Network Security

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

April 16, 2015

Malware

- *Malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted – and usually harmful – action* [cia14]
- a general term that refers to a wide variety of damaging or annoying software programs

Malware classification by primary objective

- Spreading
- Concealing
- Profiting

Malware

- Two types of malware that have a primary objective of spreading
- Virus and Worm

Virus

- A computer virus (virus) is malicious computer code that reproduces itself on the same computer
- Inserts itself into a computer file (which can be either a data file or program)
- Can only be transmitted from one computer to another through user copying the infected files

Computer virus

- On launching the infected file, the virus performs two actions
- First, it tries to reproduce itself by inserting its code into another file on the same computer
- Second, it unloads a malicious payload and performs some action
- Actions vary from displaying a simple annoying message to loss of data

Virus actions

- Caused a computer to crash repeatedly
- Erased files from a hard drive
- Made multiple copies of itself and consumed all of the free space in a hard drive
- Turned off the computer's security settings
- Reformatted the hard disk drive

Virus types I

- Program virus: infects program executable files (.EXE or .COM file extension). Virus is activated when the program is launched
- Macro virus: is written in a script known as a macro (a series of instructions that can be grouped together as a single command and are often used to automate a complex set of tasks or a repeated series of tasks
- Resident virus: is loaded into RAM each time the computer is turned on and infects files that are opened by the user or the operating system

Virus types II

- Boot virus: infects the Master Boot Record (MBR) of a hard disk drive. The MBR contains the program necessary for the computer to start up and a description of how the hard drive is organized (the partition table)
- Companion virus: adds a program to the operating system that is a malicious copycat version to a legitimate program (.com version of .exe version)
- The last two are rare these days

Worms

- A malicious program designed to take advantage of a vulnerability in an application or an operating system in order to enter a computer
- Once the worm has exploited the vulnerability on one system, it immediately searches for another computer that has the same vulnerability
- A worm uses a network to send copies of itself to other devices also connected to the network
- Worm can leave a payload behind to perform similar actions as virus does

Concealing malware

Primary objective of hiding their presence from the user

- Trojans
- Rootkits
- Logic bombs
- Back doors

Concealing malware

Trojans

- An executable program advertised as performing one activity, but actually does something else (may be both)
- Typically executable programs that contain hidden code that launches an attack
- Appearing of a program not to be executable is in fact executable and contains malicious code (New folder.exe)
- Apparently useful program containing a malicious code

Concealing malware

Rootkits

- Set of software tools used by an attacker to hide the actions or presence of other types of malicious software, such as Trojans, viruses, or worms
- Rootkits do this by hiding or removing traces of log-in records, log entries, and related processes
- Also change the operating system to force it to ignore any malicious activity
- One approach used by rootkits is to alter or replace operating system files with modified versions that are specifically designed to ignore malicious activity
- For example instructing operating system not to display malicious files

Concealing malware

Logic bombs

- Computer code that lies dormant until it is triggered by a specific logical event
- Once it is triggered, the program can then perform any number of malicious activities

Concealing malware

back doors

- Software code that gives access to a program or service that circumvents any normal security protections
- Might be legitimate left by programmers themseleves (not removed latter)
- Malware from attackers can also install backdoors on a computer

Profiting malware

Botnets

- Places the infected computer under remote control of an attacker
- Carried as a payload by worms, trojans and viruses
- The infected computer is called bot or zombie
- A logical network of numerous bots under the control of an attacker is called a botnet
- To steal information from the victims' computers and to launch attacks against other computers
- Sending massive amount of spam, spreading malware, manipulating online polls, flooding web servres to launch denial of service attack

Profiting malware

Spyware

- Malware that spies on users by gathering information without consent
- Automatic download: downloading and installing softwares without user's knowledge and consent
- Passive tracking: collecting information about user's activity (browsing history)
- System-modifying software: Mofiying configuration (browser home page, search page)
- Tacking software: Collecting personal information that may result in identity theft or fraud
- Slow performance, system instability, browser's new toolbars and menus, new shortcuts, hijacked home page, increased pop-ups are usually effects of spyware

Profiting malware

Adware

- A software program that delivers advertising content in a manner that is unexpected and unwanted by the user
- Infects the computer through using a virus, worm or trojan
- Installed adware typically displays advertising banners, pop-up ads, or opens new Web browser windows at random intervals
- Can also tack user's online activities to get him trapped in cusomised advertisements

Profiting malware

Keyloggers

- Captures and stores each keystroke that a user types on the computer's keyboard
- Can be later retrieved by the attacker or secretly transmitted to a remote location
- Can come as trojan or virus

Social engineering

- A means of gathering information for an attack by relying on the weaknesses of individuals
- Can involve psychological approaches (mental and emotional) as well as physical procedures

Social engineering

Phishing

- One of the most common forms of social engineering
- Sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information
- Users are directed to an imposter site where they are asked to provide personal information (passwords, credit card number)

Social engineering

Spam

- Unsolicited or irrelevent messages
- A lucrative business
- E-mail addresses are generated through softwares or purchased
- Spam messages containing certain words can easily be blocked by filters
- Spammers use graphical images of the text to avoid text-based filters

Social engineering

Hoax

- A false warning, often contained in an e-mail message claiming to come from the IT departmen
- Is used as a first step in an attack
- May incite user to change certain security configuation that may allow the attacker to compromise the system

Mark ciampia.
Security+ guide to network security fundamentals.
Course Technology, Boston, MA, 2014.