Understanding and Managing Information Security Threats

Malware

- is a catch-all term for any type of malicious software designed to harm or exploit any programmable device or network Refers to any malicious software or computer program that performs malicious activities
- Unwanted and potentially dangerous set of programs
- Can cause harm to your computer and even stop you from using it
- Complex and constantly evolving

Software bugs vs Malicious Activities

- Bugs : errors in programs that can occur unintentionally and can affect a program’s performance
- Malicious activities:
  - Propagation
  - Destruction
  - Unauthorized activities
  - Opening backdoors
  - Theft
  - Exploitation
  - Deception
  - Hidden activities

Types of Malware

- Viruses
- Worms
- Trojan Horses or Trojans
- Blended threats

Virus

- **Infects files:** Infection is the capability of a virus to insert a copy of itself, or any malicious code, on another executable code called “host”
- They are executable codes or programs
- Some viruses must be loaded into memory first: will infect files once they get triggered by certain events such as: *executing*, *opening*, or even *closing* a file
- Acts like a virus pathogen that attacks animals and plants

Common Types of Viruses

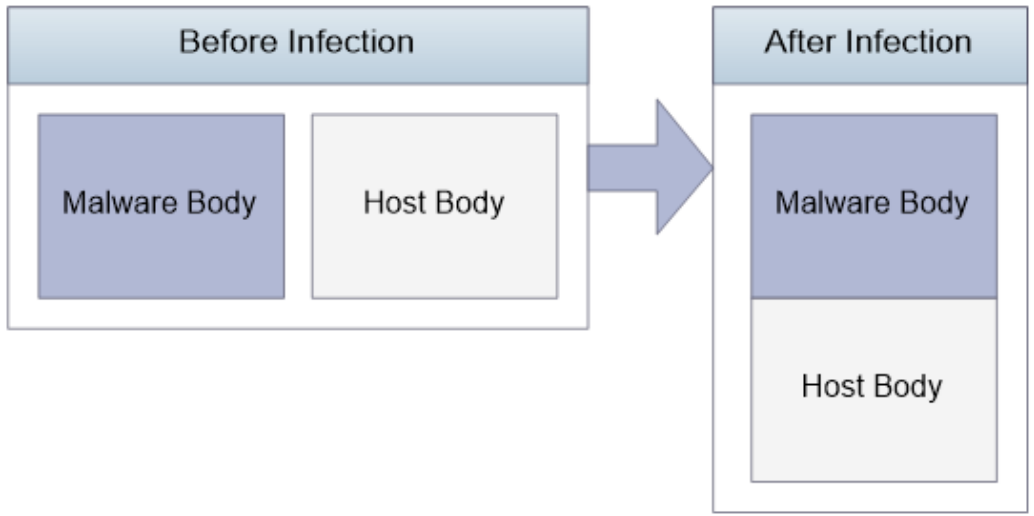
- **Boot viruses** : infect a boot sector of a disk like a hard drive's Master Boot Record (MBR). A boot sector contains codes that are being executed during the system's startup procedure, often to load the operating system.
  - Once a boot sector is infected, the virus will run every time the system boots up.
- **Binary File Infectors**: Infect binary executable files like EXE and DLL files.
  - Once an executable file is infected, the virus executes every time the host executable file is executed.
- **Multipartite Viruses**: Hybrids of boot viruses and binary file infectors as they are capable of infecting both the boot sectors and other binary executable files.

Common Types of Viruses

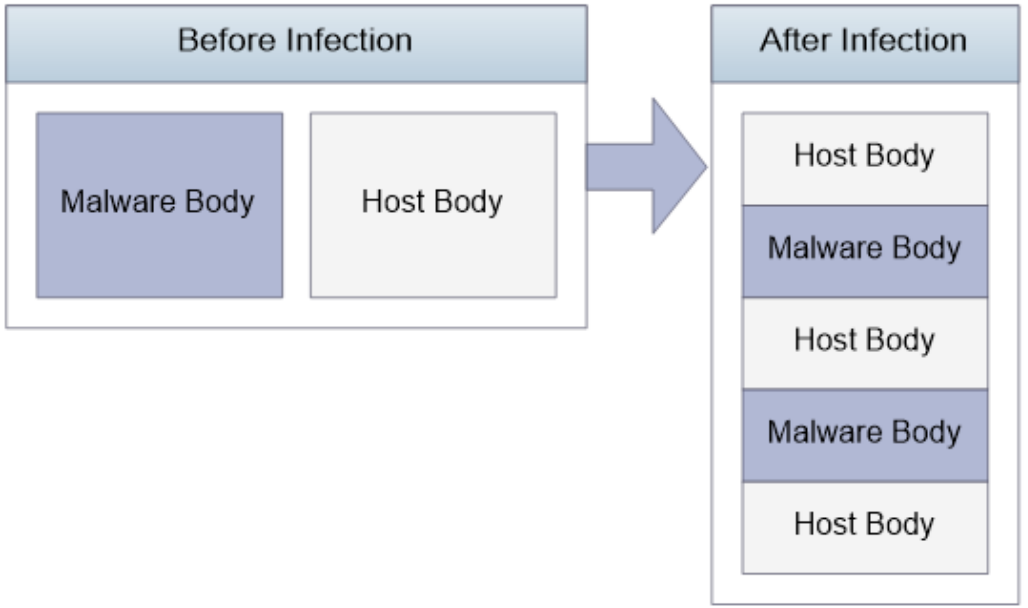
- **Macro Viruses**: Written in VBA code, they target and infect MS Office files. These files use macro codes to automate the way an application behaves for a particular file (like what MS Word does when opening a compatible document).
  - A macro virus is executed whenever the infected document is opened or closed.
- **Script Viruses**: are in the form of scripts that infect scripts. A script, unlike a program, is an executable code that is interpreted or run without being compiled.
  - Scripts are plain-text codes that utilizes an interpreter to get executed – such as VBS, Java Script, batch files, PERL, etc.

