



Malicious Software (Malware)

Information Security (CSC-407)

Fall 2024 (BSE-7A & 7B)

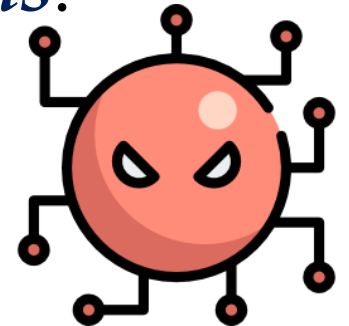
Software Attacks

- **Deliberate** software attacks occur when an attacker designs and deploys a software to attack a system.
- The attack can consist of specially crafted software that attackers **trick users** into installing it on their systems.
- These designed software are commonly known as **Malware** (Malicious Software).



Malware

- **Malware:** a program inserted into a system with the intent of compromising **confidentiality**, **integrity** or **availability** of the victim's data, applications or operating system **OR** to **annoy/disrupt** the victim.
- Malware can pose threats to *application programs*, *utility programs* (such as compilers) and *kernel-level programs*.
- Several approaches exist to classify malware.



Malware Classification

Two major approaches to classify malware:

- a. One approach classifies malware based on **the means malware uses to spread / propagate** to reach desired targets.
- b. Another approach classifies malware based on **the variety of actions / payloads used** once a target is reached.

Malware Classification (Cont.)

Propagation mechanisms include:

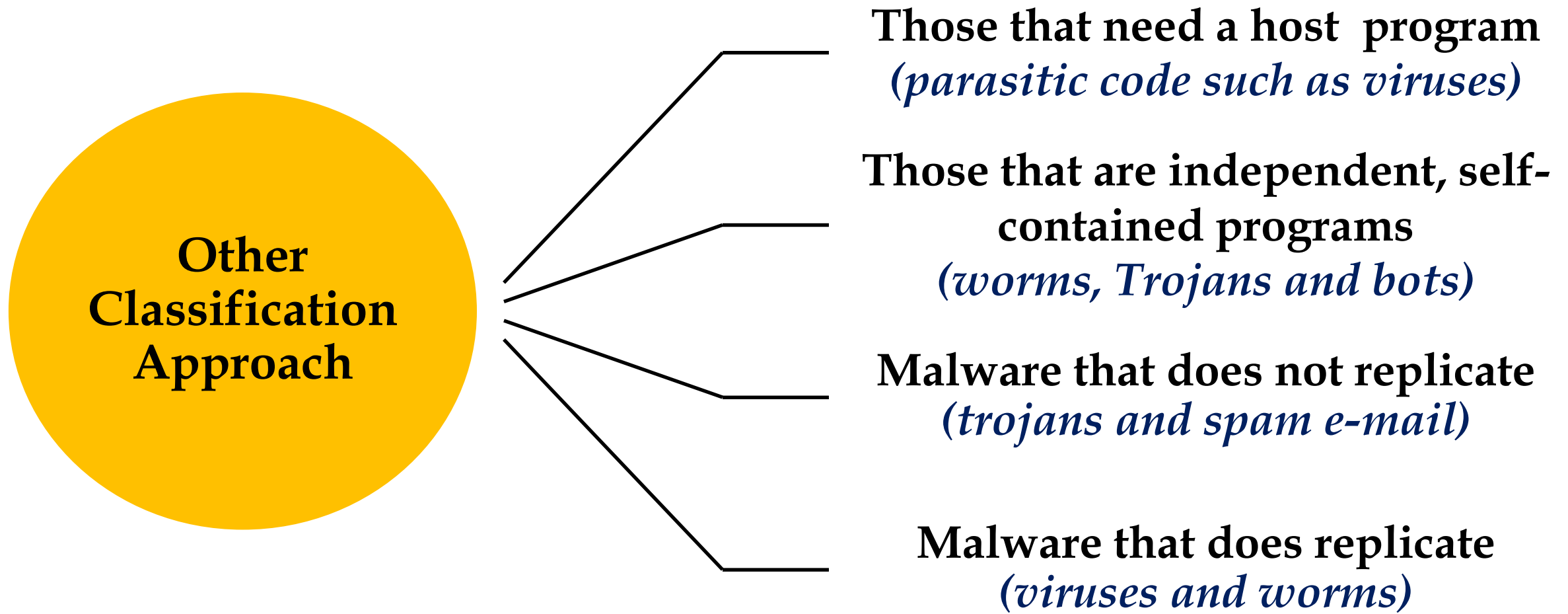
- **Infection of existing content** by **viruses** that is subsequently spread to other files.
- **Exploit of software vulnerabilities** by **worms** to allow the malware to replicate.
- **Social engineering** attacks that convince users to install **Trojans** or respond to **phishing attacks**.

