Virus Analysis

Techniques, Tools, and Research Issues

Part I: Introduction

Michael Venable
Arun Lakhotia

University of Louisiana at Lafayette, USA

Introduction to Malware

Common Forms of Malware

Detection Techniques

Anti-Detection Techniques

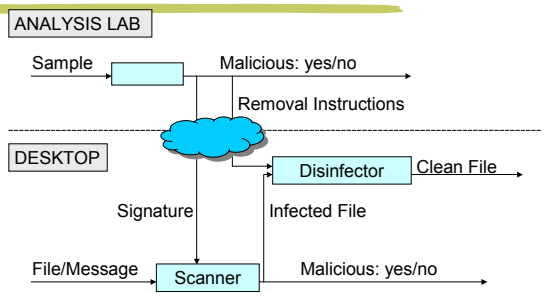
Common Forms of Malware

- Virus
  - Needs a vector for propagation
- Worm
  - No vector needed
  - Can spread by: network shares, email, security holes
- Trojan horse
  - Performs unstated and undesirable function
- Spyware, adware, logic bomb, backdoors, rootkits

Detection Technologies

- Integrity Checking
- Static Anti-Virus (AV) Scanners
  - Signature-based
    - Strings
    - Regular expressions
  - Static behavior analyzer
- Dynamic AV Scanners
  - Behavior Monitors

AV Detection Process



Integrity Checking

- Compute cryptographic checksums of files
- Periodically compare checksum with current checksum
- If mismatch, file has been modified

AV Scanners: Static Analysis

- Static Analysis
  - Analyze behavior of program without execution
  - Detects Properties true for all executions of a program
- Examples
  - Approximation of values
  - Analyze patterns of system calls

AV Scanners: Signature-based

- Extract byte sequences from malware
- Search for byte sequence within files
- If found, file is infected
- Byte sequences may contain wildcards

Signature-Based Scanning

- Hex strings from virus variants
  - 67 33 74 20 73 38 6D 35 20 76 37 61
  - 67 36 74 20 73 32 6D 37 20 76 38 61
  - 67 39 74 20 73 37 6D 33 20 76 36 61
- Hex string for detecting virus
  - 67 ?? 74 20 73 ?? 6D ?? 20 76 ?? 61
  - ?? = wildcard

AV Scanners: Dynamic Analysis

- Monitor a running program to detect malicious behavior
- Examples
  - Intercepting system calls
  - Analyzing audit trails
  - Looking at patterns of system calls
- Allows examination of only selected testcases

Anti-Detection Techniques

- Attacking Integrity Checkers
- Attacking Signature-Based Scanners
  - Polymorphism
  - Metamorphism
- Attacking Static Behavior Analyzer
  - Obfuscating Calls
- Attacking Behavior Monitors
  - Non-Deterministic behavior
  - Change behavior when being monitored

Attacking Integrity Checkers

- Intercept open() system call
  - Open a non-infected backup of the file instead
- Restore system to original state after attack
- Infect system before checksums are computed

Attacking Signature Scanners: Polymorphism

- Virus body is encrypted
- Decryptor is propagated with virus
- Use different encryption keys
- Morph decryptor code
  - Swap registers
  - Insert garbage instructions
  - Replace instruction with equivalents
  - Reorder subroutines

Polymorphism

- Detecting polymorphic viruses
  - Run suspect program in an emulator
  - Wait until it decrypts
  - Decrypted code will be identical for various copies
  - Use signature scanning on decrypted virus body
- Challenges
  - Determining when decryption is complete
  - Decryptor can determine whether its running in an emulator

Polymorphic Virus

- W32.Bugbear.B
  - Released in June 2003
  - Encrypted body with polymorphic decryptor
  - Spreads via email & shared network drives
  - Disarms popular anti-virus and firewall applications
  - Installs key-logger
  - Installs backdoor for remote access

Attacking Signature Scanners: Metamorphism

- Does not have a decryptor
- Morph code of the entire virus body
- No constant body
  - signature scanning will not work

Metamorphism

- Detecting metamorphic viruses
  - Run suspect program in an emulator
    - Analyze behavior while running
  - Look for changes in file structure
    - Some viruses modify files in a consistent way
  - Disassemble and look for virus-like instructions

Metamorphic Virus

- Win32.Evol
  - The Win32.Evol virus appeared in early July, 2000
  - Polymorphic operations:
    - Swaps instructions with equivalents
    - Inserts junk code between essential instructions

Metamorphic Virus [Szor, 2001]

- An early generation

```
c7060F000055    mov dword ptr [esi], 550000Fh
c746048BBC5151 mov dword ptr [esi+0004],
5151BCBBh
```

- A later generation

```
BF0F000055      mov edi, 550000Fh
893E            mov [esi], edi
5F          pop edi
52          push edx
B640            mov dh, 40
BA8BEC5151      mov edx, 5151EC8Bh
53          push ebx
8BDA            mov ebx, ebx
895E04          mov [esi+0004], ebx
```

Attacking Behavior Monitors

- Bypass higher-level system calls
  - AKA tunneling
- Act benign if running in emulator

Summary

- Types of malware
  - Virus, worms, Trojans, adware, spyware, etc.
- AV Technologies
  - Integrity checkers
  - AV Scanners – Static Dynamic
- AV Process
  - Analyze and extract signatures in lab
  - Distribute signatures to desktops
  - Analyze files/messages on desktops
- All AV technologies can be attacked