Type of File Infections

- Prepending Infection

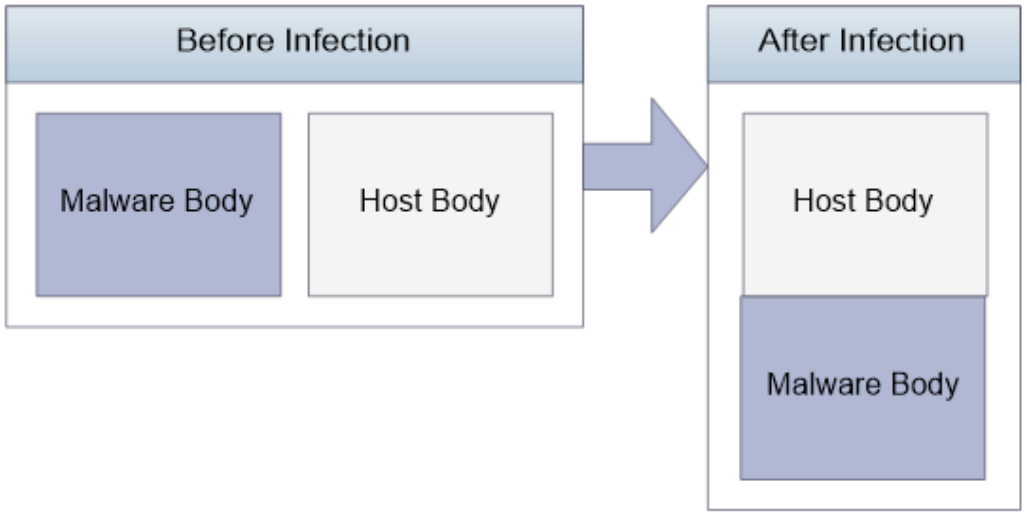


- Cavity Infection

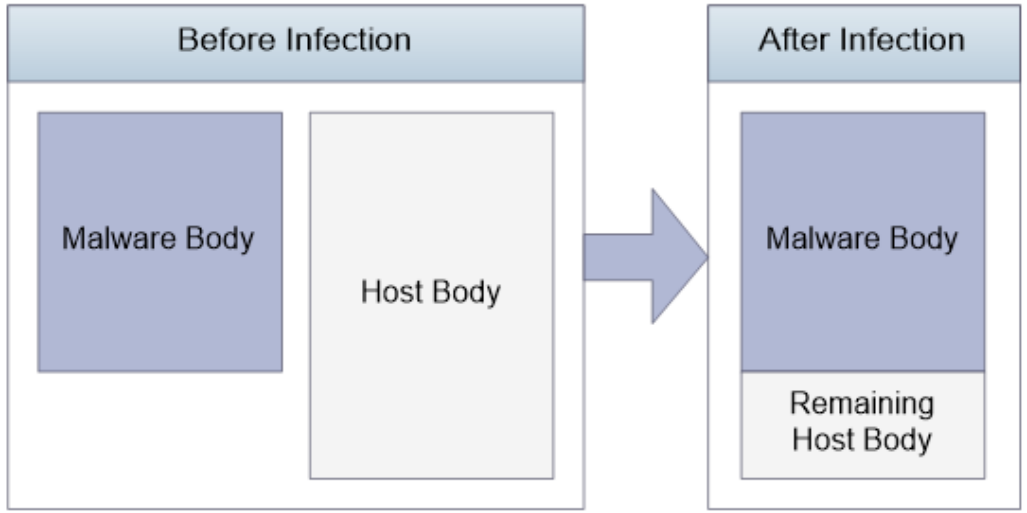


Type of File Infections

- Appending Infection

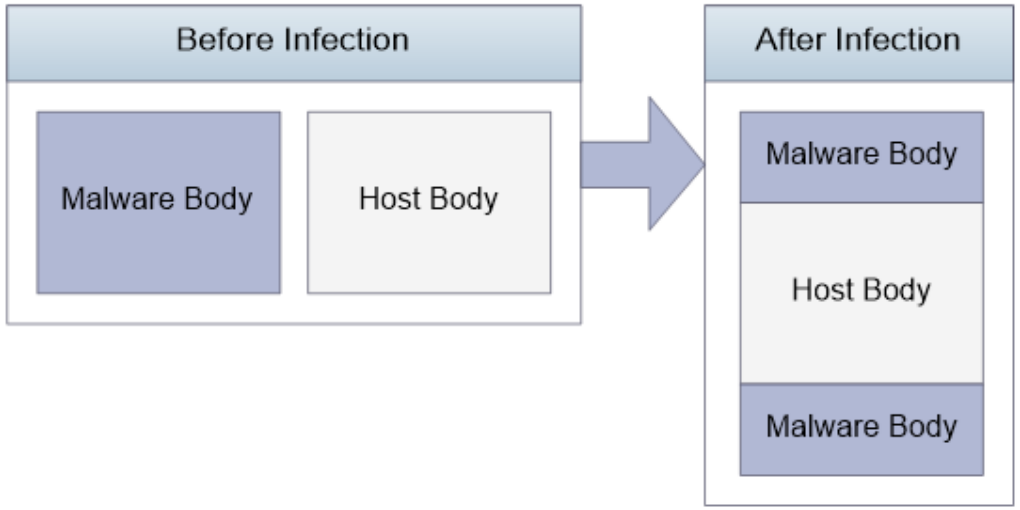


- Overwriting Infection

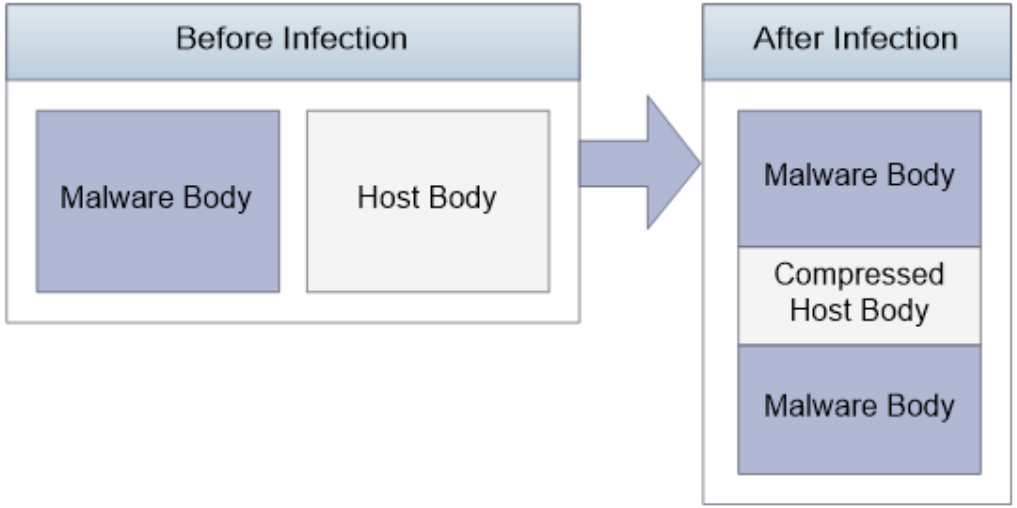


Type of File Infections

- Sandwich Infection (or Amoeba)



