Malware

EECE6029

Yizong Cheng

3/11/2016

Malware

- trojan horse
- virus
- worm
- botnet
- keylogger
- rootkit
- ransomware

Trojan Horse

- a malicious program that misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it. --- Wikipedia
- It generally does not attempt to inject/propagate itself.
- The victim is duped into its installation.
  - The malware may invoke the commands necessary to start itself whenever the machine is rebooted.
- The victim does all the work.
- A trojan horse often hides a spyware.

NetBus (1998)

- written in 1998 by Swedish programmer Carl-Fredrik Neikter in Delphi for Windows operating systems
- The server holds port 12345 (12346, 20034 also used) on the infected computer.
- The client can remotely control the infected computer.
- In 1999, NetBus was used to plant 3,500 child porn images on the work computer of a law scholar in Lund University. He lost the position but was acquitted in 2004 when NetBus was discovered.

Sub7 (1999)

- Reverse netbus (subten) and replace ten with 7.
- Also plants a server for remote control of a Windows system.
- Added features
  - Webcam, sound recording, snapshots of screen
  - key-logging
  - use different ports
  - GUI on the client site
- Back Orifice is a variation for remote administration (RAT)

Worm, 1988

- Nov 2, 1988 Robert Morris, a graduate student at Cornell, released a self-replicating program called the worm into the Internet.
- It brought down thousands of computers.
- A 99 line C code (the bootstrap) invade a machine where it is compiled and executed and makes a connection to the machine it came from to upload and execute the main worm.
- It goes through the routing table on the machine and sends the bootstrap to another machine and repeats the same.
- Worm exploits buffer overflow in the finger daemon in the UNIX system and changes the return address to run a shellcode.

ILOVEYOU Worm, 2000

- A Visual Basic script written by Reonel Ramones and Onel de Guzman in the Phillippings for the latter's undergraduate thesis.
- The script was an attachment to an email with subject ILOVEYOU.
- over 50 million infections on Windows PCs within ten days
- cost billions of dollars to remove.

Rootkits

- A rootkit is a set of programs and files that attempts to hide its existence, even in the face of the determined efforts of the host to locate and remove it.
- It may run as a virtual machine (hypervisor) for the operating system to run at.
- It may contain malicious system calls to censor directory listing functions so that the rootkit is skipped.
- Often difficult to remove.

Where is the Rootkit Hiding?

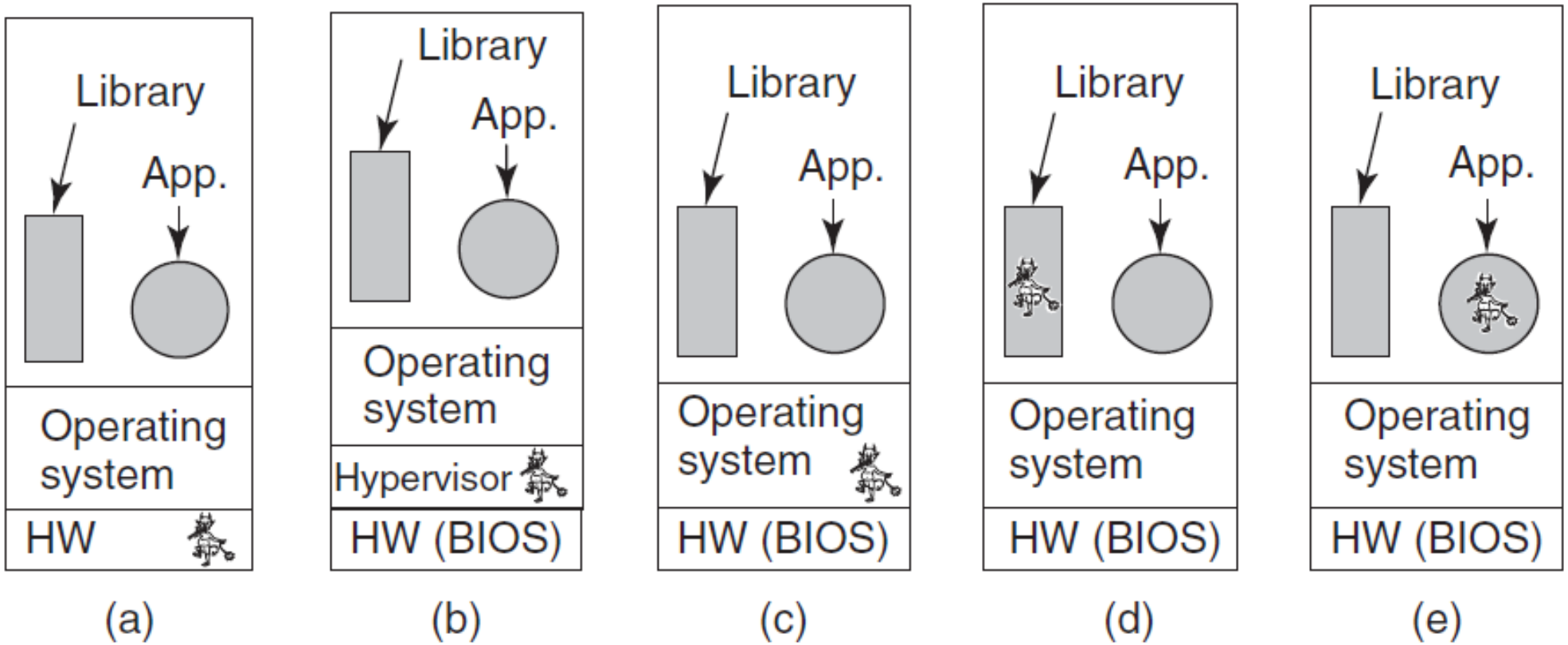

Figure 9-31. Five places a rootkit can hide.

Sony BMG Copy Protection Rootkit

- Sony put a rootkit on over 20 million audio CDs to infect computers on 500,000 networks, in 2005.
- There is no uninstallation available and the rootkit prevents copying songs from the CD to the hard disk.
- It also collects information and sends it back to Sony.
- Class action law suits in 2007.

Greek Wiretapping 2004-2005

- Rootkit software on Ericsson telephone exchanges used by Vodafone Greece.
- Firmware rootkit.
- More than 100 mobile phones including those used by the Greek prime Minister were tapped.
- The network planning manager for Vodafone Greece died after the discovery of rootkit.
- Investigation lasted 10 years and in 2015 an arrest warrant issued for a NSA operative.

Ransomware

- a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.
- Typically propagates as a trojan horse.
- AIDS trojan 1989 encrypts file names on the hard drive and demands $189. Symmetric cryptography is used.
- RSA is used in 1996 (Young and Yung) for Macintosh SE/30.
- Gpcode uses 1024-bit RSA key.
- CryptoLocker uses Bitcoin to collect $27 million ransom in 2013.