Introduction to Intelligent Security Systems

Alvin Lin

August 2018 - December 2018

Malware

Malware, also known as malicious code or malicous software, refers to a program that is inserted into a system (usually covertly) with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware has become the most significant external threat to most systems, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.

Viruses

Viruses are programs embedded in files that spread and do damage. They are typically comprised of a replicator which reproduces the virus, and a payload which performs the malicious task.

- Boot Sector Virus: infects the boot or master boot record of diskettes and hard drives through the sharing of infected disks and pirated software applications.
- Program Virus: becomes active when the program file carrying the virus is opened. It then makes copies of itself and infects other programs on the computer.
- Multipartite Virus: hybrid of a boot sector and program virus that infects program files and affects the boot record when activated.
- Stealth Virus: disguises itself to prevent detection by antivirus software. It alters its file size or conceals itself in memory.

- Polymorphic Virus: acts like a chameleon by changing its virus signature every time it multiplies and infects a new file.
- Macro Virus: programmed as a macro embedded in a document, usually found in Microsoft Word or Excel. Once a computer is infected, every document produced from the computer will become infected.

Malware Categories

	Virus	Worm	Trojan Horse
Self-contained?	no	yes	yes
Self-replicating?	yes	yes	no
Propagation method	User interaction	Self propagation	n/a

All forms introduce some undesired functionality into the infected host. Viruses are generally hidden in code while trojans may be hidden in code but are usually not. Generally worms and viruses self-propagate, but worms run independently to consume the resources of its host while viruses cannot run independently and require a host program to activate it.

Boot sector viruses infect the boot sector of hard drives, thus guaranteeing they get executed and loaded into memory whenever the computer is turned on. They have declined today due to the fact that operating systems now protect the boot sector.

Basic Timeline

- 1949: Theories for self-replicating programs are first developed.
- 1981: Apple Viruses 1, 2, and 3 are some of the first viruses found in the public domain. They were found on the Apple II operating systems and propagated through Texas A&M via pirated computer games.
- 1983: Fred Cohen, while working on his dissertation, formally defines a computer virus as "a computer program that can affect other computer programs by modifying them in such a way as ot include a possible evolved copy of itself".
- 1986: Two programmers named Basit and Amjad replace the executable code in the boot sector of a floppy disk with their own code designed to infect each 360kb floppy disk accessed on any drive.

- 1987: The Lehigh virus, one of the fist file viruses, infects command.com files.
- 1988: One of the most common viruses, Jerusalem, is unleashed. Activated every Friday the 13th, the virus affects both .exe and .com files and deletes any program run on that day.
- 1998: The first version of the CIH viruses developed by Chen Ing Hau from Taiwan are released.
- 2000: The virus ILOVEYOU is released, capable of deleting files in JPEGs, MP2, or MP3 formats.
- 2001: The Anna Kournikova is spread by emails through compromised address books of Microsoft Outlook. The emails were purported to contain pictures of the very attractive female tennis player, but in fact hid a malicious virus.
- 2006: OSX/Leap-A is the first ever known malware discovered against MAC OSX.
- 2013: Cryptolocker, a trojan horse that encrypts files and demands a ransom, is released.
- 2014: Backoff, a malware designed to compromise point-of-sale systems to steal credit card data, is released.
- 2017: The WannaCry randomware infects more than 230,000 computers in over 150 countries.

ILOVEYOU virus

In 2000, the ILOVEYOU virus infected millions of computers virtually overnight through email. It spread through email attachments and deleted all jpeg files in all disks. The virus also sent passwords and usernames back to the author. Authorities traced the virus back to a young Filipino computer student who went free because the Phillippines at that itme had no laws against hacking. This spurred the creation of the European Union's global Cybercrime Treaty.

Stuxnet

Stuxnet is a highly sophisticated computer worm discovered in June 2010. It initially spread via Microsoft Windows and targeted Siemens industrial software and

equipment. While it was not the first time hackers had target industrial systems, it was the first discovered malware that spied on and subverted industrial systems, and the first to include a programmable logic controller rootkit.

Stuxnet has been spotted in Iran, Israel, the Palestinian territories, Syria, and Lebanon. It is one of the most sophisticated viruses developed, able to activate computer microphones, log keystrokes, and steal data. Given its size, some have posited that the virus could only have been developed by the United States or Israel.

Petya.A Ransomware

Petya.A used a handful of different tools to move through a network and infect the computers. It used a modified EternalBlue exploit and scrambled a user's data using AES-128. The hackers demanded $300 for the decryption key.

Vulnerabilities

Vulnerabilities are not viruses, but could allow attackers to compromise the integrity, availability, or confidentiality of a product. One example is the Heartbleed OpenSSL vulnerability, which allowed attackers to leak data from the memory heap of any computer accepting an OpenSSL request. The heap may contain anything from random data to unencrypted data processed by OpenSSL, which may include unencrypted web certificates or plain text usernames and passwords.

Malware Detection

Modern malware can morph to avoid detection by signature based antivirus solutions. That means that today's antivirus solutions remain necessary for catching known virus threats, but they're no longer sufficient because there is no know pattern for detecting advanced attack. Strategies:

- There is a clear distinction between data and executable. Since a virus must write to the program, only allow it to write to data so it cannot execute.
- Sandbox the virus so it runs in a protected area. Libraries and system calls are replaced with limited privilege versions.
- Malicious code usurps the authority of the user, so limiting the information flow limits the spread of the virus.
- Programs run with the minimal needed privilege.

- Use multi-level security mechanisms by putting programs at the lowest level and disallowing users from operating at that level.
- Look for a pattern in malicious code, which is always a cat and mouse game with the attacker.
- Maintain a checksum of the good file and check to see if it changed.
- Validate the action of an executable against some specification, including intermediate results and actions.
- Have the code carry some proof of correctness and verify the proof against the code during execution.
- Use statistical methods such as the number of files written, volume of data transferred, and the usage of CPU time.
- Scan the hard disk, memory, and boot for known virus signatures.

Actions to Prevent Virus Infection

- Always update your antivirus software at least weekly.
- Back up your important files and ensure that they can always be restored.
- Change the computer's boot sequence to always start the PC from its hard drive.
- Don't share drives without a password and without read-only restrictions.
- Empty removable drives or other media before turning on computers, especially laptops.
- Forget opening unexpected email attachments, even if they are from friends.
- Get trained on your computer's antivirus software and use it.
- Have multiple backups of important files. This lowers the chance that all are infected.
- Install security updates for your operating system and programs as soon as possible.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech