Malware Propagation

CMSC 426 - Computer Security

Overview

- Types of malware
- Insider attacks
- Viruses
- Trojans
- Worms

Malware is...

...*malicious software*; software that has negative or unintended consequences for the targeted user.

- Backdoors and Logic Bombs
- Viruses, Trojan Horses, Worms
- Rootkits and Remote Administration Tools
- Botnets
- Adware and Spyware

Backdoors

- Method to obtain privileged access that bypasses usual authentication measures
- A type of Insider Attack; typically installed by a developer
- Malicious or benign
- Remember the Ken Thompson attack!
- Example:
  - Borland Interbase - January 2001

Logic Bombs

- Code created to take destructive action given a specific *trigger*
- Another insider attack; e.g. disgruntled developer or administrator
- Trigger could be any event
- Examples:
  - Fannie Mae logic bomb - October 2008
  - Omega Engineering logic bomb - July 1996

Fannie Mae

- Rajendrasinh Babubhai Makwana, contractor supporting nearly 5,000 servers
- Fired on 24 October 2008; planted logic bomb later that day
- Designed to destroy *all* data on network
- Date trigger: 31 January 2009
- Discovered by an engineer on 29 October 2008.

Omega Engineering

- Tim Lloyd, network administrator for 11 years
- Disgruntled due to declining status in company; was fired before "attack."
- Deleted all files on an engineering LAN, and backups could not be found.
- Date trigger: 31 July 1996
- Forensics analysis recovered portions of the malicious script; erased backup tapes found at Lloyd's house.

Preventing Insider Attacks

- No single points of failure
- Formal code reviews
- Source control / SW engineering tools
- Principle of least privilege
- Monitor employee behavior
- Physical security

Viruses

A *computer virus* is a type of malware that

- *Replicates* by modifying other files or programs
- Requires *user assistance* to replicate
  - E.g. clicking a link or running a program

Contrast with a worm, which does not require user assistance.

Virus Lifecycle

- *Dormant phase*. Virus exists, but is not active.
- *Propagation phase*. Virus is replicating and infecting new files and systems.
- *Triggering phase*. A logical condition causes the virus to initiate some action.
- *Action phase*. The virus executes its intended action, called the *payload*.

Types of Viruses

- *File viruses*. Infect regular or executable files on the target system.
- *Macro viruses*. Infect macros attached to document files (e.g. Word).
- *Boot sector viruses*. Infect the system boot code.

Sality File Virus

- Infects windows executables (.exe, .scr)
- Many features beyond executing a malicious payload: botnets, spamming, distributed password cracking, rootkit, etc.
- Difficult to remove once infected.
- Active 2003 - Present.

Melissa Macro Viruses

- *Melissa virus* contained in World and Excel macros (Word 97, 2K; Excel 97, 2K, 2003).
- Mail propagation virus. Emails itself to first 50 people in address book.
- Many variants, some malicious: Excel file deletion, ransomware, etc.
- First appeared in 1999.

Boot Sector Viruses

- *Elk Cloner* virus for the Apple II (1982)
  - Basically harmless: displayed a poem every 50th boot.
- *Parity Boot* virus for IBM PC (1980s - 90s)
  - Infects floppy boot sector and hard drive *Master Boot Record* (MBR).
  - Locks machine, requiring hard reset.
  - Was common in Germany due to infection of a software disk included with a computer magazine.

Virus Signatures

- The use of *signatures* is one approach to virus detection and prevention.
- Search for strings (the *signatures*) known to occur in viruses or other malware through *pattern matching*.
- If strings are found, files are moved to a protected storage area called *quarantine*.
- Quarantined files can be cleaned, deleted, studied, forwarded to anti-virus provider, etc.

Encrypted Viruses

Virus writers work to defeat signature-based detection:

- Encrypt most of virus code. Encryption destroys patterns (signatures) in the code.
- Prepend unencrypted program *stub* that decrypts and loads remainder of the virus.

Stub may still have signatures; structure is a sort of signature as well.

Polymorphic Viruses

- A *polymorphic virus* is one that encrypts itself with a new key whenever it replicates.
- Unlikely that any two versions of the virus will be the same.
- Makes signature-based detection difficult, but program stub may still be detectable.
- Example: Sality

Metamorphic Viruses

- A *metamorphic virus* evades signature detection by automatically re-writing itself with logically equivalent code.
- Instruction re-ordering, useless instructions (e.g. NOP, jumps, equivalent instructions)
- No detectable stub; all code is re-written.
- Examples: Simile, ZMist.

Detecting Viruses

- More complex signatures
  - *Conjunction Signature*: set of strings that can appear in any order.
  - *Sequence Signature*: set of strings that must appear in a given order.
  - *Probabilistic Signature*: set of strings and scores; high score indicates possible virus.

