Malware vs. Anti-Virus Software

CISC 3325 — CUNY Brooklyn College
Lecture Notes

Malware vs. Anti-Virus Software

In this chapter, we will:

1. Define 'malware', understand what affects it can have, and learn how it reaches a device in the first place.
2. Review the definition, propagation manner, and examples of 10+ malware types, e.g., viruses, worms, trojans, bots, etc.
3. Introduce three different types of anti-virus software, and explain how they work to detect malware on a device.

Malware

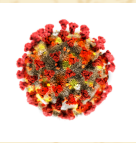
Malware (= **mal**icious soft**ware**) is a program or a piece of software whose purpose is to cause unanticipated or undesired effects, mostly causing harm or damage to computer systems, data, or people.

Several kinds of malware exist, each of which has its own harm-inflicting goals, including:

- Obtaining sensitive information (e.g., spyware)
- Deleting or modifying files (e.g., virus, worm, etc.)
- Harming availability of resources (e.g., rabbits)
- Spreading ads and spam (e.g., spamware)
- Financial exploitation (e.g., ransomware)
- Other malicious purposes (e.g., cyberbullying, harassment, political activism)

Common ways in which malware is downloaded to a device are via clicking links in suspicious email or text messages, downloading software from untrusted resources, or just visiting malicious webpages *without* clicking any links on them.

Virus



Taken from Hartford Healthcare

Malware exists in several types, each of which has its own propagation methods and targets:

1. **Definition**: A **virus** is a malicious software that attaches itself to executable files. Viruses replicate (= create copies of themselves) and thereby spread among the files of a device and possibly over the network to which the device is connected.

   This is the most known type of malware and is sometimes used, in layman terms, as a synonym for malware.
   For instance, we tend to say 'anti-virus' and not 'anti-malware'.

   Reason for the name: Due to the similarity to a biological virus that attaches itself to a living thing's cells and starts replicating.
   Propagation: Infects and modifies a computer system's files when an executable carrying the virus runs (in many cases, with the help of an unawared user who executes the program.)
   Examples of well-known viruses: Michelangelo, Brain, Klez, SQL Slammer, and Blaster.

Virus

1. A virus can be in one of several life phases:
    1. **Dormant phase**: The virus just exists as a file on the disk and avoids detection.
    2. **Propagation phase**: The virus is replicating itself, infecting new files.
    3. **Triggering phase**: Some logical condition causes the virus to move from a dormant or propagation phase to perform its intended action.
    4. **Action phase**: The virus performs the malicious action that it was designed to perform, called the **payload**, which is anything from sending spam to destroying files, launching denial-of-service attacks, and spying after users. It could also be just another type of malware, e.g., a trojan or spyware.

   Viruses attempt to conceal their action (to prevent anti-virus software from detecting it) in a few ways, including:
    - Encryption: Such a virus encrypts itself and uses a different key each time it infects a new file.
    - Stealth: Escapes anti-virus software by intercepting the software calls to the OS and pointing it to the actual virus.
    - Polymorphic / Metamorphic: Change their form (i.e., mutate) or re-write themselves before every new infection.
    - Sparse Infecting: Infect every *n*th file, or on rare occasions (e.g., Friday the 13th.)

Worm

Taken from WhatIsMyIP.com

2. **Definition**: A **worm** is another replicating malware carrying a payload. The difference between a virus and a worm is that a worm doesn't need to attach itself to an existing executable or file. Worms can multiply themselves and can propagate out of the networks, infecting other networks and other systems, thus creating huge havoc or damages.

   Since a worm doesn't depend on a carrier, it doesn't need to have a user activate it: it activates without human interaction.

   Reason for the name: Similarly to viruses, worms are parasitic creatures that infect an organism without attaching themselves to cells.
   Propagation: The same way as viruses, by launching the payload software that it carries. The difference is that there is no human intervention. Worms propagate by finding and infecting vulnerable hosts.
   Examples of well-known worms: Melissa, Morris, ILOVEYOU, and W32.Stuxnet.