Malware Classification (Cont.)

Payload actions performed by malware include:

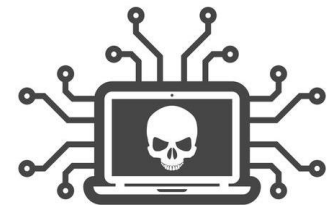
- **Corruption** of system or data files.
- **Theft of information** from the system, usually by **keylogging** or through **spyware** programs.
- **Theft of service** to make the system an attack **zombie agent** as part of a **botnet**.
- **Stealth** where malware hides its presence on the system.

Malware Classification (Cont.)



Blended Malware Attacks

- Currently, a growth of **blended malware attacks** are noticed.
- **Blended malware attacks** incorporates a range of both **propagation mechanisms** and **payloads**.
- Blending both techniques increase its ability to spread, hide and perform a range of actions on targets.
- **Polymorphic malware:** a type of malware that constantly changes its *identifiable features* to evade detection.



Attack Kits

- **Malware creation toolkits** and the more general **attack kits** greatly assist in development and deployment of malware.
- **These toolkits (crimeware) have following properties:**
 - Include a variety of **propagation mechanisms** and **payload modules** that even novices can deploy.
 - Can be customized with latest discovered vulnerabilities.
 - Malware from such toolkits tends to be less sophisticated.
 - New variants can be generated by attackers.
- **E.g.** crimeware toolkits: ***Zeus, Blackhole, Sakura, Phoenix.***

INTERNET WORM MAKER THING V4

Worm Name:

Author:

Version:
 .

Message:

☒ Include [C] Notice

Output Path:

☒ Compile To EXE Support

Spreading Options

Startup:

☐ Global Registry Startup

☐ Local Registry Startup

☐ Winlogon Shell Hook

☐ Start As Service

☒ English Startup

☐ German Startup

☐ Spanish Startup

☐ French Startup

☐ Italian Startup

Payloads:

☐ Activate Payloads On Date

Day: /

OR

☐ Randomly Activate Payloads

Chance of activating payloads:
1 IN CHANCE

☐ Hide All Drives

☐ Disable Task Manager

☐ Disable Keyboard

☐ Disable Mouse

☐ Message Box

Title:

Message:

Icon:

☐ Disable Regedit

☐ Disable Explorer.exe

☐ Change Reg Owner

Owner:

☐ Change Reg Organisation

Organisation:

☐ Change Homepage

URL:

☐ Disable Windows Security

☐ Uninstall Norton Script Blocking

☐ Disable Macro Security

☐ Disable Run Command

☐ Disable Shutdown

☐ Disable Logoff

☐ Disable Windows Update

☐ No Search Command

☐ Swap Mouse Buttons

☐ Open Webpage

URL:

☐ Change IE Title Bar

Text:

☐ Change Win Media Player Txt

Text:

☐ Open Cd Drives

☐ Lock Workstation

☐ Download File **More?**

URL:

☐ Save As:

☐ Execute Downloaded

☐ Print Message

☐ Disable System Restore

☐ Change NOD32 Text

Title:

Message:

URL:

Sender Name:

☐ Mute Speakers

☐ Delete a File

Path:

