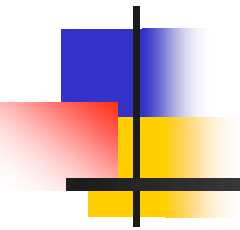

Malware and Defense

Professor Stephen S. Yau

What is Malware?

- A piece of software injected in an information system by attacker to cause harm to the system or other systems, or to subvert the ways using systems other than those intended by their owners
- Malware can be used to cause following troubles:
  - Gain unauthorized access to an information system
  - Steal sensitive data from an information system
  - Disable security measures of an information system
  - Damage an information system, both functional and non-functional
  - Compromise data and system integrity

Characteristics of Malware

- ***Multi-functional and modular***
- ***Difficult to detect***
- ***Easy to obtain***
- ***User-friendly***
- ***Enable broader cyber attack***
- ***Affect various devices and computers***
- ***Profitable***
- ***Self propagating and self replicating***

Definitions

- ***Trap Doors*** (also called ***Back Doors***)**:** *Holes in security* of a system deliberately left in places by designers or maintainers for privileged accesses
  - Some operating systems have privileged accounts for use by field service technicians or maintenance programmers.
  - Example, in Unix-style operating systems, ***root*** is the conventional name of the user who has all rights or permissions in all modes (single- or multi-users).

Definitions (cont.)

- ***Logic Bombs*: Code surreptitiously inserted in an application program or operating system to perform some *destructive* or *security-compromising* activity whenever specified conditions are met**
  - Example: In 1998, Timothy Allen Lloyd, a former chief computer network program designer was sentenced to 41 months in prison for unleashing a $10 million “logic bomb" 20 days after his dismissal. The “bomb” deleted all the design and production programs of Omega Engineering Corp., a New Jersey-based manufacturer of high-tech measurement and control instruments used by NASA and the U.S. Navy.

Definitions (cont.)

- ***Trojan horse*:** Malicious, security-breaking program that invites the user to run it, concealing its harmful or malicious activities.
  - Usually disguised as something normal or desirable software that users may be tempted to install without realizing hidden malicious functionalities.
  - Can be in the guise of various forms people find desirable, such as a freeware, game, movie, song.
  - Do not self-replicate, nor propagate to other computers by itself, but it can be spread out through WWW, FTP, P2P networks, IRC/instant messaging, email, social networks and mobile phone.

Definitions (cont.)

- Examples of Trojan Horse
  - **Gator**, spyware that covertly monitors web-surfing habits, uploads data to a server for analysis and then serves targeted pop-up ads..
  - **Qhost**, a Trojan that modifies the Hosts file to point to a different DNS server when banking sites are accessed and then opens a spoofed login page to steal login credentials for those financial institutions.

Definitions (cont.)

- ***Virus*: Program that *infects* one or more other programs by modifying them; modification includes a copy of virus program, which can then infect other programs**
  - A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels
  - Normally invisible to user
  - Virus may exist on your computer, but it cannot infect your computer unless you run or open the malicious program. A virus cannot be spread without a human action, such as running an infected program, to keep it going.

Definitions (cont.)

- Examples of Virus
  - **C-Brain:** Designed to infect the boot sector of the hard disks making the infected computer unbootable.
  - **Jerusalem**: Designed to activate only on Friday, January 13 and delete all the files executed on that day.
  - **Columbus** : Similar to Jerusalem and programmed to attack on October 13. Computer hard disk is destroyed and the contents of discs are rendered unreadable.

Definitions (cont.)

- ***Worm*: Program that propagates and reproduces itself as it goes over a network**
  - Only crackers write worms
  - ***Crackers***: a person engages in ***breaking computer security systems***
  - Similar to a virus by design, but unlike a virus, it has the capability of ***self-replicating and propagating without any human action***. The biggest danger with a worm is its capability to replicate itself on your system, rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

Definitions (cont.)

- Examples of Worm
  - **Melissa:** Looked through all ***Outlook address books*** and sent a copy of itself to the first 50 individuals. The first major e-mail worm and quickly spreaded around the world. The process of transferring so many messages overwhelmed many e-mail servers causing denial of service.

http://en.wikipedia.org/wiki/Melissa_(computer_virus)

  - **ILOVEYOU**: Came in an e-mail with "I LOVE YOU" in subject and contained an attachment that, when opened, would result in the message being re-sent to everyone in the recipient's Microsoft ***Outlook address book,*** and the loss of every JPEG, MP3, and other files on the recipient's hard disk. Reached about 45 million users in a day.

http://en.wikipedia.org/wiki/ILOVEYOU)

Definitions (cont.)

- ***Zombie*: Process that has terminated (either killed or exited) and its parent process has not yet received notification of its termination**
  - Exists as a process table entry
  - Consumes computer resources disrupting executions of other legitimate processes.

Definitions (cont.)