Trojan

Taken from Twinkl USA

3. **Definition**: A **Trojan** is a seemingly harmless program that appears to perform a useful task (e.g., a game) but, in the background, performs something with negative consequences, such as spying after a user.

   The program is either actively installed by a computer's user or administrator, not knowing that the program does a malicious activity, or is installed as a payload of a virus or a worm.

   Reason for the name: It is based on the story of the wooden Trojan Horse that was sent by the Greeks into the city of Troy during the Trojan War. The gigantic horse, which was presented to Troy as a gift, was the hiding place of Greek warriors who launched an attack on Troy.
   Propagation: When a user runs the program, it performs the task that the user intends to do in the foreground while also performing a disguised, malicious task in the background, without the user's awareness.
   Examples of well-known Trojans: Flame, Zero Access, Banker, Zeus, and Beast.

Rootkit

Taken from Digital Defense

4. **Definition**: A **rootkit** malicious software installed without the user's awareness with the following intentions:
   - Hide the rootkit's own activities and their presence from the OS.
   - Hide the activities performed by other malicious utilities / software installed on the compromised system.
   - Gather data of interest to the attacker and provide this data to the attackers silently.
   - Act as a repository of malicious programs serving other systems like zombies or bots.

   Rootkits contain various malicious utilities like network sniffers, and the tools which wipe off the logs. These replace some of the OS functions and calls with their own malicious versions, thus compromising the security of the targeted system. Once they are installed, they provide complete access to the attacker on the compromised system. Rootkits are not easy to detect as they are primarily meant to be working in stealth mode, hiding themselves and their activities.

   Reason for the name: Since they work from inside the root of an OS.
   Propagation: Once installed, the rootkit will start working in the background without the OS being able to detect it.
   Examples of well-known rootkits: Windows NT/2000 Rootkit, Fu, and KBeast.

Spyware

Taken from Vigilant

5. **Definition**: **Spyware**, as the name suggests, is malicious software whose intention is to spy on an operating system, user, organization, or government. They track or monitor the activities of others. There are even official spyware which are used by Governments and national agencies. These work secretly or in stealth mode.

   Spyware may be installed as a payload of another malware, e.g., a virus.

   Reason for the name: Abbreviation of "**spy**ing mal**ware**".
   Propagation: Once installed, spyware will begin collecting confidential data about the user or OS for the attackers' specific needs and send this data out to the attackers.
   Examples of well-known spyware types: Tracking Cookies, which track what you did on the web pages, and Keyloggers (e.g., ComputerSpy), which can log everything you've typed including user IDs and passwords. Recall that we already spoke about keyloggers in Topic 3: Access Control.

Malware vs. Anti-Virus Software

Any questions?

Adware

Taken from Savvy Security

6. **Definition**: **Adware** is usually a software element (a program) whose purpose is to generate revenue for the owner of an application, service, or website. These ads may be in the form of popups, streaming messages, whole areas of a web page, through a bar on the screen, or installed and played when a user downloads software.

   What's malicious about adware is that the underlying code within these ads may track a user's personal behavior (e.g., which ads are clicked the most) and pass on the information to 3rd parties for commercial purposes, which, without the user's awareness and explicit consent, is illegal in certain states and countries.

   Reason for the name: Abbreviation of "**ad**vertisement mal**ware**".
   Propagation: Adware might illegally collect data or perform other unaware of or undesired actions when a user interacts with the ad (hovers over it, clicks it, plays it, etc.)
   Examples of well-known adware types: Zango and Fireball.

Backdoor

Taken from Malware Fox

7. **Definition**: A **Backdoor** (also called a **trapdoor**) is a malicious software which is installed on a system or application with the intention of the attacker to access the system at a later date via a hidden feature or command in the software.