☐ Delete a Folder

Path:

☐ Change Wallpaper

Path Or URL:

☐ CPU Monster

☐ Change Time

Hour : Min

☐ Change Date

DD MM YY

☐ Play a Sound

☐ Loop Sound

☐ Hide Desktop

☐ Disable Malware Remove

☐ Disable Windows File Protection

☐ Corrupt Antivirus

☐ Change Computer Name

☐ Change Drive Icon

DLL, EXE, ICO: Index:

☐ Add To Context Menu

☐ Change Clock Text

Text (Max 8 Chars):

☐ Hack Bill Gates ?

☐ Keyboard Disco

☐ Add To Favorites

Name:

URL:

☐ Exploit Windows Admin Lockout Bug

☐ Blue Screen Of Death

Infection Options:

☐ Infect Bat Files

☐ Infect Vbs Files

☐ Infect Vbe Files

Extras:

☐ Hide Virus Files

Plugins

☐ Custom Code

If You Liked This Program Please Visit Me On
<http://xirusteam.fallennetwork.com>
If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.

Control Panel

JPS (Virus Maker 4.0)

Virus Options :

☐ Disable Registry

☐ Disable MsConfig

☐ Disable TaskManager

☐ Disable Telegram

☐ Disable Media Player

☐ Disable Internet Explorer

☐ Disable Time

☐ Disable Group Policy

☐ Disable Windows Explorer

☐ Disable Notepad

☐ Disable Wordpad

☐ Disable Windows

☐ Disable System Restore

☐ Disable Taskbar

☐ Disable Start Button

☐ Disable DHCP Client

☐ Disable CMD

☐ Disable Windows Update

☐ Disable Control Panel

☐ Disable Desktop Icons

☐ Disable Screen Saver

☐ Disable Browsers

☐ Disable Drives

☐ Hide Services

☐ Hide Windows Clock

☐ Hide Desktop Icons

☐ Hide Run

☐ Hide Taskbar

☐ Hide Cursor

☐ Swap Mouse Button

