Malware
CS 136
Computer Security

Peter Reiher

February 26, 2008

Outline

- Introduction
- Viruses
- Trojan horses
- Trap doors
- Logic bombs
- Worms
- Botnets
- Spyware
- Some related topics
  - Hoaxes
  - Rootkits

Introduction

Clever programmers can get software to do their dirty work for them

Programs have several advantages for these purposes

- Speed
- Mutability
- Anonymity

Where Does Malicious Code Come From?

- Most typically, it's willingly (but unwittingly) imported into the system
  - Electronic mail (most common today)
  - Downloaded executables
    - Often automatically from web pages
  - Sometimes shrink-wrapped software
- Sometimes it breaks in
- Sometimes an insider intentionally introduces it

Is Malicious Code Really a Problem?

- Considering viruses only, by 1994 there were over 1,000,000 annual infections
  - One survey shows 10-fold increase in viruses since 1996
- In November 2003, 1 email in 93 scanned by particular survey contained a virus
- 2007 FBI report shows 52% of survey respondents had virus incidents
  - Viruses caused the second most economic damage of all attacks to respondents

More Alarming Statistics

- In 1992, there were around 2000 unique viruses known
- Today, Symantec’s databases of viruses includes 73,000+ entries
- Kaspersky Labs has over 580,000 virus signatures in its database
- The numbers continue to grow

But Don’t Get too Alarmed

- Most viruses are never found “in the wild”
- Most viruses die out quickly
- The Wild List[1] shows 590 active viruses worldwide (January 2008)
  - With another 2057 with only a single incident reported
  - Many on both lists are slight variants on a particular virus

[1] www.wildlist.org

How Much Do Viruses Cost?

- Group called mi2g estimated that MyDoom worm cost $38.5 billion worldwide
  - Cleanup costs, lost productivity, etc.
- Many folks believe this (and other estimates) are bogus publicity stunts
  - Methodology lacking for real estimates
- Even if it's two or three orders of magnitude off, that's serious money

But Do I Really Have to Worry About Viruses?

- "After all, I run Linux/Mac OS/Solaris/BSD"
- "Aren't all viruses for Windows?"
- Mostly true in practice
  - Definitely not true in theory
  - First MacOSX virus discovered one month ago
    - OSX/Leap-A
- Anyone, at any time, can write and release a virus that can clobber your machine, regardless of what OS you run

Viruses

- "Self-replicating programs containing code that explicitly copies itself and that can 'infect' other programs by modifying them or their environment"
- Typically attached to some other program
  - When that program runs, the virus becomes active and infects others
- Not all malicious codes are viruses

How Do Viruses Work?

- When a program is run, it typically has the full privileges of its running user
- Including write privileges for some other programs
- A virus can use those privileges to replace those programs with infected versions