- Complex Infection



Operating Algorithm of Viruses

- **Direct file infectors**:
  - First identify a file to infect. Directories and sub-directories are searched for target files that match pre-defined criteria.
  - Once it has validated that the target file is suited for infection, it checks if the file has already been infected before.
  - If not yet infected, the malicious code is inserted to the target and the payload, if there is any, is generated. Once completed, virus either passes the control to the host or executes the host

Operating Algorithm of Viruses

- **Memory resident viruses**:
  - starts the infection process by first installing itself. Then it checks if another instance of itself is already residing in memory (called memory residency check). If not yet installed, it allocates memory space and loads itself to the allocated space to become resident.
  - The virus then hooks DOS functions or APIs. Other executable files that make use of the hooked functions or APIs are validated for suitability by the virus. If the executable file can be infected, the virus checks if it has already been infected before.
  - Similar with the process followed by direct file injectors, once the executable has been checked, the malicious code is inserted to the target and the payload, if there is any, is generated. Once completed, either the control is passed onto the host or the virus executes the host.

Mother Virus

- The origin of an infection comes from a MOTHER VIRUS which is a program that searches for targets and copies its contents to target files.

Virus Payload

- Viruses were the first malware to implement payloads as part of their malicious routines
- Not all malware have payloads
- These are also known as "*symptoms of infection*" because most of them are visible to the user

Virus Payload

- Examples of payloads:
  - Display images and/or messages
  - Generate sounds
  - Execute other applications abnormally or without user intervention
  - Reboot or shutdown the computer automatically
  - Slow down the computer
  - Alter desktop and taskbar settings

Worms

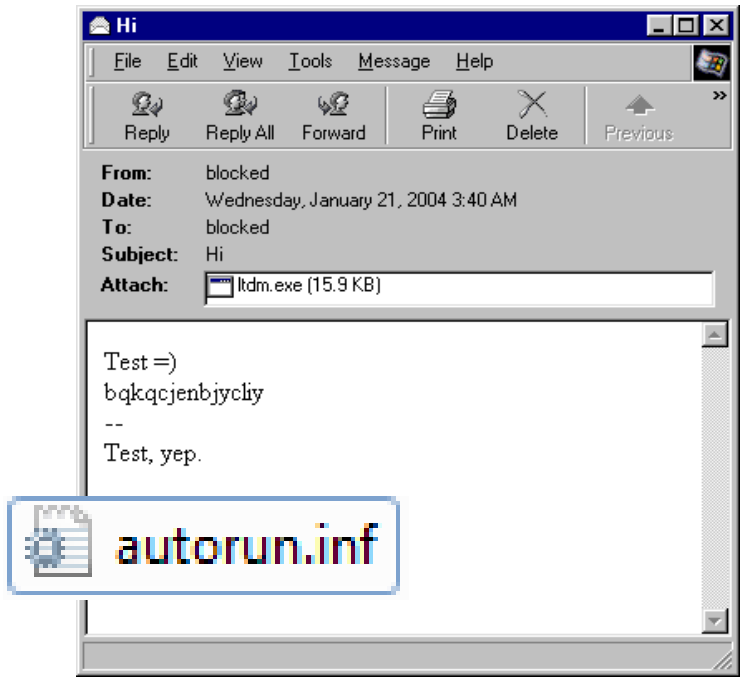
- A form of malware that creates a copy of itself and then sends itself over the network to infect other systems Named after the tapeworm in John Brunner's novel, the Shockwave Rider
- Program that replicates itself constantly, without requiring another program environment
- Can continue to replicate themselves until they completely fill available resources such as memory, hard drive space, and network bandwidth
  - Ex. Code Red, Sircam, Nimda (admin spelled backwards), and Klez

Worms

- MyDoom, Netsky are variants of the multifaceted attak worms that exploit weaknesses in the leading operating systems and applications
- Worms can distribute themselves to all email addresses found on the infected systems
- Can also infect web servers – targeting users who visit the site

Worms

- Email
- Internet Relay Chat (IRC)
- Instant Messaging (IM) Applications
- Peer-to-Peer File Sharing Applications
- Network Shares
- Vulnerability Exploits
- Disk Drives / Thumb Drives



Characteristics of Worms

- May exhibit other malware behavior similar to viruses, backdoors, trojans, or keyloggers
- It is NOT capable of infecting files but it can propagate by spreading itself in a Network
- A host is not required although some may argue that a worm's host is the machine it has infected

Trojans / Trojan Horses

- Trojans cannot propagate by themselves because they do not have the mechanism to send their own copy to another computer
  - It gets into a users machine by riding on a third-party application that is trusted by the user
- Named after the horse-like structure in Greek mythology
  - In Greek legends, a hollow wooden statue of a horse in which the Greeks concealed themselves in order to enter Troy.

Trojans / Trojan Horses

- Programs that hide their true nature and reveal their designed behavior only when activated
- Often disguised as helpful, interesting, or necessary pieces of software, such as readme.exe, often included with shareware or freeware packages
- type of malware that is often disguised as legitimate software. **Trojans** can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing **Trojans** on their systems.