☐ Remove Folder Options

☐ Lock Mouse and Keyboard

☐ Always Open CD_ROM

☐ Turn Off Monitor

☐ Crazy Mouse

☐ Enable Remote Desktop

☐ Destroy Clipboard

☐ Lock Screen

☐ Mute Sound

☐ Remove Bluetooth

☐ Remove Windows Themes

☐ Slow Mouse Speed

☐ Turn Off Windows Firewall

☐ Turn Off Windows Defender

☐ Run In System Mode

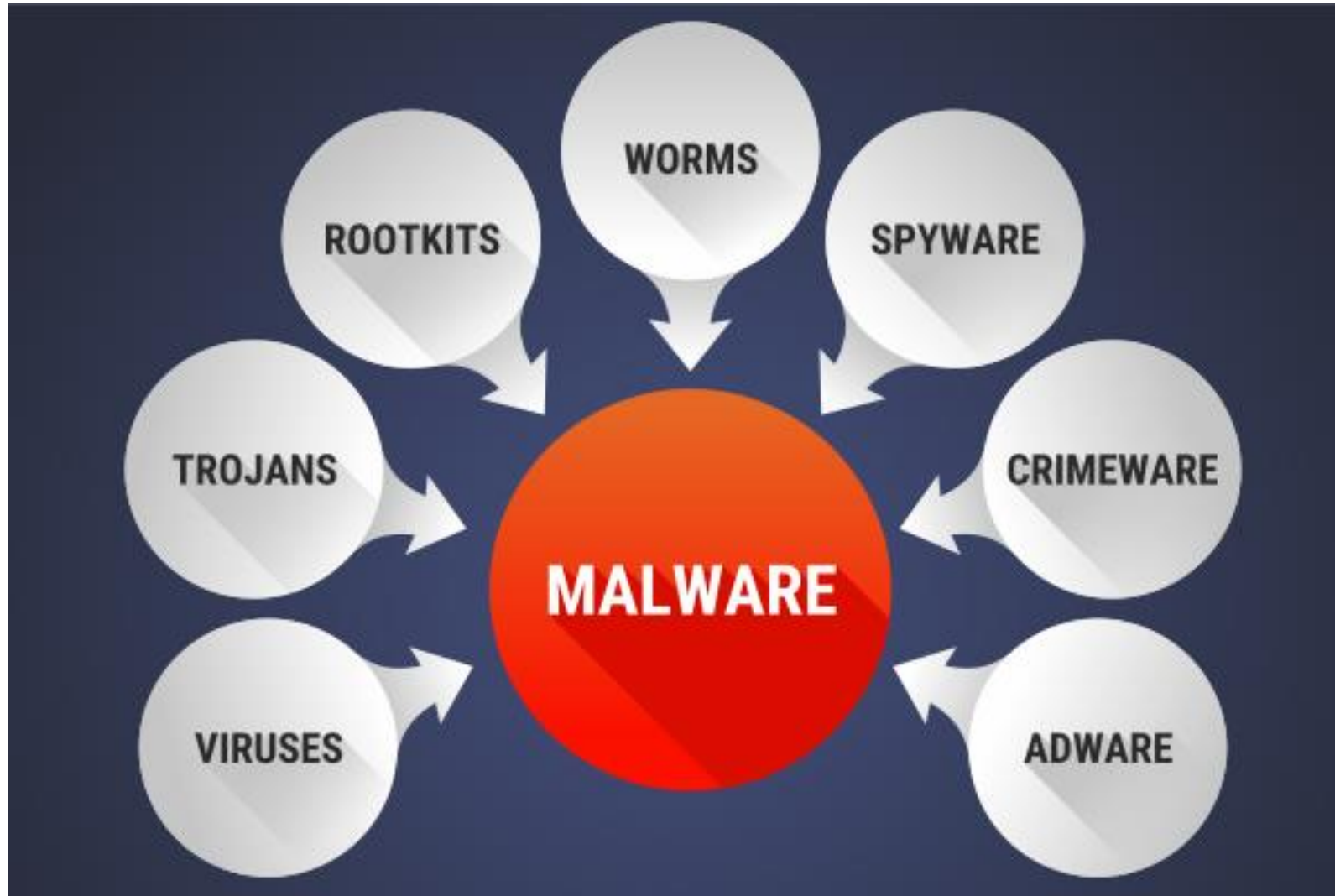
☒ Auto Startup

☐ Restart ☐ LogOff ☐ TurnOff ☐ Hibrinate ☒ None

Name After Install : **Server Name :**

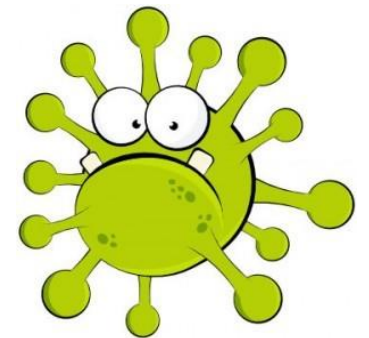
JPS Virus Maker 4.0

Malware Types



Computer Virus

- **Virus:** **parasitic software** fragments that attach themselves to some existing executable content (*i.e. infects*), and when executed, tries to replicate itself into other executable contents.
- Infections by computer virus formed the **majority of malware** seen in the early personal computer era.
- The term “**computer virus**” is still often used to refer to malware in general.



Nature of Computer Virus

- The **nature** of a computer virus include:
 - **Modifies** other programs by injecting the “**original code**” with a routine to make copies of the “**virus code**”, which can then go on to infect other content.
 - **Replicates** itself where the computer virus can make perfect copies of itself and goes on to infect other content.
 - **Easily spreads** by exchanging **carrier files** though USB stick or in a networked environments.

Nature of Computer Virus (Cont.)

