Topic 5 - Malware

Eric Casanovas

Universitat d'Andorra

27th April, 2022

1. Introduction
2. Types of Malware
3. Infection
4. Propagation
5. Detection and Protection
6. Antivirus

1 Introduction

2 Types of Malware

3 Infection

4 Propagation

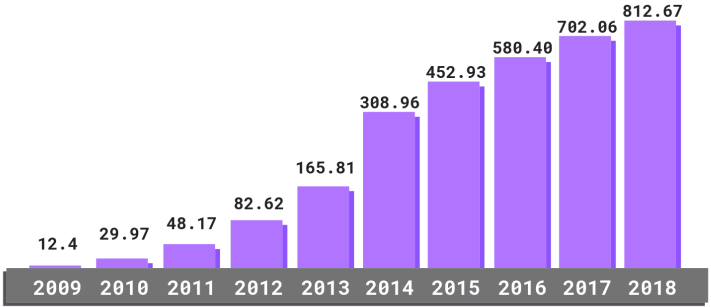
5 Detection and Protection

6 Antivirus

What Malware is I

- Malware stands for "malicious software"
- Refers to any intrusive software developed by cybercriminals to:
  - Steal data
  - Damage
  - Destroy computers or computer systems

What Malware is II



Total Malware Infection Growth Rate (In Millions)

History I

Early Years:

- 1949: The first idea of a malware was written by John von Neumann who wrote an article postulating how a computer program could reproduce itself
- 1970s: The earliest documented viruses began to appear
- 1970s: The first virus, called Creeper Worm, an experimental self-replicating program was written by Bob Thomas
- Mid 1980s: The term “virus” was introduced
- In the 80’ a virus was defined as "a program that can infect other programs by modifying them to include a, possibly evolved, version of itself" by Fred Cohen
- 1988 Morris Worm infected 6000 machines (around 10% of ARPANET) and caused dmaage of around 1M$
- 1999 Melissa Virus: Generally acknowledged as the first mass-emailed virus

History II

Recent years:

- Malware evolved and became really sophisitcated
- We can find not only viruses and worms, we can find also ransomwares, rootkits, trojans...
- 2017: Wannacry ransomware affected more than 150 countries and countless financial losses

1 Introduction

2 Types of Malware

3 Infection

4 Propagation

5 Detection and Protection

6 Antivirus

Types of malware

- We can divide malware depending on what they do:
  - Virus
  - Trojan Horse
  - Worm
  - Keylogger
  - Ransomware
  - Rootkits
  - Adware
  - Spyware
  - Backdoor

Virus

- Is a program that can infect other programs by modifying them to include a, possibly evolved, version of itself
- We can consider 2 types of virus:
  - Polymorphic: has the capability to auto-encrypt itself with different keys, therefore, each copy of the virus is different
  - Metamorphic: has the capability to modify its own code to avoid being detected

Trojan Horse I

Trojan Horse II

- Is a type of malware that disguises itself as legitimate code or software
- Trojan malware cannot replicate itself or self-execute
- It requires specific and deliberate action from the user
- To defend against trojans is to never download or install software from unknown sources

Worm

- Like a virus, a worm can spread itself to other devices or systems
- However, a worm does not infect other programs
- Worms often try to spread through the network using known vulnerabilities, waiting for the malicious actor to act.
- To protect yourself against worms, the best way is to keep the devices updated

Keylogger

- Monitors user activity, specifically keyboard keystrokes
- Can be used to steal sensitive information as passwords, bank accounts...

Ransomware

- Is software that uses encryption to disable a target's access to its data until a ransom is paid
- The victim often has to pay to recover its data, but he has no guarantee that the payment results in the decryption of the data
- One of the most well-known ransomware attack is wannacry

Rootkits

- Is software that gives malicious actors remote control of a victim's computer with full administrative privileges
- Rootkits can be injected into applications, kernels, hypervisors, or firmware
- Rootkits can be hard to remove if they reside, for example, in the kernel or firmware

Adware

- Tracks a user's surfing activity to determine which ads to serve them
- Really annoying kind of malware
- To avoid this malware the best way is to keep the devices and software updated

Spyware

- Is a malware that collects information about users' activities without their knowledge or consent
- Spyware usually aims to track and sell your internet usage data, capture sensible information or steal personally identifiable information

Backdoor

- Is a covert method of bypassing normal authentication or encryption in a computer
- Used to gain unauthorized access to computers

1 Introduction

2 Types of Malware

3 Infection

4 Propagation

5 Detection and Protection

6 Antivirus

Infection I

- The first phase of a malware to harm a computer or a network of computers is the infection
- Consists in the introduction of malware on the device
- Most of the cases this is because a vulnerability (keep updated your devices)
- This phase can be automatic (written in code what the malware has to do) or orchestrated by an attacker (remote control or direct attack)
- After this phase, the attacker can damage devices or spread through the network before performing the attack