Destructive Trojans

- Downloader
- Lowers security settings
- Open ports
- Key logger
- Format computer / destroy files

Kinds of Trojans

- Destructive Trojans
- Trojan Droppers
- Trojan Downloaders
- Trojan Clickers
- Flooders/Nukers, and DOS/DDOS attacks
- Trojan Backdoors
- Trojan Spies
- Trojan Proxies
- Ransomware

Destructive Trojans

- They have payloads that can be triggered by time or b a specific event
- Intention: To destroy
- Payload:
  - Format hard drives
  - Overwrite MBRs or boot sectors
  - Delete files
  - Delete important registry entries
  - Corrupt files
  - Corrupt data/information
  - Disable hardware settings
  - Hang Windows and make OS unusable
  - Make OS unbootable

Trojan Dropper

- Act as carriers for other malware and can come in the form of an installation or setup package
- Compression utilities such as WinZip or WinRAR
- Oftentimes the by-products of application that join two or more executable files
- Intention: to drop and execute other malware
- Payload:
  - Drop one or more malicious files in the system
  - Execute the files they dropped

Trojan Downloaders

- Act as agents for other malware
- They only work if there is an Internet connection available
- They often use WININET APIs to download malicious files. The downloaded files are usually other trojans but they can also include worms and viruses
- Intention: To download malware and execute
- Payload:
  - Connect to a malicious website
  - Download malware from malicious website
  - Execute the downloaded files

Trojan Clickers

- Bait users into accessing malicious websites or any other sites that users don't intend to access. If trojan downloaders directly download malware, clickers do it indirectly by redirecting the user to the malicious website where other malware are downloaded once accessed
- Intention: To cause users to access malicious website
- Payload:
  - Continuously attempting to connect to the Internet
  - Modify Windows HOSTS files to redirect users to the infected website
  - Modify browser settings (such as default home page, search page)
  - Hijack any attempt of the user to access websites by auto-completing the typed URL in the address bar

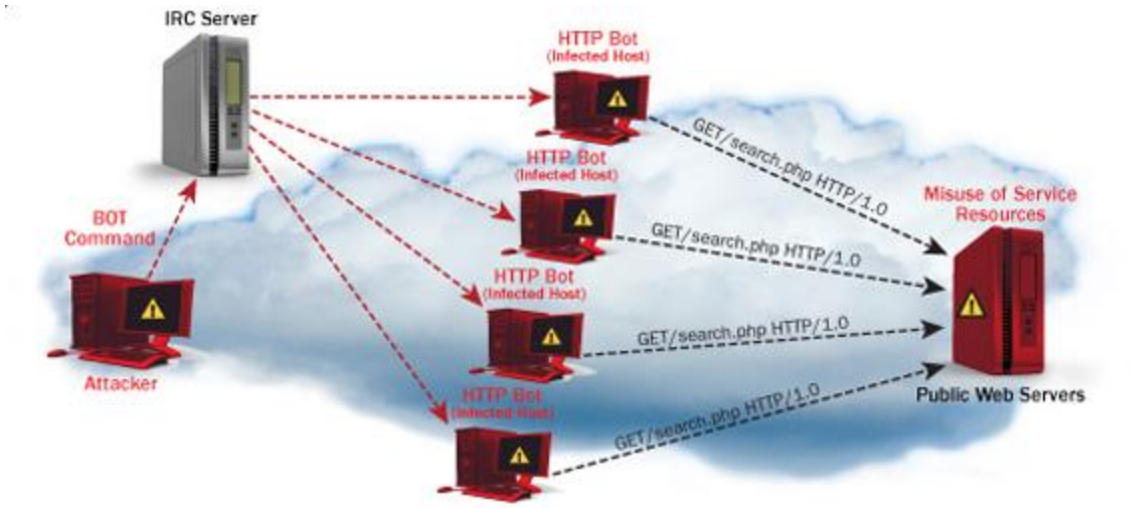
Flooders, Nukers, DOS/DDOS Attacks

- DOS is a general term used to describe what malware is doing to deny users of their computing privileges
- Forms of DOS:
  - Land attack: A (land) local area network denial attack that is done by simply redirecting all packets which the infected machine has been sending, to itself.
    - Ping flood (or Ping of Death): In this type of dos attack, ICMP (or ping) packets are used to attack a target computer
    - SYN flood: In this form of attack, the TCP SYN packets are used to attack the target machine. In standard TCP communication, for every SYN message that is sent, the target machine must respond with an ACK message. If there is a large amount of SYN messages simultaneously received, the target machine will not be able to respond with ACK message anymore. Thus, communication would be denied.

Flooders, Nukers, DOS/DDOS Attacks

- Flooders: Flood the network with garbage packets. Nuking is a term used for sending a lot of garbage packets to a single target machine.
- DDoS: A distributed denial of service attack is the simultaneous nuking of a single target machine from several sources

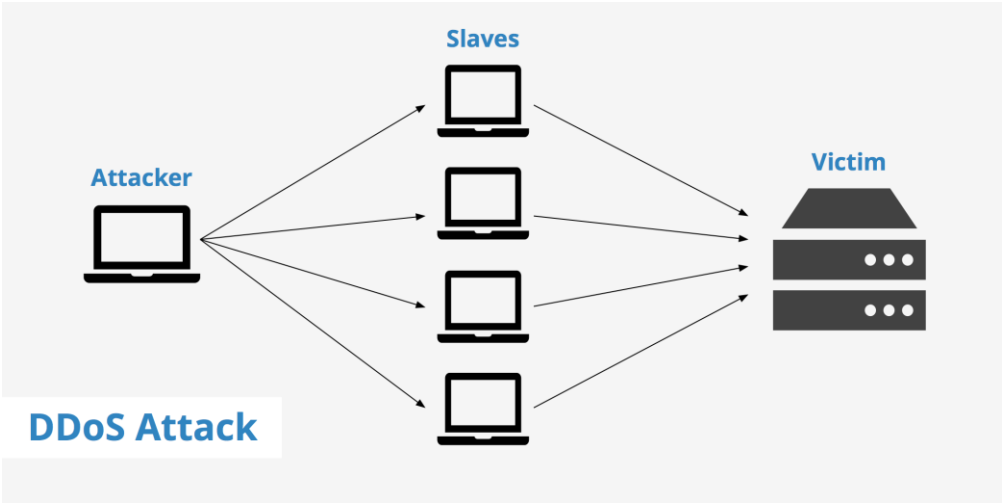
Flooders, Nukers, DOS/DDOS Attacks



Intention: To make computer resources unavailable

Payload:

- Modify Windows HOSTSS file to deny connection to some websites
- 100% CPU Utilization
- Make it difficult to access the network or Internet



Trojan Backdoors (Backdoors)

- Backdoor malware has two components: a server and a client
  - Server component: the one that is being spread across the Internet which can be remotely controlled by the hacker using the client component
  - Client component: in possession of the hacker and is used for remote access
- Intention: To allow a malicious remote user to connect to the affected machine and to have access/control over it
- Payload:
  - Open/close CD tray
  - Pop-up messages
  - Execute available applications on the system
  - Shut down Windows
  - Browse file systems
  - Capture clipboard data and screenshots