- A virus can do anything that the program is permitted to do, i.e. allowed by *privileges* of the *current user*.
- Viruses dominated the malware scene in earlier years due to the *lack of user authentication* and *access controls* on personal computer systems at that time.
- Inclusion of tighter *access controls* on modern OS significantly hinders the ease of infection of such traditional viruses.
- Many forms of infection can also be blocked by denying normal users the *right to modify programs* on the system.

Computer Virus Lifetime

Typical virus goes through four phases during its lifetime:

1. Dormant phase

- Virus is **idle**, but will eventually be activated by some event.

2. Triggering phase

- Virus is **activated**.
- Can be caused by a variety of system events, such as *date, presence of another program or file, disk capacity exceeding some limit, a command*.

Virus Phases (Cont.)

Typical virus goes through four phases during its lifetime (Cont.):

3. Propagation phase

- Virus places a copy of itself into other programs.
- The copy may not be identical to the propagating version.
- Each infected program will contain a clone of virus which itself will enter a propagation phase.

4. Execution phase

- Function is performed.
- May be **harmless** or **damaging**.

Antiviruses

- Current software marketplace has several established vendors, such as:
 - *Avast*
 - *Bitdefender*
 - *Symantec Norton Antivirus*
 - *Kaspersky Antivirus*
 - *AVG Antivirus*
 - *McAfee VirusScan*
 - *Panda Antivirus*

Macro Computer Virus

- **Macro viruses:** a virus that attaches itself to documents and uses the **macro programming** capabilities of the document's application to execute and propagate.
- **Macro viruses** infect **scripting code** used to support the **active content** in a variety of user document types, such as **MS Word**, **Excel files** or **Adobe PDF**.



Macro Computer Virus (Cont.)

- More recently (since mid-1990s), **macro viruses** became by far the most prevalent type of virus.
- **Properties of such documents:**
 - Easily modified
 - Easily shared by users
 - Not protected by same *access controls* as programs

Macro Computer Virus (Cont.)

- Macro viruses are threatening for a number of reasons:
 1. Macro viruses are **platform independent**.
 - *Many macro viruses infect “**active content**” in commonly used applications.*
 - *Any **OS or hardware platform** that supports such applications can be infected.*
 2. Macro viruses **infect documents**, whereas most of the information shared among computer system is in the form of documents.

Macro Computer Virus (Cont.)

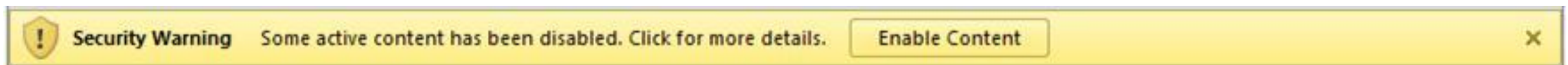
- Macro viruses are threatening for a number of reasons (Cont.):
 3. Macro viruses are easily spread as the documents they exploit are **shared commonly**, such as through **E-mails**.
 4. Traditional file system **access controls are of limited use** in preventing their spread.
 5. Macro viruses are much **easier to write / modify** than traditional executable viruses.

Microsoft Macro Security

- Macros are a powerful way to **automate tasks** in MS office. But, macro malware uses this functionality to infect devices.
- **MS Word** and **Excel** documents are common targets of **Macro viruses** due to their widespread use.
- Macro malware hides in MS office files and can be delivered as email attachments or inside ZIP files (*e.g. invoices, receipts, legal documents, etc.*).
- Macro malware was fairly common several years ago since macros **ran automatically** whenever a document was opened.

Microsoft Macro Security (Cont.)

- In recent versions of MS office, macros are **disabled by default**, while malware authors need to convince users to turn on macros so that their malware can run.
- Ways to prevent such viruses can be summarized as below:
 1. Microsoft offers a *Macro Virus Protection tool* that detects suspicious Word files and alerts the customer to the potential risk of opening a file with macros.