   A backdoor may be installed through a Trojan. These are usually in stealth mode and get activated by the attackers based on their intentions.

   Reason for the name: Just as not everyone is aware of entrances into a house besides the front door, such as a backdoor, most people are also not aware of the hidden feature in the software.
   Propagation: When used in a normal way, the software performs completely as expected and advertised (e.g., a game). However, if the hidden feature is activated by the attacker (possibly remotely,) the software does something unexpected, such as getting admin privileges in the OS.
   Examples of well-known backdoors: the SolarWinds hack and the WordPress hack.

Bots and Zombies

Taken from Hacker News

8. **Definition**: A **zombie** (sometimes also a **bot**) is a computer that is controlled remotely, either partially or fully, by an attacker. An attacker would have a network of zombies or a zombie army (sometimes across the world) that are already compromised / infected by attackers and are used for attacking other systems.

   Bots are used to initiate attacks, like denial of service, on other systems. These attacks are carried out by pooling the infected systems so that the impact can match the scale required (that is, to use as many bots as needed to crash the system.) A network of bots is called a **botnet**, and the attacker is the **controller** or **herder** of the bots.

   Reason for the name: Bot is a shorthand for 'robot', and zombie is due to the army-like nature of malicious robots.
   Propagation: A device first gets infected. Then, when the attacker decides so, he or she sends a remote command to the bot to make it start doing its malicious action.
   Examples of well-known botnets: the Mirai botnet and the Miner botnet.

Ransomware

Taken from GlobalSign

9. **Definition**: We all watched movies in which criminals kidnap people and demand ransom (usually, in the form of a large sum of money) to release them. The same nowadays also happens with devices and data: Software that breaks into a device, encrypts its files, and publishes a ransom request notification to have the data decrypted (= released back to the user) is called **ransomware**.

   The fear is that, as in real life, there is no guarantee that the attacker actually releases the data. Also, the attacker might sell the data or post it online, regardless of the received ransom. For these reasons, the U.S. government, and specifically the FBI, advises NOT to pay any ransom.

   Reason for the name: Abbreviation of **ransom** mal**ware**.
   Propagation: Ransomware first gets access to a device (possibly, with the help of other malware,) encrypts the files on the device, and then posts a ransom request to the user.
   Examples of well-known ransomware: WannaCry and Locky.

Rabbit

Taken from Cartoon Stock

10. **Definition**: A **rabbit** (also called a **`fork()` bomb**) is malware whose purpose is to harm the availability of computer (OS) resources, such as memory, disk space, CPU time, and I/O devices (= a **denial of service (DoS)** attack.) It replicates (just like a virus or worm) without limits, but doesn't carry any payload: its only purpose is to use an OS resource to the greatest extent possible to make it crash. A small example of a memory-exhausting rabbit in the C language:

```
int main() {
   while(1)
      fork();
   return 0;
}
```

Reason for the name: Since rabbits are animals that naturally multiply very fast. *Fun fact*: the Fibonacci sequence, which we all know grows very fast, was an early attempt to model the growth of the population of rabbits!
Propagation: Once installed and triggered, the rabbit will start indefinitely creating copies of itself to clot up the OS.
Examples of a rabbit: an attack against Iran's state broadcaster in 2022.

CIA and Malware

Malware might harm any of Confidentiality, Integrity, and Availability (CIA). Some malware types affect only one of these three, while others affect two or even all three.

Example: Ransomware might affect all three, while Spyware usually affects only one.

Fun class activity:

1. Explain how Ransomware might affect (i) Confidentiality (ii) Integrity (iii) Availability.
2. Which CIA principle is affected by Spyware? Why?
3. Which CIA principle is affected by a Rabbit? Why?