Heuristics

- The use of general properties of viruses (*heuristics*) to identify suspicious software:
  - Detect useless code
  - Disassemble executable and look for functionality resembling a virus
  - Look for small executable stub with large "random" looking data
  - Execute code in virtual environment and monitor for suspicious activity

Trojan Horse

A *trojan horse* is a type of malware that

- *Masquerades* as useful or desirable software, enticing users to install and run it
- Includes malicious functionality
  - Password theft, data destruction, etc.

As with viruses, requires user assistance.

Android.Counterclank

- Symantec identified 13 Android apps that included the Android.Counterclank Trojan
- Copies information such as bookmarks, notifications, build information, browsing history, etc.
- Up to 5 *Million* downloads as of 27 January 2012
- Is it malware or "an aggressive form of ad network?"

SMSSend.3666 Trojan

- First fake installer trojan to target Macs
- Masquerades as "VKMusic 4 Mac", a Russian music player
- User enters phone number to register and receives SMS response
  - If responds to SMS, recurring charges made to their mobile account
- December 2012

Trojan.Stabuniq

- Trojan targeting US financial institutions
- Spread through spam emails; found on workstations, mail servers, firewalls, proxy servers, and gateways
- Steals system information and forwards it to one of several remote servers
- Thought to be a proof-of-concept or purely for reconnaissance
- Discovered in December 2012

Mocmex

- Trojan contained in digital picture frames manufactured in China
- Designed to steal personal or financial data; deployed version only stole passwords for online games
- Able to spread to other portable storage devices
- Discovered in February 2008

Worms

A *computer worm* is a type of malware that

- Spreads without injecting code into other applications
- Typically spreads without human assistance
  - Exploits vulnerabilities such as buffer overflows

Since worms do not modify other programs, they are not a type of virus

Morris Worm

- One of the first Internet worms - 1988
- Developed by Robert Morris at Cornell
- Spread using multiple vulnerabilities
  - buffer overflow in *fingerd* daemon
  - vulnerability in SMTP debug mode
  - password guessing
- No malicious payload, but high re-infection rate led to effective denial-of-service

Conficker

- Massive worm - estimated 9 to 15 *million* infections in January 2009
- Infected UK MoD, German Bundeswehr, French Navy, ...
- Spread using multiple vulnerabilities
  - Microsoft SMB vulnerability
  - Attack on ADMIN$ shares; password guessing if necessary
  - Infection of USB memory sticks
- Capable of downloading and running various payloads
- Thought to originate from the Ukraine

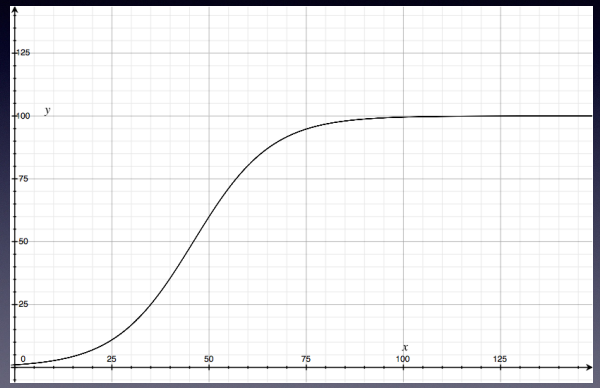
Propagation Model

- Simplified epidemiological model

$$\frac{dI(t)}{dt} = \beta I(t)S(t)$$

  - I(t) is number of infected individuals
  - S(t) is number of susceptible individuals
  - β is the infection rate
  - N = I(t) + S(t) is the population size

Propagation Curve



Detecting Worms

- A worm may modify various files in the system, making it detectable through signatures (as with viruses)
- Unusual network traffic or protocols may also be detectable (Conficker)
- In some cases, worms may cause degraded system performance (Morris Worm)

References

- Fannie Mae Logic Bomb

  http://www.fbi.gov/baltimore/press-releases/2010/ba100410a.htm

  http://www.informationweek.com/security/management/fannie-mae-contractor-indicted-for-logic/212903521
- Omega Engineering Logic Bomb

  http://articles.cnn.com/2000-06-27/tech/omega.files.idg_1_server-manufacturing-capabilities-manufacturing-programs?_s=PM:TECH
- Sality Virus

  http://en.wikipedia.org/wiki/Sality

References (cont.)

- Android.Counterclank

  http://arstechnica.com/gadgets/2012/01/android-trojans-downloaded-by-millions-still-on-android-market/

- SMSSend.3666

  http://arstechnica.com/security/2012/12/new-mac-trojan-tricks-users-into-paying-pricey-cell-phone-fees

- Trojan.Stabuniq

  http://arstechnica.com/security/2012/12/symantec-finds-a-new-trojan-that-steals-data-from-us-banks-customers/

References (cont.)

- Mocmex

  http://www.seattlepi.com/business/article/Chinese-PC-virus-may-have-hidden-agenda-1264738.php

- Morris Worm

  http://spaf.cerias.purdue.edu/tech-reps/823.pdf

- Conficker

  http://mtc.sri.com/Conficker/

  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed1.pdf