Note: Because of the unique behavior of backdoors and its damage potential to an infected machine, it was classified as a separate type of malware from a trojan horse malware

Trojan Spies

- **Main focus**: information theft
  - Capable of monitoring and logging information that is related to users' computing and web browsing habits. These logs are sent to unknown users through email, IRC, instant messaging apps, or even through FTP.
  - May also be capable of hijacking the web browsing activities of users
  - May intercept accesses to online banking and internet shopping websites to steal banking and payment information
- **Intention**:
  - To monitor and log a user's computing activities which will be sent to an unknown host. It also intends to trick users into divulging their personal information
- Payload:
    - Steal user accounts and passwords
    - Steal user keystrokes
    - Steal system information
    - Steal internet browsing-related information
    - Steal serial keys of installed applications
    - Steal Email messages
    - Steal clipboard data and screenshots

Trojan Proxies

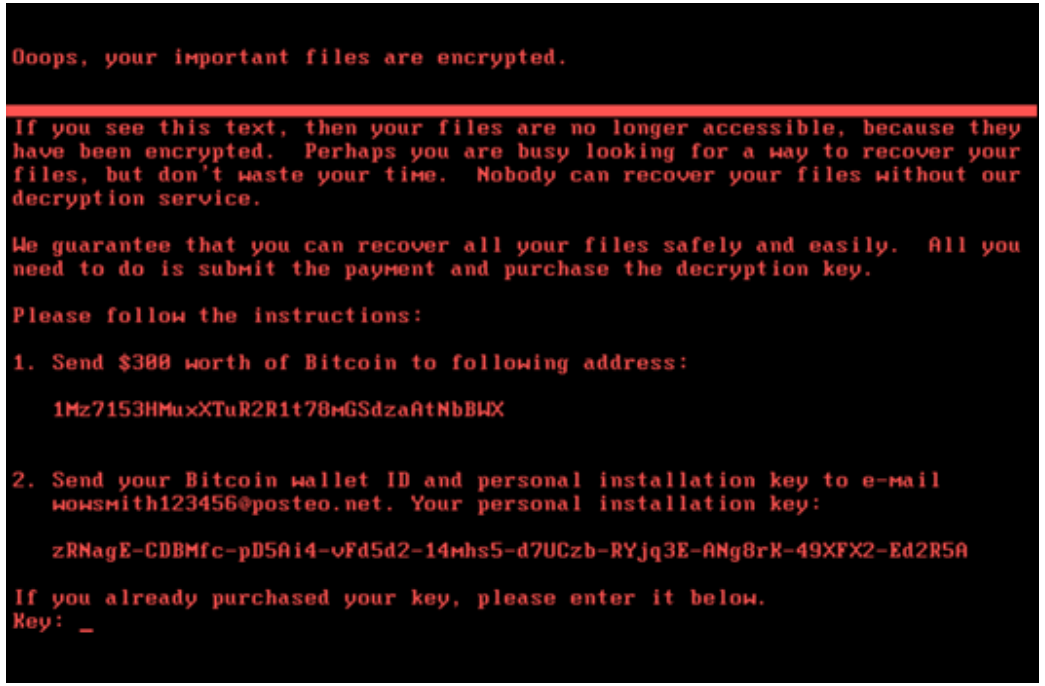
- Two purposes:
  (1) Sniff Internet traffic so it can monitor Internet activities happening within the network
  (2) Used by hackers to hide the hacker's true location
- Intention: To install themselves as web proxy on the affected machine
- Payload: Accept all Internet traffic

Ransomware

- Primary motivation: money
- Seize a user's important files, encrypt them, and request for a ransom in exchange for the restoration and/or decryption of files
- Intention: To encrypt user data files so that it cannot be used/opened by the user. The hacker will extort money from the user in exchange for the restoration of the data files
- Payload: Encrypt user data files

Ransomware

- For almost the past month, key computer systems serving the government of Baltimore, Md. have been held hostage by a ransomware strain known as "**Robbinhood**."
- Media publications have cited sources saying the Robbinhood version that hit Baltimore city computers was powered by "**Eternal Blue**," a hacking tool developed by the **U.S. National Security Agency** (NSA) and leaked online in 2017.
- But new analysis suggests that while Eternal Blue could have been used to spread the infection, the Robbinhood malware itself contains no traces of it.
- Security experts briefed on the attack who blamed the ransomware's spread on the Eternal Blue exploit, which was linked to the global WannaCry ransomware outbreak in May 2017.



Fileless Malware

- Fileless malware doesn't install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell or WMI.
- Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software — and because these attacks are stealthy, they are up to ten times more successful than traditional malware attacks.
- Example: Astaroth is a fileless malware campaign that spammed users with links to a .LNK shortcut file. When users downloaded the file, a WMIC tool was launched, along with a number of other legitimate Windows tools. These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners. Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server.

Rootkits

- A rootkit is software that gives malicious actors remote control of a victim's computer with full administrative privileges.
  - can be injected into applications, kernels, hypervisors, or firmware
  - they spread through phishing, malicious attachments, malicious downloads, and compromised shared drives.
  - can also be used to conceal other malware, such as keyloggers

Rootkits

- Example Zacinlo infects systems when users download a fake VPN app. Once installed, Zacinlo conducts a security sweep for competing malware and tries to remove it.
  - Then it opens invisible browsers and interacts with content like a human would — by scrolling, highlighting and clicking. This activity is meant to fool behavioral analysis software.
  - Zacinlo's payload occurs when the malware clicks on ads in the invisible browsers. This advertising click fraud provides malicious actors with a cut of the commission.

Other Forms of Threats and Malware

Spyware

- Spyware collects information about users' activities without their knowledge or consent. This can include passwords, pins, payment information and unstructured messages.
- The use of spyware is not limited to the desktop browser: it can also operate in a critical app or on a mobile phone.
- *Even if the data stolen is not critical, the effects of spyware often ripple throughout the organization as performance is degraded and productivity eroded.*
- Example: *DarkHotel*, which targeted business and government leaders using hotel WIFI, used several types of malware in order to gain access to the systems belonging to specific powerful people. Once that access was gained, the attackers installed **keyloggers** to capture their targets passwords and other sensitive information.

Keyloggers

- A keylogger is a type of spyware that monitors user activity. Keyloggers have legitimate uses; businesses can use them to monitor employee activity and families may use them to keep track of children's online behaviors.
- However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering or malicious downloads.

