent as an unwanted email to users. Spams are also known as Electronic junk emails or junk newsgroup postings. These spam emails are very annoying as it keeps coming every day and keeps your mailbox full.
- **Worm:** A program that replicates itself and destroys data and files on the computer. Worms work to "eat" the system operating files and data files until the drive is empty.
- **Trojan:** A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources, and in larger systems creating a "denial-of-service attack" which is making a machine or network resource unavailable to those attempting to reach it. Example: Google, AOL, Yahoo or your business network becoming unavailable.
- **Backdoors:** Backdoors are much the same as Trojans or worms, except that they open a "backdoor" on a computer, providing a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.
- **Rootkit:** This one is likened to the burglar hiding in the attic, waiting to take from you while you are not home. It is the hardest of all Malware to detect and therefore to remove; many experts recommend completely wiping your hard drive and reinstalling everything from scratch. It is designed to permit the other information gathering Malware in to get the identity information from your computer without you realising anything is going on.
- **Keyloggers:** Records everything you type on your PC in order to glean your log-in names, passwords, and other sensitive information, and send it on to the source of the keylogging program. Many times keyloggers are used by corporations and parents to acquire computer usage information.
- **Rogue security software**: This one deceives or misleads users. It pretends to be a good program to remove Malware infections, but all the while it is the Malware. Often it will turn off the real Anti-Virus software.
- **Ransomware**: If you see this screen that warns you that you have been locked out of your computer until you pay for your cybercrimes. Your system is severely infected with a form of Malware called Ransomware. Even if you pay to unlock the system, the system is unlocked, but you are not free of it locking you out again.
- **Browser Hijacker**: When your homepage changes to one that looks like those in the images inserted next, you may have been infected with one form or another of a Browser Hijacker. This dangerous Malware will redirect your normal search activity and give you the results the developers want you to see. Its intention is to make money off your web surfing. Using this homepage and not removing the Malware lets the source developers capture your surfing interests.

How does a Malware spread?

Cybercriminals continuously devise innovative resources to get malware into the computer. Here are some of the most common ways of spreading:

- **Email**: Cybercriminals are notorious for including malicious attachments and links in emails that appear to come from friends, reputable organisations, or other trusted sources. Some malicious emails can even infect your computer from the email client's preview pane, without your opening or be downloading an attachment or a link.
- **The Internet:** Surfing the Web may feel like a private activity, but in fact, you're exposing your computer to unwanted contact with anyone else who has a computer and Internet access.
- **Outdated software:** Malwares can crawl the Internet, looking for vulnerabilities of outmoded software to spread its influence over computer systems.
- **Local Area Networks (LANs):** A LAN is a group of locally connected computers that can share information over a private network. If one computer becomes infected with malware, all other computers in the LAN may quickly become infected as well.
- **Instant messaging (IM) and peer-to-peer (P2P) file-sharing systems:** If one is using a client for these online activities, malware may spread to your computer.
- **Social networks:** Malware authors take advantage of many popular social networks, infecting the massive user-data networks with worms. If a social website account is infected with a worm, just about anyone who visits a poster's profile page could "catch" the worm on her system.
- **Pop-ups:** Some of the most sophisticated malware spreads through well-disguised screen pop-ups that look like genuine alerts or messages. One particularly devious and widespread "hoax pop-up" claims to have scanned your computer and detected malware. If you attempt to remove the malware as urged, you'll actually *install* the malware.
- **Computer storage media:** Malware can be easily spread if you share computer storage media with others, such as USB drives, DVDs, and CDs. While it may seem safe to open a CD of photos from a colleague, it's always best to scan unfamiliar files first for possible corruptions or security risks before you copy or open them.

- **Mobile devices:** Mobile malware threats have become increasingly prevalent, as more people use their smartphones and tablets as mini-computers, helping malware problems proliferate across additional platforms.

Recent case of Malware attack: WannaCry

In 2017 May, there was a massive global ransomware attack. The attack infected more than 230,000 computers in 150 countries including India, demanding ransom payments in bitcoin in 28 languages.

What is WannaCry?

- WannaCry is Encrypting Ransomware or Crypto Locker type of ransomware that is programmed to attack Microsoft Windows software.
- According to some statistics, hackers extorted business and institutions for more than $209 million in Ransomware payments in the first three months of 2016. The business of Ransomware is on pace to be a $1 billion a year crime.
- **Shadow Brokers**: People (Hackers) behind these attacks call themselves by this term.

