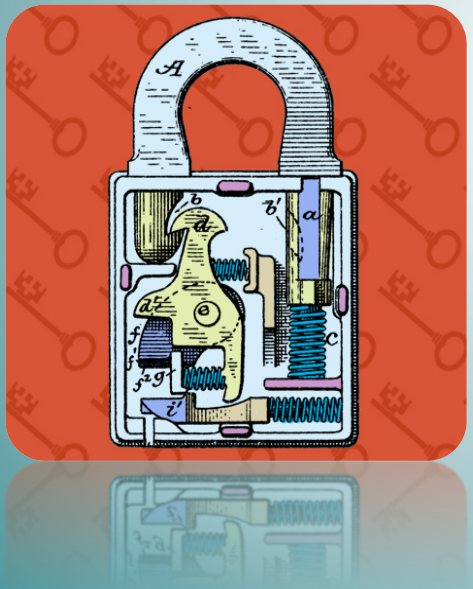
# Garantía y Seguridad en Sistemas y Redes

## Tema 5. Malicious Software



**Esteban Stafford**

Departamento de Ingeniería Informática y Electrónica

# Contents

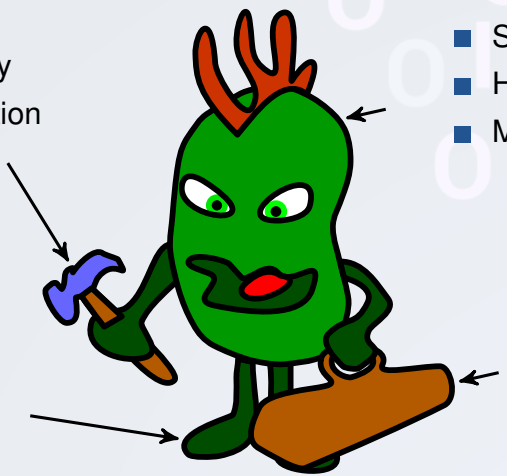
# Anatomy of Malware

**Infiltration Tool**

- User
- Vulnerability
- Code injection

**Attitude**

- Spread
- Hide
- Mutate



**Means of Transport**

- Removable media
- Network
- Email

**Payload**

- Destroy stuff
- Send Spam
- Attack elsewhere
- Spy

# Broad malware classification

| Name | Description |
|---|---|
| Virus | When executed, tries to replicate itself into other executable code, infecting it. When the infected code is executed, the virus also executes. |
| Worm | A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network. |
| Logic bomb | A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act. |
| Trojan horse | A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program. |
| Backdoor | Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality. |
| Mobile code | Software (e.g., script, macro...) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics. |
| Exploits | Code specific to a single vulnerability or set of vulnerabilities. |
| Downloaders | Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail. |
| Auto-rooter | Malicious tools used to break into new machines remotely. |
| Attack Kits | Set of tools for generating new malware automatically. |
| Spammer | Used to send large volumes of unwanted e-mail. |
| Flooders | Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack. |
| Keyloggers | Captures keystrokes on a compromised system. |
| Rootkit | Set of tools used after attacker has broken into a computer system and gained root-level access. |
| Zombie, bot | Program activated on an infected machine that is activated to launch attacks on other machines. |
| Spyware | Software that collects information from a computer and transmits it to another system. |
| Adware | Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site. |

# Attack kits and Attack sources

## Attack Kits

- Creation of malware requires great technical skills.
- Today, tools exist to create and manage malware easily.
- These toolkits are known as **crimeware**.
- Malware created this way is easier to detect.
- But their large amount make them difficult to defend against.

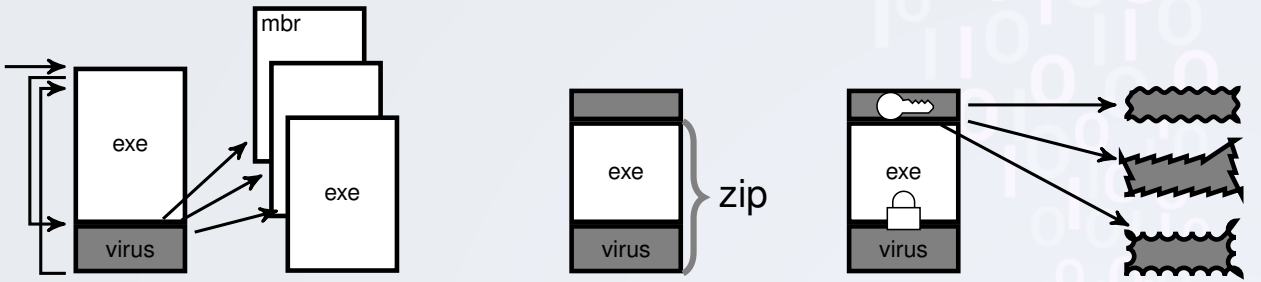
## Attack Sources

- In the past attackers sought demonstrating technical ability.
- Today, the main motivation is money, but can be also political or even military.

# Viruses

## At a glance...

- Means of transport: Removable media, Email.
- Infiltration tool: User.
- Attitude: Spread.
- Payload: Destroy stuff, encrypt files and ask for ransom.



# Worms

## At a glance...

- Means of transport: Network.
- Infiltration tool: Vulnerability.
- Attitude: Spread.
- Payload: Spy, open backdoor, deploy bot...

- Worms propagate through vulnerabilities. Viruses do not need this. They propagate by “legitimate" methods. The user “helps" the virus. The worm “helps itself", therefore spreads much faster.
- Vulnerabilities can be reduced by patching and firewalls.
- Infections can be removed by antivirus software.

# Worms

- Zero-Day vulnerabilities are those that don't have a patch available.
- Typically, worm exploit vulnerabilities of:
  - Remote file transfer, login or execution services.
  - Email or Instant Messenger
  - Browser: Drive-by-download.
  - Web-server: Code injection, Cross-Site-Scripting (XSS)
- Finds new targets by:
  - Random IP address.
  - Pre-written Hit-list.
  - Topological search.
  - Local subnet.

# Spam

- Not widely known as Unsolicited Bulk Email (UBE).
- Not strictly malware — No code.
- Accounts for 70-90% of all emails sent.
- In the past, Spam was sent by compromised legitimate mail servers.
- Large scale protection by blacklisting.
- Today, Spam is sent by botnets.
- User scale protection by antispam filtering: keywords, bayesian filters.

# Trojan horses

## At a glance...

- Means of transport: User download.
- Infiltration tool: User.
- Attitude: Hide.
- Payload: Spy.

- Trojan horses pose as useful software, that the user installs.
- Trojan might:
  - Perform original and malicious functionality.
  - Pervert the original purpose of the application.
  - Perform only malicious activity.

# Destructive malware

## Data destruction

- Delete files. Zero filesystem structures.
- Encrypt files and demand payment to obtain key.

## Real-World Damage

- Alter BIOS settings to render the computer unbootable.
- Continuously write media and produce bad sectors.
- Rewrite industrial equipment firmware inducing failure.

## Logic bomb

- Malware produces damage when some conditions are met.
- Date. Number of infections. User starts application. Incomplete malware removal. Successful spying.

# Remote control

## Bots, Zombies

- Compromised machine obeys commands from master.
- A group of [ro]bots is called a **botnet**.
  - DDoS attack
  - Relay Spam
  - Sniff traffic
  - Use computing power
  - Keylog/Video capture
  - Seed new malware
  - Install unwanted Software
  - Manipulate of Polls/Games
  - Anonymizing Proxy
- Communication to master: IRC, HTTP, Peer-to-peer.
- Bot functionality is usually preinstalled, but they can also be updated.

# Personal information theft

## Credential theft, keylogging and spyware

- Since authentication encryption, traffic sniffers are less effective.
- **Keyloggers** monitor keyboard events and keep login data.
- Mouse-driven authentication caused the development of **spyware**.
  - Wider monitoring capabilities.
  - Redirection of certain web-pages.
  - Alter browser-server communication.

# Personal information theft

## Identity theft, Phishing and Spear-phishing

- **Phishing** uses Spam to lure users to fake web-servers.
- Unaware users might give important credentials or data to fake-server.
- **Spear-phishing** is a carefully crafted phishing attack directed to selected victims.

## Reconnaissance and Espionage

- Same techniques as above but not focused on personal credentials.

# Stealth Access

## Backdoor

- Also known as **Maintenance hook** allows developer to debug software.
- Unscrupulous programmer might leave/forget it in the production version.

## Rootkit

- Set of tools to grant covert privileged access to a system.
- They modify the system to hide their presence.
- Persistent, memory based, user mode, kernel mode, external mode, virtual machine based.