Types of Keyloggers

- There are two main types of software keyloggers: **user mode keyloggers** and **kernel mode keyloggers**.
  - **A user mode keylogger** uses a Windows API to intercept keyboard and mouse movements. GetAsyncKeyState or GetKeyState API functions might also be captured depending on the keylogger. These keyloggers require the attacker to actively monitor each keypress.
  - A **kernel mode keylogger** is a more powerful and complex software keylogging method. It works with higher privileges and can be harder to locate in a system. It uses filter drivers that can intercept keystrokes. They can also modify the internal Windows system through the kernel.

Protection Against Key Loggers

- Visual inspection
- Firewalls
- Password Managers
- Monitoring software
- System cages
- Security tokens as part of two-factor authentical (2FA)
- Application AllowListing

Adware

- Adware tracks a user's surfing activity to determine which ads to serve them. Although adware is similar to spyware, it does not install any software on a user's computer, nor does it capture keystrokes.
- The danger in adware is the erosion of a user's privacy — the data captured by adware is collated with data captured, overtly or covertly, about the user's activity elsewhere on the internet and used to create a profile of that person which includes who their friends are, what they've purchased, where they've traveled, and more. That information can be shared or sold to advertisers without the user's consent.
- Example: Adware called *Fireball* infected 250 million computers and devices in 2017, hijacking browsers to change default search engines and track web activity. However, the malware had the potential to become more than a mere nuisance. Three-quarters of it was able to run code remotely and download malicious files.

Polymorphic Threats

- **Polymorphic malware** is a type of malware that constantly changes its identifiable features in order to evade detection. Many of the common forms of malware can be polymorphic, including viruses, worms, bots, trojans, or keyloggers
- Polymorphic viruses are complex file infectors that can create modified versions of itself to avoid detection yet retain the same basic routines after every infection.

Polymorphic Threats

- Webroot researchers have found that **97% of malware infections employ polymorphic techniques**.
- To vary their physical file makeup during each infection, polymorphic viruses encrypt their codes and use different encryption keys every time.
  - One of the biggest challenges to fighting viruses and worms
  - One that changes the way it appears to antivirus programs, making it undetectable by techniques that look for preconfigured signatures
  - These viruses/worms evolve, changing their size and external file characteristics to elude detection

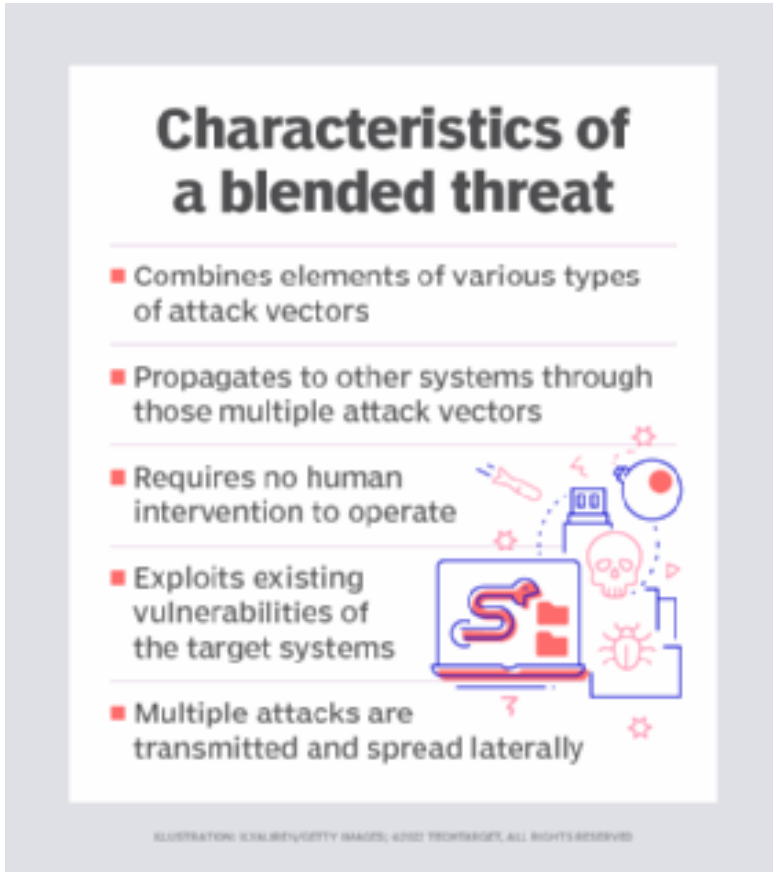
New Wave of Polymorphic Threats

- **Storm Worm Email**: The infamous spam email sent in 2007 with the subject “230 dead as storm batters Europe” was, at one point, responsible for as much as 8% of all global malware infections.
  - When the message’s attachment is opened, the malware installs wincom32 service and a trojan onto the recipient’s computer, transforming it into a bot. One of the reasons the storm worm was so hard to detect with traditional antivirus software was the malicious code used morphed every 30 minutes or so.
- **CryptoWall Ransomware**: a polymorphic ransomware strain that encrypts files on the victim’s computer and demands a ransom payment for their decryption. The polymorphic builder used in Cryptowall is used to develop what is essentially a new variant for every potential victim.

Protection Against Polymorphic Threats

- Because polymorphic malware is engineered to evade detection by traditional antivirus tools, the best solutions for this threat use advanced, **behavior-based detection techniques**.
  - Behavior-based detection solutions like endpoint detection and response or advanced threat protection can pinpoint threats in real time, before any of your data is compromised.
    - **Endpoint detection and response (EDR),** also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities
  - Behavior-based malware protection is more accurate than traditional signature-based methods which struggle to deal with polymorphic attacks.

Blended Threats



Blended Threats

- They have a complex malicious behavior
- These are bundles of malicious programs that combine the functionality of different types of malware, including trojans, worms, backdoors.
- Often involves an infection chain whereby a visitor to a website is first diverted to a malicious URL, then compelled via social engineering to download a malicious file
- BY using multiple methods and techniques, cybercriminals are able to quickly and surreptitiously spread threats.