Infection II

Examples infection

- Being infected via email (downloading stuff or clicking links)
- Inserting a pen drive in your computer
- Compromised webpages
- Malicious software downloaded from untrusted locations
- Exploiting vulnerabilities in your OS or apps
- Network propagation

1 Introduction

2 Types of Malware

3 Infection

4 Propagation

5 Detection and Protection

6 Antivirus

Propagation

- Consists in the infection of more devices of a network before performing the attack
- This phase can be also done automatic or orchestrated by an attacker
  - Automatic: Worms, virus...
  - Attacker: keylogger, trojan...
- Known vulnerabilities are almost always used to spread malware to other machines

Examples Propagation

- Send bulk email messages to the next victims
- Exploit OS vulnerabilities of machines connected to the same network
- Exploit app vulnerabilities of machines connected to the same network

1 Introduction

2 Types of Malware

3 Infection

4 Propagation

5 Detection and Protection

6 Antivirus

Detection I

- If the malware is already in the system, it is necessary to detect it to remove it asap
- The detection part can be done by multiple tools:
  - IDS
  - Sandbox Analysis
  - Malware signature
  - Antivirus
- It is impossible to build a perfect malware detection system

Detection II

Malware can do some things to avoid being detected

- Obfuscate the code (packer):
  - Dead-Code Insertion: Insert code that does nothing
  - Subroutine Reordering: Modify the order of the code
  - Code evolution: Modification code but doing same stuff
  - Code compression: Compress the code
  - Code Integration: Binds in others code
    - Prepending
    - Appending
    - Cavity
    - Multicavity
    - Overwriting

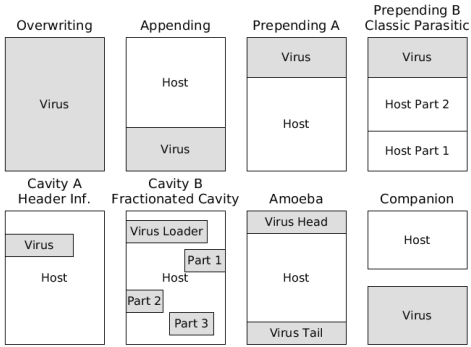
Detection III

Original Source Code Before Rename Obfuscation

```
private void
CalculatePayroll (SpecialList employee-
Group) {
    while (employeeGroup.HasMore()) {
        employee =
employeeGroup.GetNext(true) ;
        employee.UpdateSalary() ;
        Distribute Check(employee) ;
    }
}
```

Reverse-Engineered Source Code After Rename Obfuscation

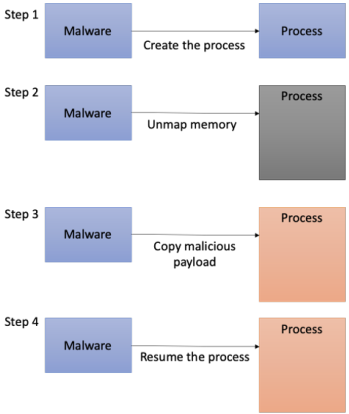
```
private void a(a b) {
    while (b a()) {
        a = b.a(true);
        a.a () ;
        a.(a) ;
    }
}
```



Detection IV

- Environmental awareness:
  - User interaction
  - Domain/IP identification
  - Check hardware
- Time-based: Malware takes action in some periods of time
- Process hiding: Inject code to a running process

Detection V


Step 1
Malware
Create the process
Process
Step 2
Malware
Unmap memory
Process
Step 3
Malware
Copy malicious payload
Process
Step 4
Malware
Resume the process
Process

Detection - IDS I

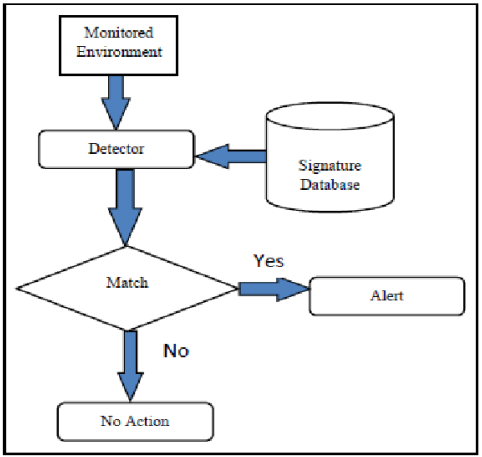
- Analyze and monitor network traffic for signs that indicate something weird in the network
- Notify the user if something is suspicious
- Signature based IDS vs Anomaly based IDS

Detection - IDS II

Signature based IDS:

- Compares software signatures with its database
- Less false positives
- Not effective to detect new threats
- Low cost and low resources
- Effective to detect known malware but not effective to unknown malware
- Malware as virus can modify or obfuscate it's own code and therefore it's signature