Typical Virus Actions

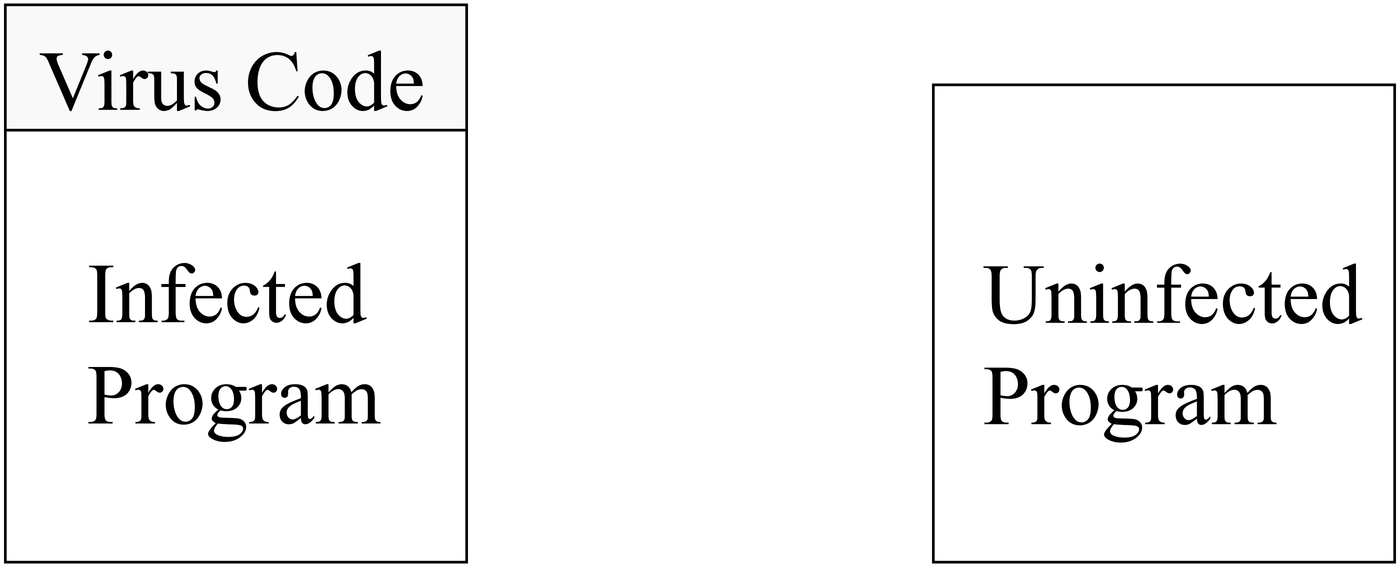
1). Find uninfected writable programs

2). Modify those programs

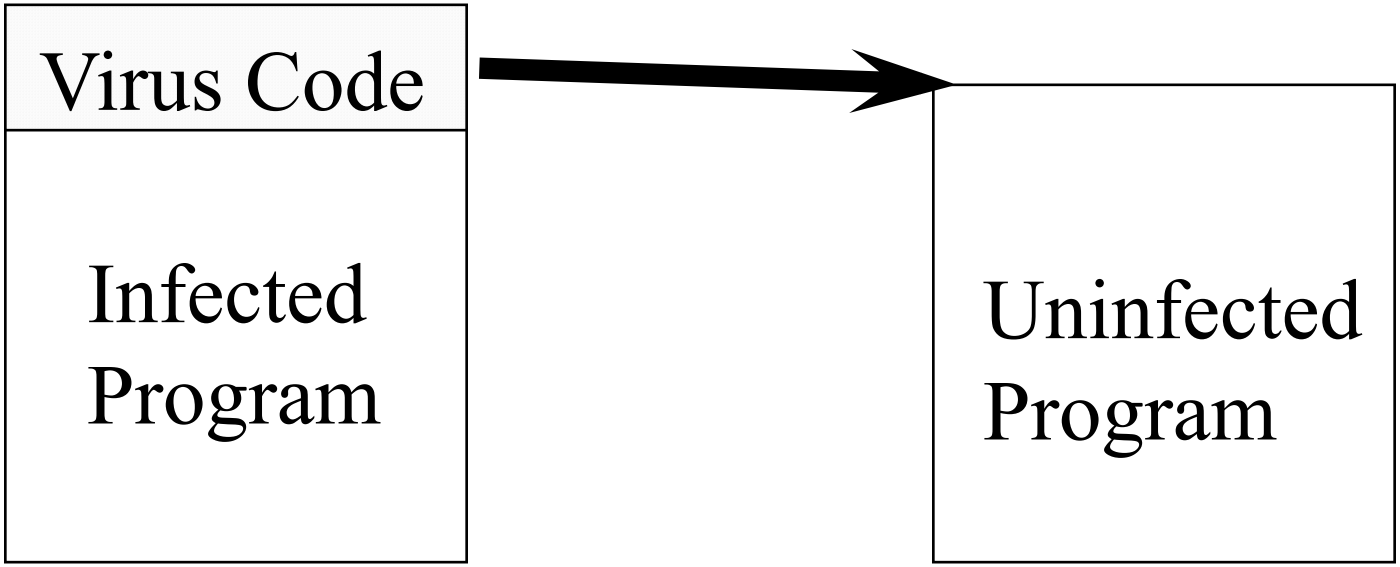
3). Perform normal actions of infected program

