CSE 465

Information Assurance and Security

Malware and Defense

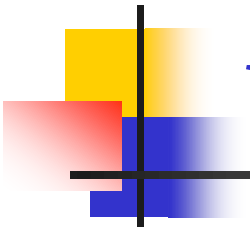
Professor Stephen S. Yau

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 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***

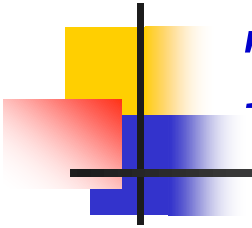
Characteristics of Malware

- ***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***



Well Known Malware

- Virus
- Worms
- Trojan horses
- Trap doors
- Logic bombs
- Zombie
- . . . . . .



Trap Doors

- ***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).

Logic Bombs

- ***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.

Trojan Horse

- ***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.

Trojan Horse (Cont.)

- Examples of Trojan Horse
  - **Bancos**, an info stealer that waits for the user to access banking websites, and then spoofs pages of the bank website to steal sensitive information.
  - **Gator**, spyware that covertly monitors web-surfing habits, uploads data to a server for analysis and then serves targeted pop-up ads.
  - **LegMir**, spyware that steals personal information, such as account names and passwords related to online games.
  - **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.

Virus

- ***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.
  - 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
  - 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 human action, such as running an infected program, to keep it going.

Virus (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. This infects the COM and EXE files.
  - **Columbus** : Similar to Jerusalem and programmed to attack on October 13. Computer hard disk is destroyed and the contents of discs are rendered unreadable.

Worm

- ***Worm*: Program that propagates and reproduces itself as it goes over a network**
  - Worms are written by ***Crackers***: who are engaged 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 thousands of copies of itself, creating a huge devastating effect.

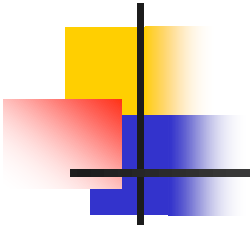
Worm (Cont.)

- 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)



Zombie

- ***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.

Botnet

- ***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.news.gatech.edu/hg/file/25892

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.
- Compromising access control mechanism
  - Compromise access control mechanism on target computers, and gain unauthorized remote control over compromised computers
- Compromising integrity of system
  - Damage or corrupt operating system, database or critical programs to cause destruction or unauthorized modifications of important data

Attacks Using Malware (Cont.)

- Stealing online identity
  - Some malware, such as spyware, can hide in a computer system and capture personal information covertly.
- Spreading spam emails
  - Some malware, such as viruses and worms, can be used to compromise computers, and spam emails can be sent 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
- Coding bugs
- Improper software configuration
- Poor user practices
- Inadequate security policies and procedures
- Social engineering
- Vulnerabilities in hardware
- Once these vulnerabilities are discovered, malware can be developed to exploit the vulnerabilities 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

- Do ***not have the resources or expertise*** ***to prevent or respon***d to ***malware attacks and associated secondary crimes from those attacks,*** such as identity theft, frauds and DDoS.
- Most security technologies are ***signature–based*** and can only detect ***known malware***. Signature-based solutions are insufficient
- ***Global*** nature of the ***Internet*** as well as the complications of ***laws and jurisdictions*** bound by ***geographical*** boundaries to reduce the risks of being identified and prosecuted.
- ***Time lag*** between when a new malware is released by attackers, and when it is discovered and prevented.
- Common monolithic OS ***sharing same vulnerabilities***
- ***Internet, social networks, mobile devices and clouds*** provide extensive connectivity, by which malware can be spread quickly.

Malware Prevention

- Reduce system vulnerabilities
  - 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***)
  - ***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***
  - 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.)

- ***Entities and Programs***
  - *Software vendors, anti-virus vendors, Internet service providers*
  - *Governments and inter-governmental organizations*
  - *R&D*
  - *Global partnership*
  - *Improving awareness and education on malware*
  - ****
- ***Tools and Techniques***
  - *Firewalls, sandbox*
  - *Intrusion detection*
  - *Fuzz testing*
  - *Create quality gates/bug bars*
  - ****

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)
- Prevx Malware Center (http://www.prevx.com/malwarecenter.asp)
- 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)