Detection - IDS III

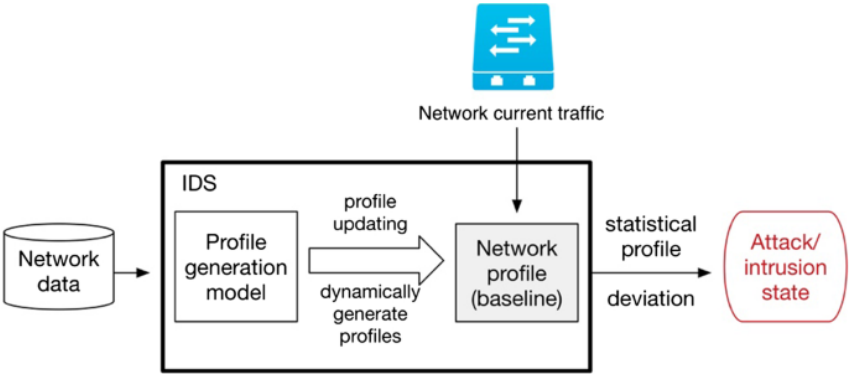


Detection - IDS IV

Anomaly based IDS:

- Looks for strange patterns or behaviors
- More false positives
- Effective to detect new threats
- High cost and high resources
- Necessary to create a custom profile for each user
- Useful ML techniques
- Effective to detect known malware but some known and unknown can be passed as false positives

Detection - IDS V



Detection - Sandbox

- Running the executable in a VM and observe:
  - File activity
  - Network
  - Memory
- Environment detection can detect the use of a sandbox and prevent the execution of malware to avoid detection

Detection - Malware Signatures

- Find something that can identify the malware
- Like the "fingerprint" of the malware
- Examples:
  - Pieces of code
  - Hash of payloads
- Obfuscation of code can elude malware detection using signatures

Detection - Heuristics

- Analyze program behavior:
  - Files modifications
  - Network access
  - Modifications of OS
  - Modification of boot sector
- Detect modifications in program binaries

Detection - Antivirus

- Mix of all the last techniques
- Analyze system behavior
- Analyze binary to decide if it a virus using different techniques

Protection and Prevention

- Use trusted antivirus and anti-malware software
- Keep OS and software updated
- Regular scans and monitor settings
- Rely only on secure networks
- Stay up-to-date on the latest cyber threats
- Beware of downloads
- Employ common sense in while surfing internet
- Firewalls/IDS/IPS
- Regular backups of data

1 Introduction

2 Types of Malware

3 Infection

4 Propagation

5 Detection and Protection

6 Antivirus

What is an Antivirus I

- Is a computer program used to prevent, detect, and remove malware
- Originally developed to detect and remove computer viruses
- However, today they protect against other computer threats
- Most antivirus uses a combination of signature detection and behavior detection
- Frederick B. Cohen's in 1987 demonstrated that there is no algorithm that can perfectly detect all possible viruses
- However, using different layers of defense, a good detection rate may be achieved.

What is an Antivirus II

Modes of operation I

- Static file scanning: Inspection of the file without being run inspecting the internal structure of the application
  - Examining source code
  - Examining binaries
- Dynamic file scanning: Inspection of the file during its execution
  - Examining process behavior, files opened, resources required...

Modes of operation II

- Static is useful when:
  - Check signatures
  - The malware can be reverse engineered to see what is capable to do
- Dynamic is useful when:
  - In a sandbox environment see the behavior of the malware and study it

Antivirus tools

- Uses a mix of all techniques described in the last section
- It can use heuristics to analyze the behavior in a sandbox environment
- Check signatures of installed softwares
- Monitor the incoming and outgoing packets (IDS)
- etc...
- However some security professionalsthink that the current approach is not the best...
- But all help is welcome

Weaknesses of Antivirus I

- Inability to protect themselves: With enough system permissions, malware can change antivirus settings and configurations to hide
- Updates: An antivirus is only as good as its last update, it cannot protect against:
  - New or modified malicious code
  - Rootkit programs
  - Software misuse
- Stupid users: Large number of attacks are due to the ignorance of users (phishing, click on malicious links...)
- Malware antivirus: Malware injected in antivirus process 👀

Weaknesses of Antivirus II

- False sense of security: Can cause that the users think that is 100% secure and drop their guard
- Can't revert result of malware infection: They cannot revert the harm done by malware
- The cost of the antivirus: Some users don't buy antivirus because of its cost
- Performance problems: Some antivirus can degrade computer performance due to their scans
- Problem of false positives: Some antivirus can be configured to delete the detected malware or isolate it. However removing a false positive file may cause the failure of the system. See this

Strengths of Antivirus I

- Good protection against known and not mutable malware
- Execution of suspicious software in sandboxes
- Increases the user's protection
- Limits access to some websites

The END!