- ***Botnet:*** a group of computers compromised by malware controlled remotely by an attacker to carry out various attacks against targeted computer systems
  - A botnet usually consists of ***tens of thousands*** of compromised computers
  - More than 100 million computers in US are currently part of botnets*

*Emerging Cyber Threats Report 2011, Georgia Tech Information Security Center
http://www.gtise.gatech.edu/pdf/cyberThreatReport2011.pdf

Types of Attacks Using Malware

- Distributed Denial of Service (DDoS) attacks
  - Some malware, such as viruses and worms, seek to render an organization's websites or other network services by making them inaccessible by overwhelming them with an unusually large volume of traffic.
  - A large volume of traffic is generated by malware on compromised computers over the network.
  - This flood of traffic is intended to exceed the capacity of the network bandwidth and/or the computer resources of the targeted servers so that the services of these resources are unavailable or with degraded performance to their legitimate users.

Types of Attacks Using Malware (cont.)

- Compromising access control mechanism
  - Malware is used to compromise access control mechanism on target computers. Attackers gain unauthorized remote control over the compromised computers
- Compromising integrity of system
  - Damage or corrupt operating system, database or critical programs
  - Destruction or unauthorized modification of important data

Types of Attacks Using Malware (cont.)

- Espionage
  - Involves an organization or individual obtaining unauthorized information that is considered confidential without the permission of the holder of the information
- Stealing online identity
  - Some malware, such as spyware, can hide in a computer system and capture personal information covertly.

Types of Attacks Using Malware (cont.)

- Spreading spam emails
  - Some malware, such as viruses and worms, can be used to compromise computers, and spam emails can be sent out through these compromised computers to email servers across the Internet.
  - The spam emails may contain embedded malware or a link to a malicious website for phishing attack.

Trends of Malware Attacks

- More sophisticated
- Using increasingly deceptive social engineering techniques to entice users
- Blended, multi-faceted and phased attacks
- Large scale targeted attacks
- More powerful and destructive
- More prevalent through social networks and mobile devices.

Malware Propagation Mechanisms

- Email and instant messaging applications
- World Wide Web (WWW)
- Removable media (such as USB storage)
- Network-shared file systems
- P2P file sharing networks
- Bluetooth and wireless networks

Vulnerabilities Exploited by Malware

- Insecure software design and related software vulnerabilities, e.g. Milissa
- Coding bugs
- Improper software configuration
- Poor user practices
- Inadequate security policies and procedures
- Social engineering, e.g. ILOVEYOU
- Vulnerabilities in hardware

Vulnerabilities Exploited by Malware (cont.)

- Once these vulnerabilities are discovered, malware can be developed by attackers to exploit the vulnerabilities for malicious purposes before the security community has developed a patch.
- Once malware compromises an information system, the malware may install additional more powerful malware

Challenges to Fighting Malware

- Malware and the underlying criminal activities supporting the malware are ***rapidly evolving*** and taking advantage of the global nature of the ***Internet*** and ***social networks***.
- Many organizations and individuals do ***not have the resources, skills or expertise to prevent and/or respon***d effectively to malware attacks and the associated secondary crimes from those attacks, such as identity theft, fraud and DDoS.
- It is difficult for an organization to combat malware because it is ***unable to keep up*** with the overwhelming amount of malware.

Challenges to Fighting Malware (cont.)

- Most security technologies, such as anti-virus or anti-spyware products, are ***signature–based*** and hence they can only detect ***known malware***. Signature-based solutions are insufficient to combat complex and prevalent malware.
- Attackers exploit the distributed and ***global*** nature of the ***Internet*** as well as the complications of ***laws and jurisdictions*** bound by ***traditional geographical*** boundaries to reduce the risks of being identified and prosecuted.
- There is always a ***time lag*** between when new malware is released by attackers, and when it is discovered and prevented.

Challenges to Fighting Malware (cont.)

- Easy for attackers to ***target*** average Internet users, who are not adequately informed how they can securely manage their information systems.
- Common monolithic OS in widespread use ***sharing the same vulnerabilities*** gives attackers big incentive for generating malware.
- ***Internet, wireless networks, social networks, mobile devices and clouds*** provide extensive connectivity, by which malware can be spread quickly.

Malware Prevention

- Reduce system vulnerabilities
  - Reduce vulnerabilities in systems, such as design flaws and coding bugs.
  - Always ***patch*** your system and software ***up-to-date***.
  - Run ***security tests,*** such as penetration tests and fuzz tests thoroughly and frequently
  - ***Risk management***: identifying, tracking, and mitigating security risk over system lifetime
  - ***Plan on failure:*** Handling damages by malware gracefully (system backup and contingency planning)
  - ***Create quality gates/Bug bars*** to define acceptable levels of security and privacy quality

Malware Prevention (cont.)

- Establish robust ***access control mechanisms and security policies***.
  - Use ***least privilege***.
  - Check security policies for ***inconsistency and incompleteness.***
  - Four types of access control for preventing malware
    - **Network access control** to check computers to meet your security policies before allowing them on network
    - **Application control** to stop installing unauthorized applications
    - **Device control** to prevent use of unauthorized devices
    - **File type control** to minimize impact of high-risk and suspicious downloads

Malware Prevention (cont.)

- ***Honeynet:*** Prevent malware proactively.
  - A ***honeypot*** is a computer system set up with intentional vulnerabilities to attract malware and gather information about the malware.
  - A ***honeynet*** is a network of honeypots, and usually has security-sensitive applications and services running so that it seems to be a worthwhile target for attackers
  - Many honeynets are used for studying malware's motives, activities, methods, and fingerprints http://www.honeynet.org/

Malware Prevention (cont.)

- ***Anti-malware software:*** Prevent, detect and remove viruses, worms, and Trojan horses.
  - Signature-based detection for known malware.
  - Heuristic analysis, such as ***generic detection***, for detecting variants of known malware
    - Trojan-Downloader:W32/Mebroot.gen!B

      (a Generic Detection for variants of the Mebroot trojan-downloader family covering a "set of characteristics B") http://www.f-secure.com/v-descs/trojan-downloader_w32_mebroot_gen!b.shtml

Malware Prevention (cont.)

- ***Firewalls***: Block unauthorized access to protected software systems
- ***Intrusion detection***: Monitors abnormal system behavior or attack patterns
- ***Sandbox***: Provides isolated environment for safely executing untested code from unverified third-parties, suppliers and untrusted users.*

*http://en.wikipedia.org/wiki/Sandbox_(computer_security)

Malware Prevention (cont.)

- ***Fuzz testing*** -- provide invalid, unexpected, or random data as inputs to a program
  - The program is monitored for occurrences of exceptions, such as crashes, or failing built-in code assertions, or for finding potential memory leaks.
  - Two forms of fuzzing program, *mutation-based* and *generation-based*, which can be employed to generate inputs for white-, grey-, or black-box testing
- ***Create quality gates/Bug bars***, Set a meaningful bug bar which involves clearly defining the severity thresholds of security vulnerabilities and never relaxing it once it has been set,
  - Example, there should be no known vulnerabilities in the application with a “critical” or “important” rating at time of release

Malware Prevention (cont.)

- ***Software vendors:*** Developing trustworthy, reliable, safe and secure software.
- ***Anti-virus vendors:*** Providing security solutions to users (such as updating anti-virus software with the latest information on malware).
  - Examples: Symantec, AVAST and McAfee
- ***Internet Service Providers (ISPs):*** Preventing distribution of malware through their networks by scanning and blocking network traffics containing malware.
  - Use network tools to monitor, collect and analyze router and traffic data. http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
  - Block any malicious traffics using firewalls.

Malware Prevention (cont.)

- ***Law enforcement entities:*** Mandate to investigate and prosecute cybercrime related to malware.
- ***Government agencies:*** Managing risks to the security of government information systems and critical information infrastructure.
- ***Governments and inter-governmental organizations:*** Developing national and international policies and legal instruments to enhance prevention, detection and response to malware proliferation and its related crimes.

Malware Prevention (cont.)

- ***R&D***
  - Malware detection and analysis
  - Anti-malware development
  - Intrusion detection and malware filtering
  - Computer forensics
  - Recovery from damages of malware
- ***Global partnership***
  - Establish a strong partnership among industry, academia, standardization bodies and government for sharing information on discovered malware effectively.
  - Share information on malware's motives, activities, methods, fingerprints, prevention and recovery mechanisms.

Malware Prevention (cont.)

- Improving ***awareness and education on malware***
  - Malware often uses social engineering skills to deceive users. (exploits human aspects of computing)
  - Social engineering cannot be prevented by technologies.
    - Human aspects are unpredictable.
    - The weakest link in any security scheme is ***the user***.

Malware Prevention (cont.)

- Improving ***awareness and education on malware*** (cont.)
  - Educate users about social engineering
    - Avoid downloading or running software from ***unknown or untrusted web sites***
    - Never open attachments or click on links in emails from ***unknown or untrusted senders***
    - Do not install ***pirate, unlicensed or unapproved software***
    - Do not insert ***untrusted storage media***
    - ***Scan files*** for malware before copying or opening
    - Never install ***untrusted software on your mobile devices***
    - Make sure all software is kept ***updated*** with latest security updates

Resources for Fighting Malware

- Microsoft Malware Protection Center
  www.microsoft.com/security/portal/
- Malware Research Group
  www.youtube.com/user/MalwareResearchGroup
- Prevx Malware Center
  www.prevx.com/malwarecenter.asp
- Malware Threat Center mtc.sri.com/
- International Conference on Malicious and Unwanted Software (Malware 2012)

  isiom.wssrl.org/

References

- United State Computer Emergency Readiness Team (http://www.us-cert.gov/)
- Help Net Security Malware Center (http://www.net-security.org/malware_center.php)
- Microsoft Malware Protection Center (http://www.microsoft.com/security/portal/)
- Malware Research Group (http://malwareresearchgroup.com/)
- Prevx Malware Center (http://www.prevx.com/malwarecenter.asp)
- Malware Threat Center (http://mtc.sri.com/)
- International Conference on Malicious and Unwanted Software (Malware 2011) (http://isiom.wssrl.org/)
- 2012 Virus Bulletin International Conference (VB 2012) (http://www.virusbtn.com/conference/vb2012/index)