Security Measures

- **Technical measures** include the hardware and software that protects data — everything from encryption to firewalls
- **Organizational measures** include the creation of an internal unit dedicated to information security, along with making infosec part of the duties of some staff in every department
- **Human measures** include providing awareness training for users on proper infosec practices
- **Physical measures** include controlling access to the office locations and, especially, data centers

Technical Security Measures

- **Access control and authentication -** Access control and authentication are basic security measures for the protection against unauthorized access to the IT system used for the processing of personal data. They implement the access control policy of the by technically enforcing it into specific components and applications
- **Logging and monitoring -** The use of log files is an essential security measure that enables identification and tracking of user actions (with regard to the processing of personal data), thus supporting accountability in case of an unauthorized disclosure, modification or destruction of personal data. Monitoring of log files is important for identifying potential internal or external attempts for system violation

Technical Security Measures

- **Security of data at rest -** Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Therefore, this category of measures is mainly related to the processing of personal data in databases or other relevant systems (including cloud storage). It also relates to the processing of personal data by employees with the use of specific workstations or other devices
- **Server/Database security -** Servers and databases consist the backbone of the information system processing personal data. They must be security hardened to ensure a secure operating environment

Technical Security Measures

- **Workstation security -** This measure is mainly related to the security configuration of users' workstations or other devices. It is important for enforcing specific security policies and restricting users from performing certain actions that could compromise the security of the IT system (e.g. deactivating of antivirus programs or installation of unauthorized software)

- **Network/Communication security -** Essentially, it is the password or code needed to access a local area network. Network security keys allow users to establish a secure connection and prevent unauthorized access to the network.

Technical Security Measures

- **Back-ups -** A back up system is an essential means of recovering from the loss or destruction of data. While some system should be in place, the frequency and nature of back up will depend, amongst other factors, on the type of organization and the nature of data being processed. It is the“ability to restore the availability and access to personal data” in part of the data security obligations for the data controller or data processor

Technical Security Measures

- **Mobile/Portable devices -** Mobile/Portable devices can extent the level of services offered by the data controller but increase exposure to theft and accidental loss. In the case of mobile devices, such as smartphones or tablets, users might also apply them for personal use and special care must be taken to ensure that business data is not compromised

Technical Security Measures

- **Data deletion/disposal -** The purpose of disposal/deletion is to irreversibly delete or destroy the personal data so that it cannot be recovered. The method(s) used must, therefore, match with the type of storage technology, including paper-based copies
- When disposing obsolete or redundant equipment, the data controller must ensure that all data previously stored on the devices has been removed prior to disposal. Personal data should not be retained for longer than necessary in relation to the purposes for which they were collected, or for which they are further processed. In some cases, data subjects are also entitled to request deletion prior to the end of the maximum retention period

Technical Security Measures

- **Application lifecycle security -** During all phases of application development lifecycle, the organization must ensure that data protection compliance, including personal data security, is taken into consideration.
  - The principles of data protection by design and by default which require data controllers to design and implement processing activities with data protection in mind while applying the strictest privacy settings
- **Physical security -** Physical security is equally important to the technology-oriented security measures as physical access to the information system can be the foundation for the overall security strategy

Organizational Security Measures

- **Security Management - Security policy and procedures for the protection of personal data** The security policy is a high-level document that sets the basic principles for the security and protection of personal data in an organization. It thus forms the basis for the implementation of all specific technical and organizational measures.
- The security policy shows the overall commitment of the organization's management towards security and data protection. It can be based on or form part of the organization's general IT security policy; in any case, it should explicitly address also the protection of personal data.

Organizational Security Measures

- **Roles and responsibilities -** As a first and basic control for the security of personal data, all the organization's jobs requiring access to personal data should have clearly defined and documented roles and responsibilities
- **Access control policy -** Following the definition of roles and responsibilities, it is essential to determine an access control policy to the systems used for the processing of personal data. This should be based on the ‘need to know’ principle, i.e. each role/user should only have the level of access to personal data that is strictly necessary for the performance of its relevant tasks

Organizational Security Measures

- **Resource/asset management -** The proper management of hardware, software and network resources is essential for the security of personal data, as it allows control of the means of the processing (and, thus, control of the subsequent organizational and technical measures)
  - Resource management as a minimum includes the registration of IT resources and network topology (which are used for the processing of personal data)
- **Change management -** Change management aims at synchronizing and controlling all changes performed in the IT system used for the processing of personal data. It is an important security measure, as an unsuccessful change attempt could lead to unauthorized disclosure, modification or destruction of data

Organizational Security Measures

- **Incident response and business continuity** - Incidents handling / Personal data breaches. In the event of a data security breach, the organization should asses if this leads to:
  - an “accidental or unlawful destruction,
  - loss, alteration,
  - unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”

Organizational Security Measures

- Controllers should make sure that they meet their obligations regarding notification of a personal data breach to the supervisory authority and to the data subjects.
- Data processors should also make sure that they meet their obligation for immediate notification of the data controller. In any case, both data controllers and processors should have appropriate procedures in place, not only for the notification of personal data breaches, but also for the overall handling and management of such events.

Organizational Security Measures

- **Business continuity -** A business continuity plan (BCP) is essential for determining the processes and technical measures that the organization should follow in case of an incident/personal data breach.
- It complements the security policy of the organization, as well as its incident response plan. This is the ability (for the controller/processor) *'to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'.*

Organizational Security Measures

- **Human Resources - Confidentiality of Personnel Information**
  - In order to ensure confidentiality of personal data, the organization should ensure that its employees also provide sufficient confidentiality guarantees, both in terms of technical expertise and personal integrity.
  - To this end, specific measures should be in place to ensure that the personnel involved in the processing of personal data are properly informed about their duty to confidentiality, as well as to guarantee that this duty is sufficiently stipulated in the organization's human resources policies.

Organizational Security Measures

- **Training -** Personnel training in data protection and security procedures (e.g. use of passwords and access to specific data processing systems) is important for the right implementation of the organizational and technical security measures.
- Information on specific data protection legal obligations is also central, especially for key personnel involved in high risk processing of personal data

Information classification in Information Security

Rationale for Using Classification Systems

- Level of Importance or Level of Relevance/Criticality
- Loss of data could create significant problems
- Unauthorized disclosure / loss of confidentiality

Rationale for Using Classification Systems

- Amount of data
- Requirements for protection (i.e. special protection)
- Obligations and responsibilities of individuals

Levels in Government organization for Information Classification

- **Unclassified –** Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.
- **Sensitive but Unclassified –** Information that has been designed as a major secret but may not create serious damage if disclosed.
- **Classified** - information that has restricted access as per law or regulation.

Levels in Government organization for Information Classification

- **Confidential –** The unauthorized disclosure of confidential information could cause some damage to the country's national security. information that is protected as confidential by all entities included or impacted by the information. The highest level of security measures should be applied to such data.
- **Restricted** Information – information that is available to most but not all employees.
- **Secret –** The unauthorized disclosure of this information could cause serious damage to the countries national security.
- **Top Secret –** This is the highest level of information classification. Any unauthorized disclosure of top-secret information will cause grave damage to the country's national security.

Levels in Private Organizations for Information Classification :

- **Public –** Information that is similar to unclassified information. However, if it is disclosed, it is not expected to seriously impact the company.
- **Sensitive –** Information that required a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from loss of integrity owing to an unauthorized alteration.
- **Private –** Typically, this is the information i.e. considered of a personal nature and is intended for company use only, its disclosure could adversely affect the company or its employee salary levels and medical information could be considered as examples of “private information”.

Not all data needs to be classified. In some cases, destroying data is the most prudent course of action.

6 steps to classifying data

1. Identify data
Discover where your data resides, how valuable it is, how many copies exist and how many people have authorized access.

2. Use data governance
Determine the regulatory requirements to satisfy for sensitive data.

3. Create categories
Confidential or restricted data has greater value and carries bigger risks than internal or public data.

4. Prioritize data
Assign data to categories according to its level of importance.

5. Budget
Factor in how much storage and redundant security is needed for effective data classification.

6. Keep at it
Data classification is an ongoing process. Keep stakeholders involved and periodically adjust your classification plan as the data set grows.

Asset Inventory

- The point of developing an asset inventory is that you know which classified information you have in your possession, and who is responsible for it (i.e., who is the owner).
- Classified information can be in different forms and types of media, e.g.:
  - electronic documents
  - information systems / databases
  - paper documents
  - storage media (e.g., disks, memory cards, etc.)
  - information transmitted verbally
  - email

Criteria for Information Classification

- **Value –** It is the most commonly used criteria for classifying data in the private sector. If the information is valuable to an organization it needs to be classified.
- **Age –** The classification of the information may be lowered if the information value decreases over time.
- **Useful Life –** Information will be more useful if it will be available to make the changes as per requirements than, it will be more useful.
- **Personal association –** If the information is personally associated with a specific individual or is addressed by a privacy law then it may need to be classified.

Classification of Information

- Organizations should develop their own levels of classification based on what is common in the country or in the industry.
- The bigger and more complex your organization is, the more levels of confidentiality you will have.

Classification of Information

- For example, for a mid-size organization you may use this kind of information classification levels with three confidential levels and one public level:
  - **Confidential** (top confidentiality level)
  - **Restricted** (medium confidentiality level)
  - **Internal use** (lowest level of confidentiality)
  - **Public** (everyone can see the information)
- Asset owner

Information Labeling

- Once you classify the information, it needs to labelled appropriately – you should develop the guidelines for each type of information asset on how it needs to be classified
- For example, you could set the rules for paper documents such that the confidentiality level is to be indicated in the top right corner of each document page, and that it is also to be indicated on the front of the cover or envelope carrying such a document, as well as on the filing folder in which the document is stored.
  - For example, public information can be placed on an open cabinet or published on social media platforms of the company, while classified information should be kept locked and safe, either on a safe server or physically watched by security professionals.
- Labeling of information is usually the responsibility of the asset owner

Handling of Assets

- Most complex part - you should develop rules on how to protect each type of asset depending on the level of confidentiality. For example, you could use a table in which you must define the rules for each level of confidentiality for each type of media, e.g.:

	Internal use	Restricted	Confidential
Electronic documents			
Information systems			
Paper documents			
Storage media			
Verbally transmitted information			
Email			

Why Does Information Classification Matter?

- **Efficiency** - on a basic level, businesses that have their information classified are able to manage and deliver day-to-day operations more efficiently. Data can be easily located and retrieved; changes easily traced.
- **Security** – protecting sensitive information is the main idea behind information classification. It is a useful tactic to classify information in order to facilitate appropriate security responses according to the type of information being retrieved, transmitted, or copied.
  - Data encryption, data storage in safe servers with strong firewalls, and compliance with data protection standards can help immensely to protect against outside threats. Besides, there can be inside threats that are equally dangerous – like intentional data theft, accidental data breaches. Hence it is very important to restrict information and prevent threats.

Why Does Information Classification Matter?

- **Safety** – information classification helps create security awareness throughout the organization. The responsibility of protection of information lies with everyone handling the information. The system ensures that employees understand the value of the information they work with and safeguard that information.
- **Compliance** – information classification in information security helps organizations label information as sensitive, protect it against threats, and help comply with regulations. Organizations can easily implement standards to classify information.

Benefits of Information Classification

- **Rediscovery of business** - Identification of information is the beginning step in Information classification. Organizations, therefore, need to actively discover information that is generated, stored, and accessed by departments within the organization. This information discovery basically leads to rediscovering the business. This allows decision-makers to review how information is empowering the business or possibly functioning ineffectively.
- **Raises awareness of cyber risk** - Information security teams connect face to face with business owners to discuss information security and how it could impact their business. Thus, owners have a direct contact point where to reach if they have questions or need help regarding managing cyber risks or incidents. Awareness of cyberthreats and information security management rises to realistic levels, prompting the issue to be discussed and accepted at all levels throughout the organization.

Benefits of Information Classification

- **Optimize risk and resources** – defining information classification improves risk and information classification resources, leading to efficient and effective protection of information. By classifying data based on sensitivity and level of business impact, businesses are informing which information must be protected with high priority, thereby deciding where to spend the information security budgets.
- **Limit dissemination** – well-defined information classification is controlled by laws and regulations, thereby allowing businesses to restrict their dissemination on a need-to-know basis. This reduces the chances of data theft or loss, which helps to minimize penalties charged due to non-compliance.

Roles and Responsibilities : CISO

- **Chief Information Security Officer** - is a senior-level employee of the company who oversees the information security program. Responsibilities of the Chief Information Security Officer include the following:
  - Developing and implementing a company-wide information security program
  - Documenting and disseminating information security policies and procedures
  - Coordinating the development and implementation of a company-wide information security training and awareness program
  - Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of company data