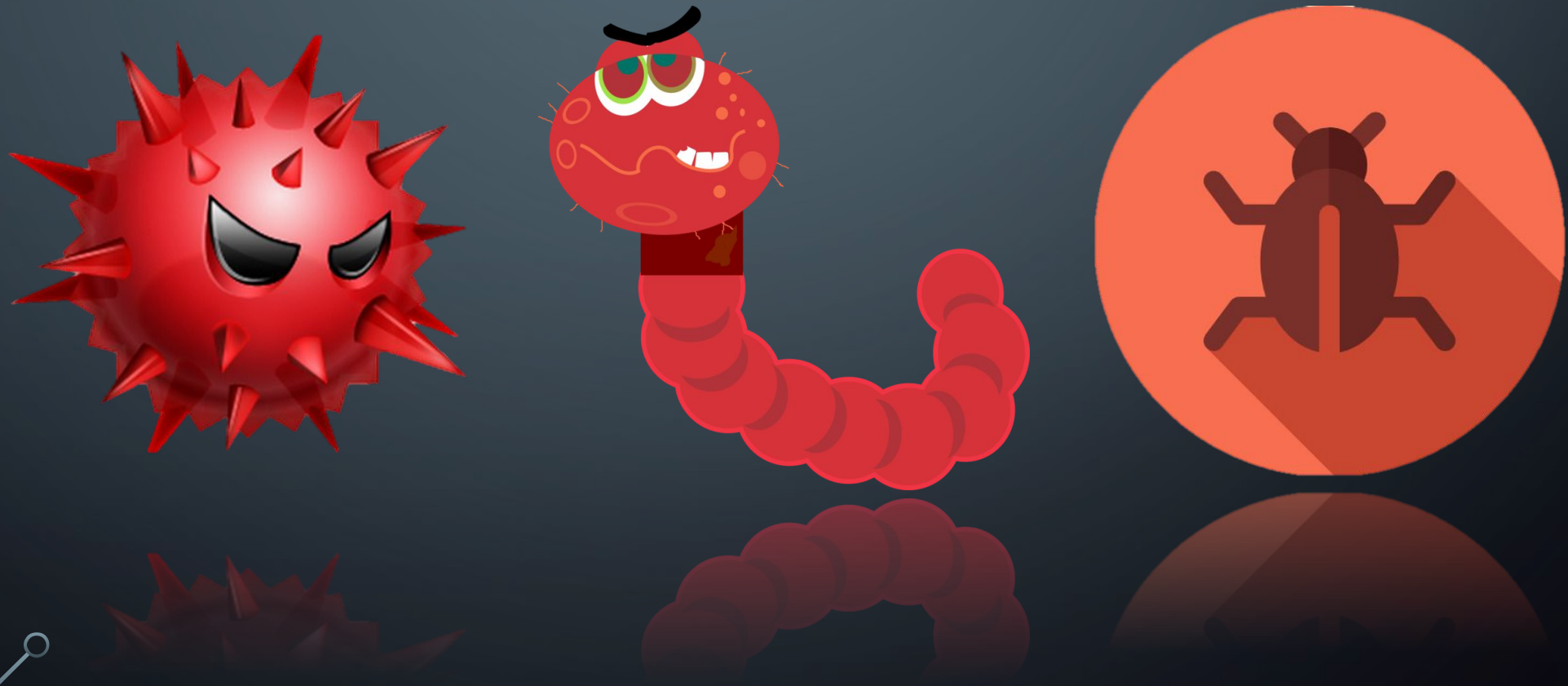
Malware in our live

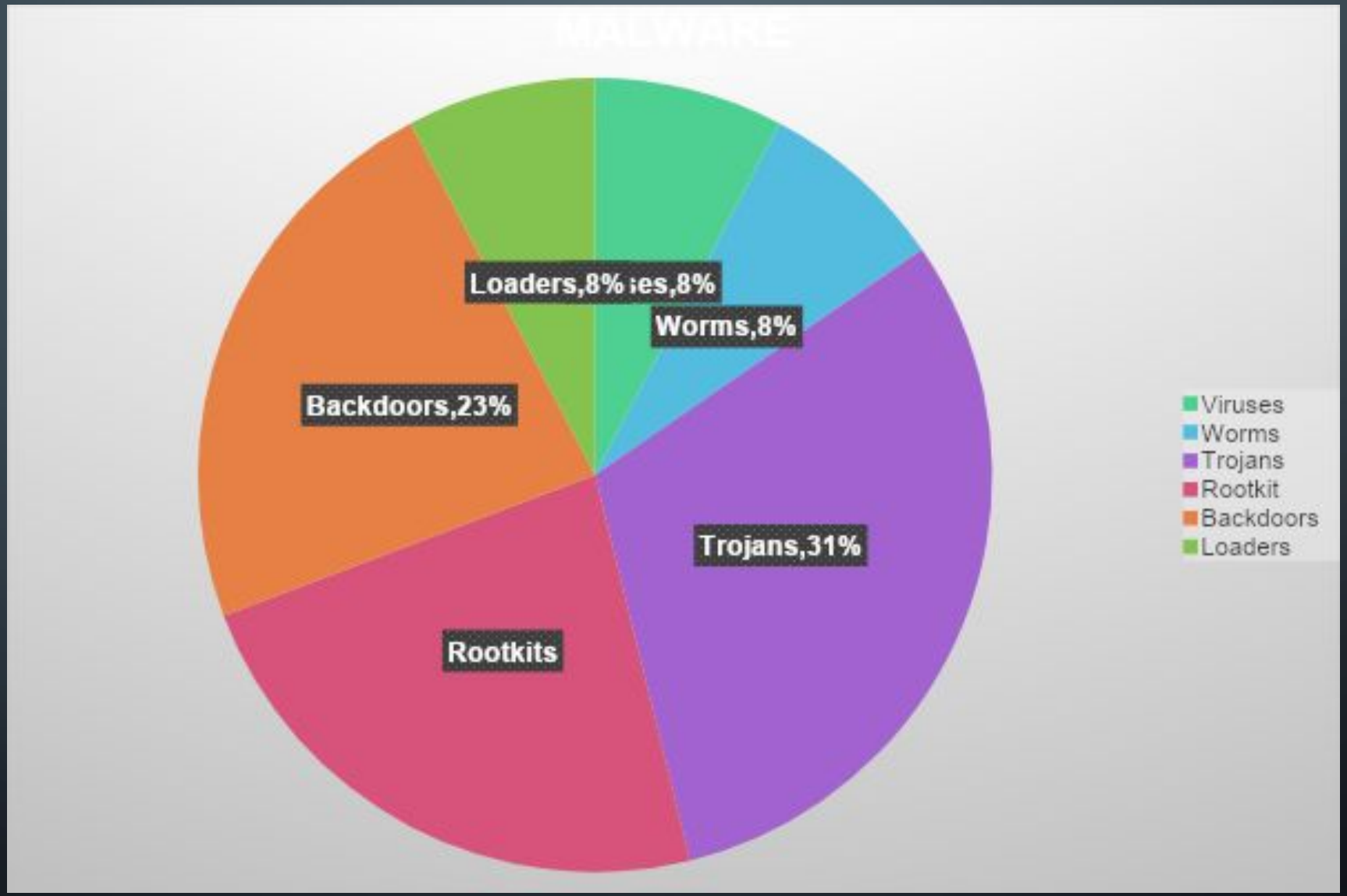


PLAN

- 1. What is a malware? Types, functions and working principle
- 2. Ways to enter malware to your computer