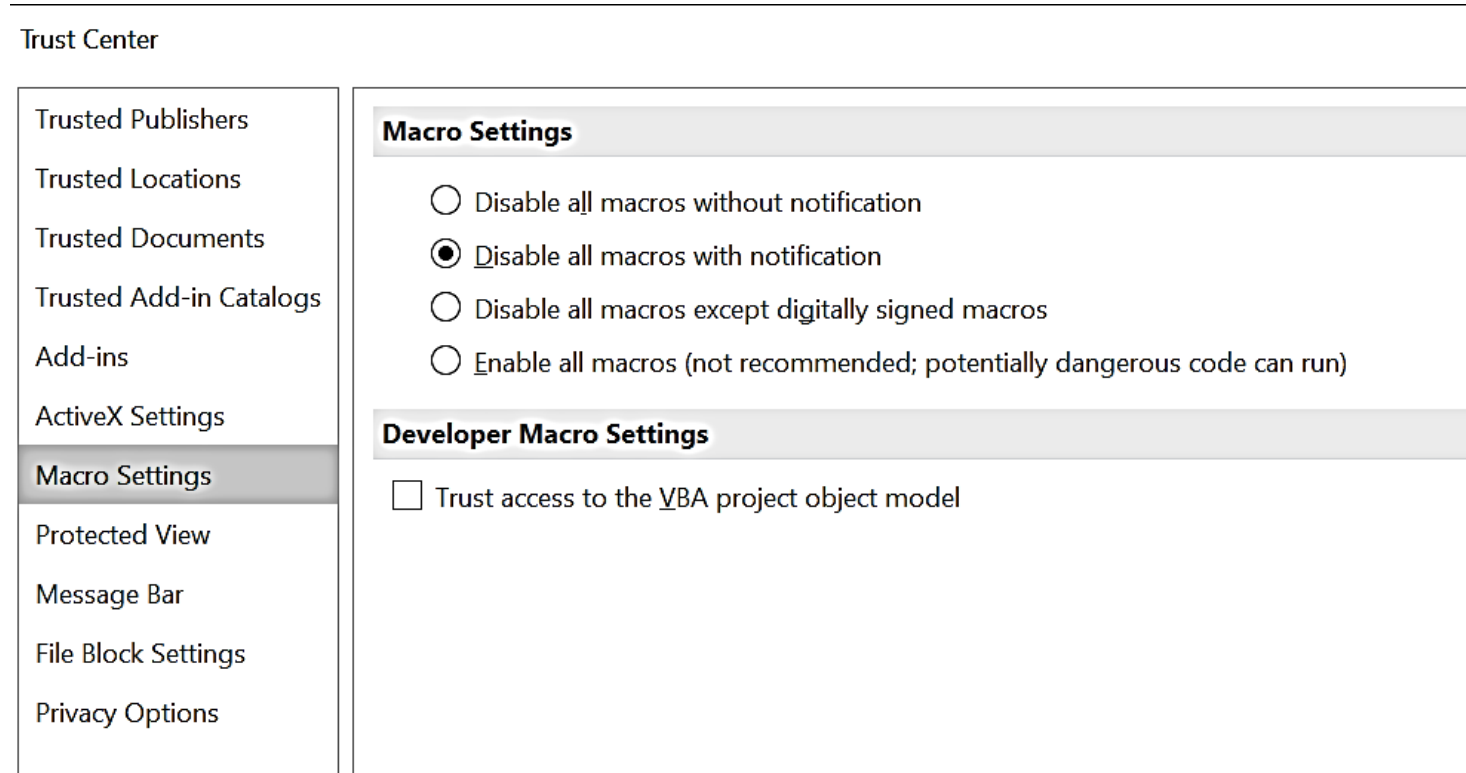


Microsoft Macro Security (Cont.)

- ...(Cont.):
 2. MS office allows macros to be **digitally signed** by their author and for authors to be **listed as trusted**. Users are warned if a document contains *unsigned* or *signed but untrusted* macros.
 3. Various **anti-virus** products have tools to detect and remove macro viruses.
 4. Avoid opening suspicious emails or attachments.

