Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Malware

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Chapter Outline

- Definition and Categories
- Virus Overview, Lifecycle, and Types
- Worms, Spyware, and Trojans

Definition and Categories

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

What is Malware

- **Malware is short for malicious software. It is intended to perform malicious and disruptive tasks.**
- **Categories of malware**
  - **Viruses**
  - **Worms**
  - **Trojan horses**
  - **Rootkits**
  - **Spyware**
  - **Adware**

Categories of Malware

- **Viruses**
  - **Replicate and attach itself to other files. Usually needs a catalyst to start the infection.**
- **Worms**
  - **Have the ability to replicate on their own and very quickly.**
- **Trojan horses**
  - **Malware that is disguised as another, usually more legitimate program.**
- **Rootkits**
  - **Malware that's hidden in the core components of the operating system and can usually avoid detection.**

Categories of Malware

- **Spyware**
  - **Used to gather information about the target's system or their activities. For example, a key logger.**
- **Adware**
  - **Used to display intrusive and unwanted advertisements on the victims computer. They can sometimes replace items within the browser and install other products.**

Virus Overview, Lifecycle, and Types

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Virus Overview

- **Potential actions of a virus**
  - **Data alteration**
  - **Infecting additional programs**
  - **Replication**
  - **Encrypting itself**
  - **Transforming itself**
  - **Manipulation of configuration settings**
  - **Deletion of data**
  - **Corruption of data**
  - **Destruction of hardware**

Virus Lifecycle

- **Design**
  - The virus is either designed from scratch or through a construction kit.
- **Replication**
  - Once deployed the virus replicates across the system.
- **Launch**
  - The virus performs its specified task on the system
- **Detection**
  - After being recognized antivirus developers work on a detection method for the virus
- **Incorporation and elimination**
  - The antivirus developers push update to their software to identify and eliminate the virus.

Types of viruses

- **Boot sector virus**
  - **Infects the master boot record, which allows the virus to load before anti virus systems.**
- **Macro viruses**
  - **Written in an embedded language like Visual Basic or Excel.**
- **Cluster viruses**
  - **Alters the fie allocation table on storage devices to make file entries point to the virus.**
- **Tunneling viruses**
  - **Attempt to evade detection systems by interrupting command from the operating system or returning invalid responses.**

Types of viruses

- **Encryption virus**
  - **They change their own code through encryption to avoid virus detection software that depend on signatures or patterns.**
- **Cavity viruses**
  - **Hide in host files without altering the files appearance or size.**
- **Sparse-infector viruses**
  - **Does action sporadically to avoid detection**
- **Companion/ camouflage virus**
  - **A virus the run in conjunction to a legitimate file on the system.**

Types of viruses

- **Logic bombs**
  - **Wait until a predetermined even occurs before taking action.**
- **Multipartite viruses**
  - **The virus infects multiple ways and must be removed from each infected subsystem. If not, one infected file can reinfect the entire system.**
- **Shell viruses**
  - **Infects a program and forces the program to boot after the virus.**
- **Cryptoviruses**
  - **Searches for specific data on a system and encrypts it. Usually the encrypted data is held for ransom.**

Worms, Spyware, and Trojans

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Worms

- **Function of worms:**
  - **Does not require a host application to perform actions.**
  - **Does not require human interaction to initiate.**
  - **Replicates extremely fast.**
  - **Consumes bandwidth and resources.**
  - **Transmits data from victim to other locations.**
  - **Can carry a payload like a virus.**
  - **Does not attach itself to other applications.**
  - **Spreads automatically through systems unlike viruses.**

Spyware

- **Method of spyware infection**
  - **Peer to Peer network**
  - **Instant messaging**
  - **Internet relay chat**
  - **Email attachments**
  - **Physical access (USB)**
  - **Browser defects**
  - **Freeware**
  - **Websites**
  - **Software installation**

Trojans

- **Trojans rely on overt and covert channels.**
  - **Overt channels are communication paths that are normally used to send information legitimately.**
  - **Covert channels are communication paths that are being used to transmit data, but were not originally designed for this purpose.**
- **Types of trojans**
  - **Remote access trojans**
  - **Data sending**
  - **Destructive**
  - **Proxy**
  - **FTP**
  - **Security software disablers**

Types of Trojans

- **Remote access trojans**
  - Used to give an attacker remote control over a system.
- **Data sending**
  - Captures data from the victim and transmits it.
- **Destructive**
  - Corrupts, erases, or destroys data.
- **Proxy**
  - The attacker uses the system as a proxy.
- **FTP**
  - Uses the infected systems as a FTP server to store data.
- **Security software disablers**
  - Disable security software on the system.

Detecting Viruses and Trojans

- **Port scanning**
  - **This allows the user to see every open port on their system. They should look for unknown process names and covert channels.**
- **Track port usage**
  - **Investigate open or recently closed ports.**