Anti-Virus Techniques

Cs4001/7001 Malware Analysis & Defense

Bill Harrison

Three Major Tasks of Anti-virus software

- Detection
  - Decide whether some code contains a virus or not
  - Precisely detecting viruses by their appearance or behavior is provably undecidable (essentially the halting problem)
- Identification
  - Which virus is it?
  - Helps determine damages and how to repair
- Disinfection
  - Repair
  - Remove
  - Quarantine

Virus Detection

- Static Scanners
  - On-demand: run explicitly when started by the user
  - On-access: runs continually, scanning every file when its accessed
- "Scanning" is the bread and butter of anti-virus software
  - Each virus is characterized by a "signature" or pattern
  - Sometimes called "scan strings"
  - Code that does the search is called a "scanner"
  - Technical challenges
    - Accuracy
    - Speed

Anti-virus Software Errors

- Anti-virus software is subject to errors in both detection and disinfection of viruses
- Detection Errors
  - False negatives
  - False positives
- Disinfection Errors
  - Failure to disinfect
  - Destructive disinfection

False Negatives

- A *false negative* in anti-virus detection is the failure to detect a virus on a system being scanned
- Consequences:
  - Virus continues to replicate and cause damage
  - User has false sense of security
  - User eventually realizes the virus is present and loses confidence in the AV software
  - User might try to run two AV programs at once, which can interfere with each other

False Positives

- A *false positive* in anti-virus detection is the false claim that a virus has been detected
- Consequences:
  - User might remove file and lose work
  - User might spend a lot of time restoring a file from backup (and lose some recent work in the process)
  - "Boy who cried wolf" syndrome: User might not believe the next positive reported by the AV program
  - A corporation could have the same false positive on hundreds of identical machines, greatly multiplying the costs of the false positive

False Positives: Example

- A recent anti-virus scan of a home computer produced the following report:

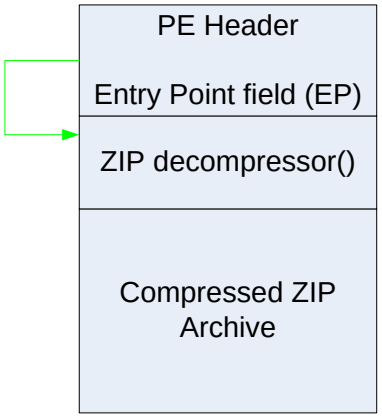
```
Freedom® Anti-Virus
Scanning Report (10/4/2005 11:21:57 PM)
Master Boot Records and Fixed Disk Boot Sectors
Scanned 1 Master Boot Record(s) for viruses.
Scanned 1 Boot Sector(s) for viruses.
Your Master Boot Record(s)/Boot Sector(s) are not infected.
Files
Drive C:\
C:\Documents and Settings\Clark Coleman\Application
   Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\javainstaller.jar-
   3cc46f89-666bee95.zip

   File is infected with a virus which is a destructive program.
Files scanned: 125177
   Infected files: 1
   Disinfected files: 0
   Deleted files: 0
   Files unable to scan: 0
```

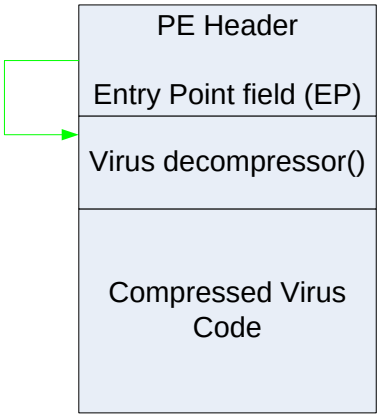
False Positives: Example

- Is this file really infected? Consider:
  - File is a ZIP archive which was downloaded from Sun and unpacked
  - The unpacked files are still on the system
  - The system has never had a virus detected
  - If the ZIP archive were truly infected, and then unpacked, would the archive itself be the only infection detected on the system?
- Recall that self-extracting archives resemble compressed viruses

False Positives: Archives and Compressed Viruses

- Self-extracting archives and compressed viruses have a nearly identical appearance:
- Both have almost no code except the decompressor, which uses the compressed code as its input data





False Positives: Summary

- The isolation of the "infection" to a ZIP archive, the failure of unpacking the archive to spread the infection, and the known resemblance of ZIP archives to compressed viruses lead us to conclude that this is a false positive
- This example happened on the home computer of a computer scientist familiar with viruses and AV software. What if it had been reported on the PC of a computer novice?
- Another potential source of false positives: installing Metasploit

Failure to Disinfect

- Aggressive anti-anti-virus techniques make it more likely that an AV scanner will fail to disinfect, e.g.:
  - Multi-partite viruses that infect the MBR and executables, which are then ready to re-infect after partial disinfection
  - Viruses that hook an interrupt chain and are resident in memory, waiting to re-hook the chain after the AV monitor disinfects the chain
- Detection followed by failed disinfection gives a false sense of security
- Infected system can cause damage for months as a result

Destructive Disinfection

- If an AV program does not make an aggressive effort to disinfect files, it will call on the user to restore from backup too frequently, which has high costs
- If an AV program has a false understanding of which virus variant it has detected, and tries to disinfect, it can leave behind a damaged file

Summary

- No error by an AV program is truly acceptable
  - The AV program cannot always err in the direction of too many false negatives OR too many false positives
  - The AV program cannot always err in the direction of asking for too many restores from backup OR in trying to disinfect files that it should have asked to be restored
- AV programs are too large and complex to be provably correct
- **Constant engineering refinement is the only solution at present**