Microsoft Macro Security (Cont.)

- ...(Cont.):
 5. Make sure macros are **disabled** in MS office applications.



Microsoft Macro Security (Cont.)

- **Disable all macros without notification;** will allow only macros installed in trusted locations to run. Any other macros, *signed or unsigned*, will be disabled.
- **Disable all macros with notification;** will prompt you to choose whether or not a macro can run.
- **Disable all macros except digitally signed macros;** allows macros *signed by trusted publishers* to run automatically, and prompts you for *signed macros from other publishers*, and *prevents unsigned macros from running*.
- **Enable all macros;** allows all macros to run. This setting is not recommend, since it allows potentially dangerous code to run without warning.

Worm



- **Worm:** a computer program that can run *independently* and can propagate a complete working version of itself onto other hosts on a network while exploiting **software vulnerabilities**.
- The most state-of-the-art malicious code attack is the **multivector worm**.
- These worms can use several **attack vectors** (*up to six known attack vectors*) to spread copies of themselves to networked peer computers by exploiting a variety of vulnerabilities.

Worm (Cont.)

- Example of worms include; *Code Red, Sircam, Nimda and Klez.*
- **Nimda:**
 - Outbreak occurred in **Sept. 2001.**
 - Spread across the Internet address space of **14 countries** in less than **25 minutes.**
 - Used five different attack vectors.

Worm Possible Impact

A worm once infects a system can have following impact:

- Redistribute itself to e-mail addresses found on infected system.
- Take advantage of open shared resources on the network.
- Place copies of their code onto the server so that users are likely to become infected.

Virus/Worm Hoaxes

- **Case#01:** sending group e-mails warning of supposedly dangerous viruses that maybe does not exist.
- **Impact:** network becomes overloaded (*may also lead to DoS*), while users waste time and energy. Some of such hoaxes are known as **“weapons of mass distraction”**.
- **Correct Approach:** follow virus-reporting procedures.
- **Case#02: Teddy Bear** hoax (e-mail spam, 2002) tricked users into deleting necessary OS file (*jdbgmgr.exe*), which made their systems stop working.



jdbgmgr

Trojan Horse

- **Trojan horse:** a computer program that *appears to have a useful function*, but also has *a hidden and potentially malicious function* that evades security mechanisms.
- E.g. **SMiShing**, in which the victim is tricked into downloading malware onto a mobile phone via a text message.

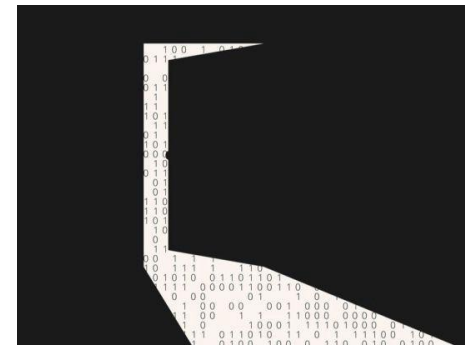


Spyware



- **Spyware:** software that secretly collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, network traffic, etc.
- E.g. “**tracking cookie**” placed on users’ computers to track their activity on different Web sites and create a detailed profile of their behavior.
- Can be used in a *social engineering* or *identity theft attack*.

Backdoors



- **Backdoor (trapdoor):** a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.
- Viruses and worms can have a payload that installs a **backdoor** or **trapdoor** component in a system, allowing the attacker to access the system at will with special privileges.
- **Backdoor** is hard to detect because the person or program that places it often makes the access **exempt** from the system's usual **audit logging** features.

Other Malware Types

- **Adware:** advertising that is integrated into software, that can result in pop-up ads or redirection to a commercial site.
- **Keyloggers:** a program that captures keystrokes on a compromised system.
- **Zero-day attack:** a software attack that makes use of a malware that is not yet known by the anti-malware software companies.
- **Zombie/bot:** program activated on an infected machine to launch attacks on other machines.

Thank You!