Severely affected:

- Britain's **National Health Service** (NHS),
- Spain's **Telefónica**,
- **FedEx** (USA)
- Deutsche **Bahn**
- Several plants of carmakers Renault and Nissan had stopped production in France and England due to the malware,
- The Russian Interior Ministry had reported about 1,000 computers.
- **Affected Areas in India**: Andra Pradesh, Kerala, some Pharma companies and over 48,000 attempts of ransomware attacks were detected in India. 60% of the attempts targeted enterprises, while 40% targeted individual customers said a cyber-security firm, **Quick Heal Technologies**.

What is the Origin of Wannacry attack?

- It is said by Wikileaks that **National Security Agency (NSA)** of USA had these methods to have monitored over subjects.
- This loophole was recently leaked by WikiLeaks.
- The same vulnerability of Windows Operating system was used by ransomware.
- However, Microsoft had released the security patches for the same earlier.

What does it do the computer?

- Some variants of ransomware encrypt data in such a way that it is impossible to decrypt unless the user has an encryption key. These are called **'Encrypting Ransomware'** that incorporate advanced encryption methods.
- Another type of ransomware that is frequently circulated is **'Locker ransomware**, which locks the victim out of the operating system, making it impossible to access the desktop and any apps or files. **CryptoLocker**, like WannaCry, is a malware when injected into a host system, scans the hard drive of the victim and targets specific file extensions and encrypts them.

How does it spread?

- Wannacry encrypts the files on an infected computer.
- It spreads by using a vulnerability in implementations of **Server Message Block (SMB)** of Windows systems. This exploit is known as **ETERNALBLUE**.
- It encrypts hard disk/drive and then spread laterally between computers on the same LAN.
- It also spreads through the malicious Email-attachment.

How to remain protected from ransomware?

- **Regular Data Backup**: This helps restore the last saved data and minimise data loss. Ransomware also attacks servers; hence it is important to have a backup on a disconnected hard drive or external device on the pre-defined regular basis.
- **Prevention**: To prevent infiltration of malware, having password protected tools to identify and filter certain file extensions like ".exe" or ". Zip", are essential. Emails that appear suspicious should also be filtered at the exchange level. There are also

some tools that detect the entry of such malware with features of zero days' protection which work on threat emulation and threat extraction techniques. Users and businesses also need to ensure that hidden file extension is displayed since it becomes easier to filter them.

- **User awareness**: Awareness among users needs to be created to avoid opening the unsolicited attachment. Malware is typically designed to mimic identities of people that users interact with on a regular basis either on a personal or professional level.
- **Rules in IPS**: It's necessary to create rules in the Intrusion Prevention Software (IPS) to discard or disallow the opening of files with extension ".exe" from local App data folders or AppData.
- **Regular patch and upgrades**: To prevent leaks or vulnerabilities in software, ensure to regularly update the software versions and apply patches released by the vendor. These patches and version are often released to wrestle with known or newly discovered exploits and can prevent known signatures of these malware, Trojans or ransomware to enter the system.
- **Install and run anti-malware** and firewall software. When selecting software, choose a program that offers tools for detecting, quarantining, and removing multiple types of malware.
- **The combination of anti-malware** software and a firewall will ensure that all incoming and existing data gets scanned for malware and that malware can be safely removed once detected.
- **Keep software and operating systems** up to date with current vulnerability patches. These patches are often released to patch bugs or other security flaws that could be exploited by attackers.
- **Be vigilant** when downloading files, programs, attachments, etc. Downloads that seem strange or are from an unfamiliar source often contain malware.

Some Initiatives by Government of India:

- **National Cyber Security Policy 2013:** Indian Government already have a National Cyber Security Policy in place. The National Cyber Security Policy document outlines a roadmap to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.
- **Computer Emergency Response Team (CERT-In**) has been designated to act as a nodal agency for coordination of crisis management efforts. CERT-In will also act as an umbrella organisation for coordination actions and operationalization of sectoral CERTs. CERT-in will also issue early warnings.
- **Cyber Swachhta Kendra**: The "Cyber Swachhta Kendra" is a Botnet Cleaning and Malware Analysis Centre (BCMAC), operated by the Indian Computer Emergency Response Team (CERT-In) as part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY). Its goal is to create a secure cyberspace by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections.