

Malware (*Malicious Software*)

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 7 November 7th, 2005

What is Malware?

- Type of software designed to take over and/ or damage a computer user's operating system, without owner's knowledge or approval.
- Once installed, it is often very difficult to remove
- Damage can range from slightly annoying (such as unwanted pop up ads) to irreparable damage requiring the reformatting of one's hard drive
- Often goal is to use a compromised computer as a staging ground for further abuse, concealing origins of original perpetrator

Aims of Malware

- Malware typically contains a payload with one or more undesirable functions.
- Some display political or ideological messages when activated.
- Some delete files or formats disks.
- Some install software for remote control of host

What is a Virus?

- A computer program that self-replicates and infects other hosts
- Usually has some unpleasant side-effect
- Rapid spread itself can cause network DOS

Virus “Hosts”

- Early common targets were executable files that are part of application programs and the boot sectors of floppy disks
- Email attachments most common today, depending on a stu^H^H^H—curious user opening the viral attachment
- Peer to peer (P2P) softwares newer culprit in the propagation of viruses

Virus Mutations

- Often less adept programs make malicious variants of original (which are often just scripts)
- Some have their own email engines or scan other files besides Outlook address book
- Some are not code but just plausible requests that get people to do dumb things (delete jdbgmgr.exe system file)

Virus vs. Worm

- Virus Attack Vector: requires user interaction (e.g. user reading an email, clicking a hyperlink, or reading an attachment)
- Virus Propagation: infected machine sends an email (using Outlook capabilities) to other users whom perform desired action
- Worm Attack Vector: takes advantage of a vulnerability on an un-patched computer system
- Worm Propagation: After the worm has compromised the system, scans for connections on network and propagates without user interaction
- Worms are more sophisticated and dangerous than a virus

Wabbit

- Unlike viruses, wabbits do not infect host programs or documents.
- Unlike worms, wabbits do not use network functionality in order to spread to other computers.
- A wabbit repeatedly replicates itself on a local computer.
- Wabbits can be programmed to have (malicious) side-effects, in addition to the direct consequences of their quick self-replication.
- An example of a simple wabbit is a fork bomb (uses up process table)

Trojan

- A trojan horse program is a harmful piece of software that is disguised as legitimate software.
- Trojan horses cannot replicate themselves
- Spread by deliberately attached to otherwise useful software
- Also spread by tricking users into believing that it is useful
- Some trojan horses can spread or activate other malware (‘droppers’).

Backdoor

- Allows access to the computer system bypassing the normal authentication procedures.
- Some work like a Trojan: manually inserted into another piece of software, executed via their host software and spread by their host software being installed.
- Some works like a worm: they get executed as part of the boot process and are usually spread by worms carrying them as their payload.
- Ratware: backdoor malware that turns computers into zombies for sending spam.
- Can also be used for anonymizing traffic, brute force cracking of passwords and encryptions, and distributed denial of service attacks (DDOS).

- May also allow processes started by a non-privileged user to execute functions normally reserved for the superuser.

Spyware

- Spyware is a piece of software that collects and sends information about users activity without explicit notification.
- Usually work and spread like Trojan horses.
- Sometimes taken to include adware of the less-forthcoming sort.

Key Logger

- Software that copies a computer user's keystrokes to a file, which it may send to a cracker at a later time.
- Often will only "awaken" when a computer user connects to a secure website, such as a bank.
- Logs the keystrokes, which may include account numbers, PIN's and passwords, before they are encrypted by the secure website.
- Also used by law enforcement, parents and suspicious spouses

Dialers

- Dials out on modem (becoming less common as broadband spreads)
- Replaces the phone number in a modem's dial-up connection with a long-distance number, often out of the country, in order to run up phone charges on pay-per-dial numbers, or d
- Or, dials out at night to send keylogger or other information to a hacker

Browser Hijacker

- Any program designed to alter a computer user's browser settings.
- New web sites added to the user's bookmarks
- The replacement of user's home page to one set by the author

Malicious Web-based Code

- ActiveX controls allow using IE to do just about anything on your computer
- Java, Javascript, Visual Basic Script also used
- May grow in use as AJAX becomes more popular

Virus Scanners

- Searches for signature or pattern of a known virus
- Watches for types of behaviors of viruses
- Searches for Terminate and Stay Resident (TSR) files in memory
- Amavis, ClamWin and Spybot S&D

Virus-Scanning Techniques

- E-mail and attachment scanning (server-based is best)
- Download scanning
- File scanning on demand
- Heuristic scanning (false positives and miss actual)
- Active X scanning

Rootkit

- Set of software tools used by intruder to hide presence of his malicious software in operation
- Often includes backdoor for controlling the host
- Conceals logins, running processes, files, logs or other system data
- May intercept data from terminals, network connections, and the keyboard for purposes of concealment
- Originally referred to a set of recompiled Unix tools such as "ps", "netstat", "w" and "passwd" that would carefully hide any trace of the intruder those commands normally display, allowing intruders to maintain "root" on the system without the system administrator seeing them.

- Also used by spyware to hide from anti-spyware software and make uninstallation difficult.
- Kernel level rootkits add/replace a portion of kernel code (device driver, module) with modified code to help hide a backdoor on a computer system. Extremely difficult to detect.
- Application level rootkits may replace regular application binaries with trojanized fakes, or they may modify the behavior of existing applications using hooks, patches, injected code, or other means.
- In general, a rootkit limits itself to maintaining control of one system

Rootkit Detection and Removal

- Shut down the computer suspected of infection and check its storage by booting from an alternative media
- Unix: chkrootkit and rkhunter — allows you to use alternative binaries or / (run from Knoppix)
- Blacklight is available in beta on F-Secure's website.
- Removing rootkits — save the data files, reformat disk and re-install OS

Rootkits as Copy Protection

- Sony is using a form of copy protection, or digital rights management, on its CDs called "XCP-Aurora" which constitutes a rootkit,
- Surreptitiously installs itself in a cloaked manner on the user's computer and resists attempts to detect, disable, or remove it.
- Sony released a patch to remove this rootkit but the patch itself requires ActiveX controls to install and adds things to the system,
- A class-action lawsuit has been filed on behalf of California consumers who may have been harmed by anti-piracy software installed by some Sony music CDs
- A new Trojan horse that exploits the controversial Sony DRM (Digital Rights Management) copy protection has been detected

- Sony announced suspension of use of XCP-Aurora