Malware
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Outline

- Introduction
- Viruses
- Trojan horses
- Trap doors
- Logic bombs
- Worms
- Botnets
- Spyware
- Malware components

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

Magnitude of the 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
- 2008 CSI report shows 50% of survey respondents had virus incidents
  - Plus 20% with bot incidents
- 2009 Trend Micro study shows 50% of infected machines still infected 300 days later

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 write new code into existing programs
  - Adding malware to an otherwise benign and useful program

Where Is The Code Put?

- Originally, at the end of the existing file
  - With new instructions to jump to the malicious instructions
- Now more cleverly hidden in the binary
  - Often fit into “holes” in the original binary
  - Unused variables
  - Empty regions created by compilers
  - Or other similar places

Macro and Attachment Viruses

- Modern data files often contain executables
  - Macros
  - Email attachments
- Many formats allow embedded commands to download of arbitrary executables
- Popular form of viruses
  - Requires less sophistication to get right

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 toolkits are getting smarter

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
  - No use to run in tightly confined mode if user allows it to get out

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
  - Replace instructions of the same size with your malicious instructions

Signature Scanning

- If a virus lives in code, it must leave some traces
- In unsophisticated viruses, these traces are 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
- Can use same approach for other kinds of malware

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 forms

Polymorphism By Hand

- Malware writers have become professional and security-aware
- They know when their malware has been identified
  - And they know the signature used
  - Smart ones subscribe to all major anti-virus programs
- They change the malware to remove that signature and re-release it

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
- Careful reboot from clean source won't allow stealth virus to get a foothold
- Concerns that malware can hide in other places, like peripheral memory

Other Detection Methods

- 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
  - Almost all serious organizations do this
  - 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 a few years ago
- Make sure users are careful about what they run
- Also make sure users are careful about what they attach to computers

How To Deal With Virus Infections

- Reboot from a clean, write-protected medium
  - Vital 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
- 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