4). Do whatever other damage is desired

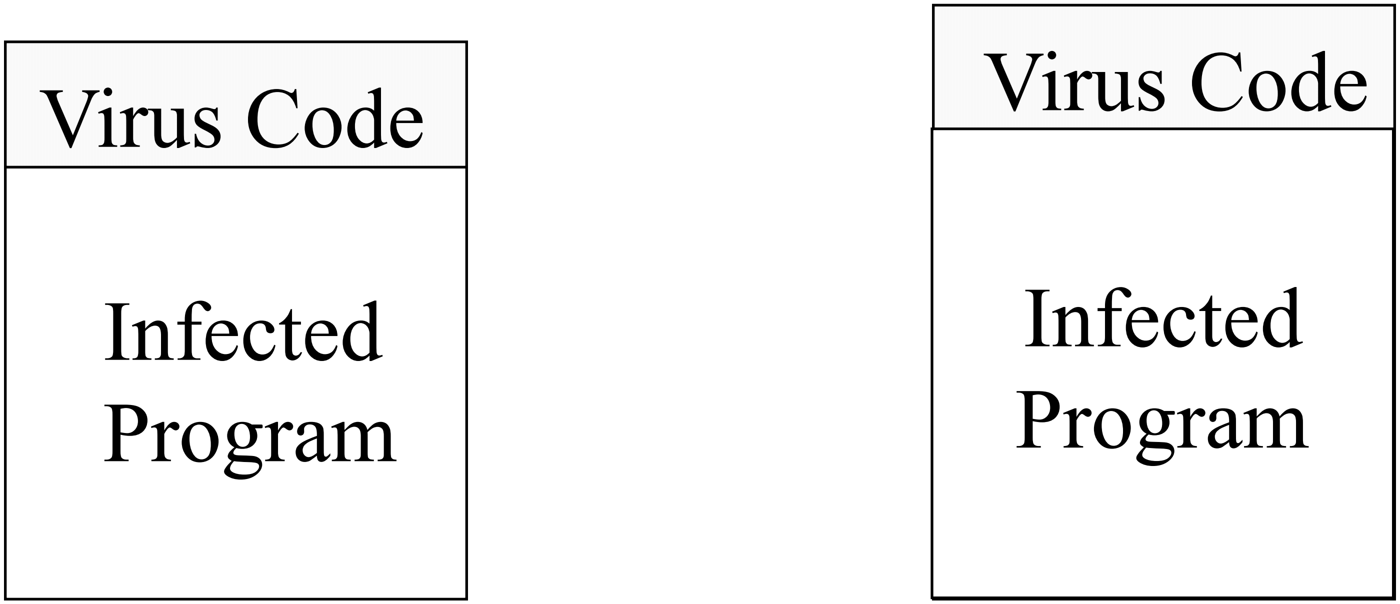
Before the Infected Program Runs



The Infected Program Runs



Infecting the Other Program



Macro and Attachment Viruses

- Modern data files often contain executables
  - Macros
  - Email attachments
  - Ability to run arbitrary executables from many applications, embedded in data
- Easily the most popular form of new viruses
  - Requires less sophistication to get right
- Most widespread viruses today use attachments

Virus Toolkits

- Helpful hackers have written toolkits that make it easy to create viruses
- A typical smart high school student can easily create a virus given a toolkit
- Generally easy to detect viruses generated by toolkits
  - But we may see "smarter" toolkits

How To Find Viruses

- Basic precautions
- Looking for changes in file sizes
- Scan for signatures of viruses
- Multi-level generic detection

Precautions to Avoid Viruses

- Don’t import untrusted programs
  - But who can you trust?
- Viruses have been found in commercial shrink-wrap software
- The hackers who released Back Orifice were embarrassed to find a virus on their CD release
- Trusting someone means not just trusting their honesty, but also their caution

Other Precautionary Measures

- Scan incoming programs for viruses
  - Some viruses are designed to hide
- Limit the targets viruses can reach
- Monitor updates to executables carefully
  - Requires a broad definition of "executable"

Containment

- Run suspect programs in an encapsulated environment
  - Limiting their forms of access to prevent virus spread
- Requires versatile security model and strong protection guarantees

Viruses and File Sizes

- Typically, a virus tries to hide
- So it doesn't disable the infected program
- Instead, extra code is added
- But if it's added naively, the size of the file grows
- Virus detectors look for this growth
- Won't work for files whose sizes typically change
- Clever viruses find ways around it
  - E.g., cavity viruses that fit themselves into "holes" in programs

Signature Scanning

- If a virus lives in code, it must leave some traces
- In early and unsophisticated viruses, these traces were essentially characteristic code patterns
- Find the virus by looking for the signature

How To Scan For Signatures

- Create a database of known virus signatures
- Read every file in the system and look for matches in its contents
- Also check every newly imported file
- Also scan boot sectors and other interesting places

Weaknesses of Scanning for Signatures

- What if the virus changes its signature?
- What if the virus takes active measures to prevent you from finding the signature?
- You can only scan for known virus signatures

Polymorphic Viruses

- A polymorphic virus produces varying but operational copies of itself
- Essentially avoiding having a signature
- Sometimes only a few possibilities
  - E.g., Whale virus has 32 forms
- But sometimes a lot
  - Storm worm had more than 54,000 formats as of 2006

Stealth Viruses

- A virus that tries actively to hide all signs of its presence
- Typically a resident virus
- For example, it traps calls to read infected files
  - And disinfects them before returning the bytes
  - E.g., the Brain virus

Combating Stealth Viruses

- Stealth viruses can hide what’s in the files
- But may be unable to hide that they’re in memory
- Also, if you reboot carefully from a clean source, the stealth virus can’t get a foothold

Multi-Level Generic Detection

- Virus detection software that is specialized to handle both known and new viruses
- Using a combination of methods
- Both continuously and on command

Generic Detection Tools

- Checksum comparison
- Intelligent checksum analysis
  - For files that might legitimately change
- Intrusion detection methods
  - E.g., look for attack invariants instead of signatures
- Identify and handle "clusters" of similar malware

Preventing Virus Infections

- Run a virus detection program
  - 98% of all CSI reporting companies do
  - And many still get clobbered
- Keep its signature database up to date
  - Modern virus scanners do this by default
- Disable program features that run executables without users asking
  - Quicktime had this problem last year
- Make sure users are very careful about what they run

