Lecture 6: Malicious Software I

Summary

In this lecture, we introduce malicious software categorized by propagation method. Later we will discuss malicious software payloads and look at viruses and worms in more detail.

Classification of Malicious Software - Propagation

References

P&P, Sections 3.3 and 3.4

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

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

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

Tim Lloyd, Omega Engineering, http://www.nytimes.com/1998/02/18/nyregion/man-charged-with-sabotage-of-computers.html

Viruses

Replicate by modifying other files or programs.

Require *user assistance* to replicate.

Trojan Horse

Masquerades as useful or desirable software, enticing users to install

Includes malicious functionality

Worms

Spread *without* injecting code into other applications

Typically spread *without user assistance*

Trapdoors (or Backdoors)

Method to obtain access that bypasses usual authentication measures

A type of *Insider Attack*; may be malicious or benign

Logic Bombs

Code created to take destructive action given a specific *trigger*

Another form of *Insider Attack*

Examples

- *Sality Virus, 2003 - Present*. Infects Windows executables (.scr and .exe); may infect files that are then transferred on removable media. Can carry many different malicious payloads: botnets, rootkits, password cracking, etc.
- *Trojan.Stabuniq, discovered December 2012*. Targeted US financial institutions; spread through spam emails; found on workstations, mail servers, firewalls, proxy servers, and gateways. Steals system information and forward to remote servers. Possibly a proof-of-concept.
- *Conficker Worm, discovered November 2008*. Massive infection — estimated 9 to 15 million infections in January 2009; infected UK MoD, German Bundeswehr, French Navy, and others. Spread using multiple vulnerabilities: Microsoft SMB vulnerability, attack on ADMIN$ shares, infection of USB memory sticks. Capable of downloading and running various payloads.

- *Omega Engineering Logic Bomb, 1996*. Tim Lloyd, network admin for 11 years; disgruntled due to declining status in company; fired. Logic bomb planted with trigger date of 31 July 1996; deleted all files on engineering LAN. Forensics analysis revealed portions of malicious script; erased backup tapes found at Lloyd's house.

Exercises

P&P, Chapter 3, Exercise 2, 3, and 4.