Malware

Following are several more malware types that we define shortly:

Malware Type	Definition
Logic Bomb	Malware triggered when a logical condition becomes true.
Time Bomb	Malware triggered at specific dates/times.
Zero-Day Bomb	Malware that quietly and secretly exists on a device.
Dropper	Malware that delivers ('drops') other malware.
Browser Hijacker	Malware taking control of the browser application.
Tool or **Toolkit**	Software that tests for the existence of vulnerabilities in a system.
Scareware or **Hoax**	False warning of malware to scare or to abuse a user financially.

Malware

Summary of our review of malware:

https://www.youtube.com/watch?v=GrdOpFFGxD0

Any questions?

Controls of Malware

Any user can apply the following countermeasures to prevent malware infection:

- Use software that is downloaded only from reliable sources.
- When creating software of your own, test software in an isolated environment (e.g., on a virtual machine.)
- Open messages/attachments only when you know/trust their sender.
- Treat every website as potentially harmful, and don't browse websites that you are harmful.
- Create and maintain backups of your data.
- Update software/applications whenever a new security update is available.
- Use the services of at least one anti-virus software on your device, and regularly update the anti-virus software.

Speaking about anti-virus software ... let's discuss it further!

Anti-Virus Software

The need for a tool to check for malware has increased in recent decades, because most of the general users of a computer system are unaware of the specific risks of transacting over the internet, even though they are generally aware that there are some risks.

Also, due to the dynamics of life, people might find themselves 'too busy' or insufficiently skilled to check the correctness and un-maliciousness of software themselves.

An **Anti-Virus Software** is an application that detects, notifies the user about, and uninstalls/deletes one or more of the malware types we introduced in the previous slides.

Every device that contains sensitive data should run at least one anti-virus software.

The more malware types an anti-virus software can detect, the better and more quality it is considered to be.

Anti-Virus Software

How does an anti-virus work?

An anti-virus searches for suspicious patterns of code in applications and files. It is equipped with a list of suspicious patterns that have been observed to be a part of malware. If one such pattern is found, the anti-virus will alert the user and allow them to either quarantine the suspicious file/application or delete it.

The reason that it is highly recommended to regularly update your anti-virus is that the updates contain more and more patterns that were found in recently detected malware. That means that updates increase your chances of being protected against the most recent malware outbreaks.

When the anti-virus performs a scan on your device, it searches for these patterns in the files on your device. An anti-virus works relatively fast because such questionable patterns are usually located at specific parts of a file/application, so the job of an anti-virus is reduced to searching only at these parts.

Anti-Virus Software

What types of anti-virus measures exist?

1. **Virus-specific detection methods** look for and identify specific viruses, which is how most anti-virus programs operate. The anti-virus program scans files in the disk (or only in certain directories), looking for bit strings that signal the presence of (that are the signature of) known viruses.
2. **Generic virus detection techniques** don't look for specific viruses but, instead, examine the computer for any suspicious, unusual, or anomalous behavior. An example of such activity is an attempt to modify the size of an executable file by a user program. A generic technique cannot identify specific viruses but can warn the user that something suspicious has taken place in a certain file or process.
3. **Virus preventive techniques** create an environment in the computer where viruses hesitate before they enter, or cannot execute once they have entered. Preventive techniques are mostly commonsense measures such as having up-to-date backups of data, running firewalls, being careful in Internet surfing, and generally being suspicious and not trusting.

Anti-Virus Software

Top 5 Best Free Anti-Virus Software for 2023:

https://www.youtube.com/watch?v=cQJfZmTvB4g

Anti-Virus Software

Any questions?

Malware vs. Anti-Virus Software: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 7: Malicious Software and Anti-Virus Software." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 141-161. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+7:+malicious+software+and+anti-virus+software

Salomon, David. "Chapter 6: Prevention and Defense." *Elements of computer security.* Springer Science & Business Media, 2010, pp. 151-177. URL: https://link-springer-com.brooklyn.ezproxy.cuny.edu/content/pdf/10.1007/978-0-85729-006-9.pdf#6+prevention+and+defense