How To Deal With Virus Infections

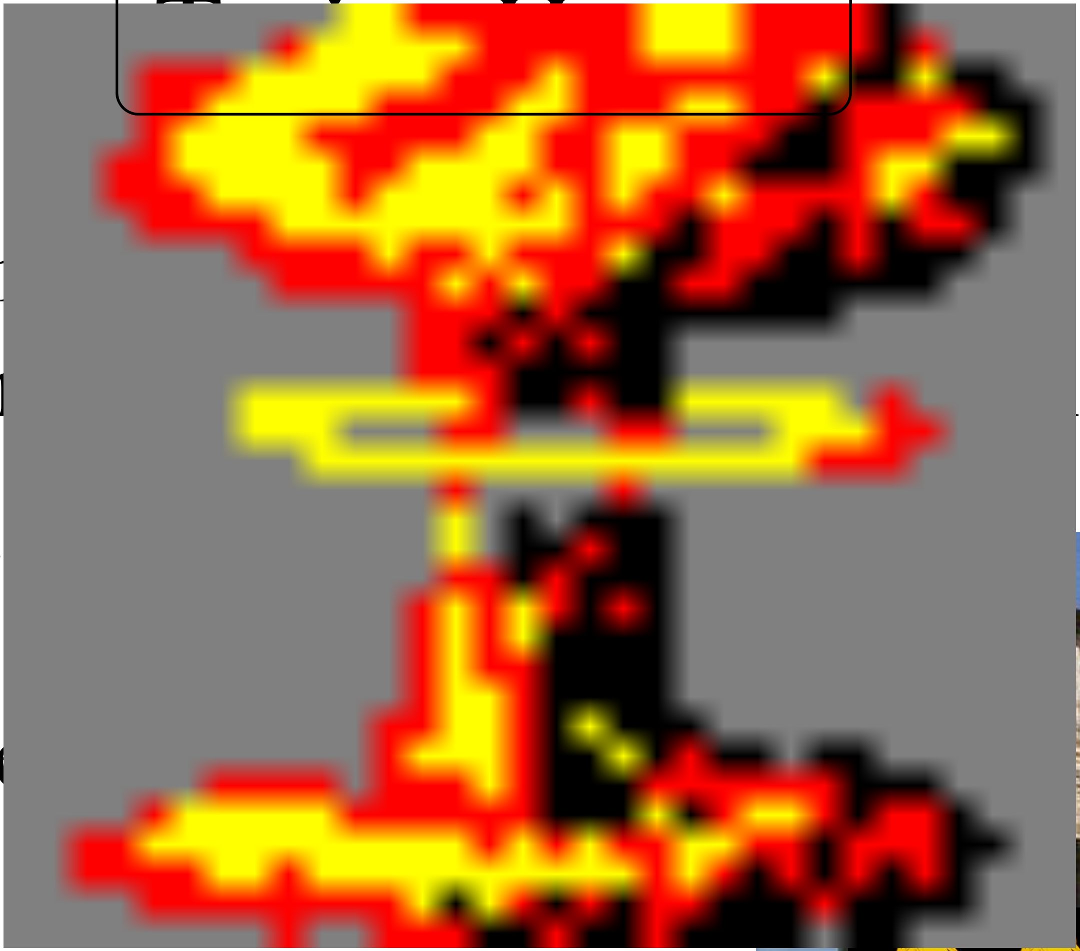
- Reboot from a clean, write-protected floppy or from a clean CD ROM
  - Important to ensure that the medium really is clean
  - Necessary, but not sufficient
- If backups are available and clean, replace infected files with clean backup copies
  - Another good reason to keep backups
- Recent proof-of-concept code showed infection of firmware in peripherals . . .

Disinfecting Programs

- Some virus utilities try to disinfect infected programs
  - Allowing you to avoid going to backup
- Potentially hazardous, since they may get it wrong
  - Some viruses destroy information needed to restore programs properly

- Seemi
  contai ings

- When
  Greeks
  slaught



Basic Trojan Horses

- A program you pick up somewhere that is supposed to do something useful
- And perhaps it does
  - But it also does something less benign
- Games are common locations for Trojan Horses
- Downloaded applets are also popular locations
- Frequently found in email attachments

Trojan Horse Login Programs

- Probably the original Trojan horse
- Spoof the login or authentication screen of a machine or service
- Capture attempts to access that service
- Then read the user IDs and the passwords

Trapdoors

- A secret entry point into an otherwise legitimate program
- Typically inserted by the writer of the program
- Most often found in login programs or programs that use the network
- But also found in system utilities

Trapdoors and Other Malware

- Malware that has taken over a machine often inserts a trapdoor
- To allow the attacker to get back in
  - If the normal entry point is closed
- Infected machine should be handled carefully to remove such trapdoors
  - Otherwise, attacker comes right back

Logic Bombs

- Like trapdoors, typically in a legitimate program
- A piece of code that, under certain conditions, “explodes”
- Also like trapdoors, typically inserted by program authors
- Often used by disgruntled employees to get revenge
  - In 2002, Paine Webber employee caused $3 million in damage to the company this way
  - In January, programmer pled guilty to planting a logic bomb in Minnesota hospital

Extortionware

- A little similar to logic bombs
- Attacker breaks in and does something to system
  - Demands money to undo it
- Encrypting vital data is common variant
- Unlike logic bombs, not timed or triggered