- 3. Ways to protect against malicious software

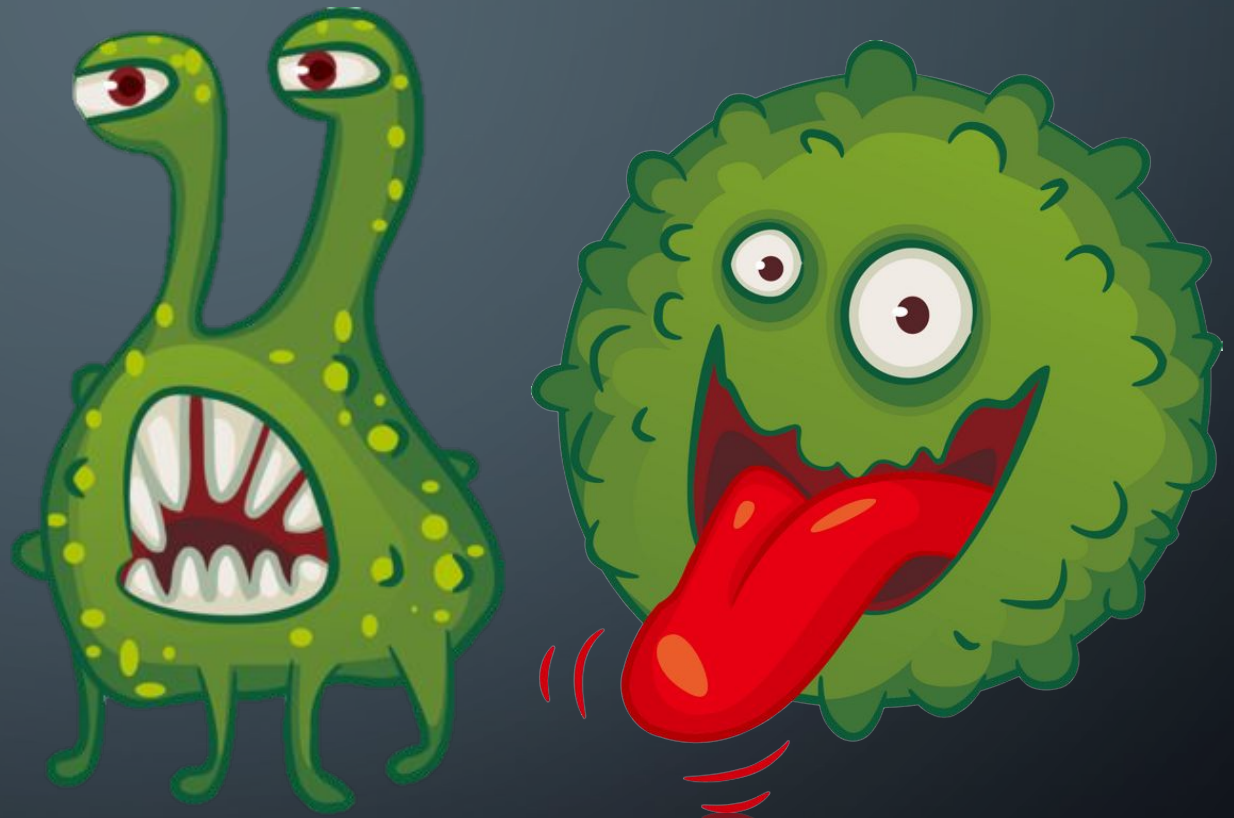
What is a malware?

- Malware is a software intentionally designed to cause damage to a computer, server, client, or computer network.

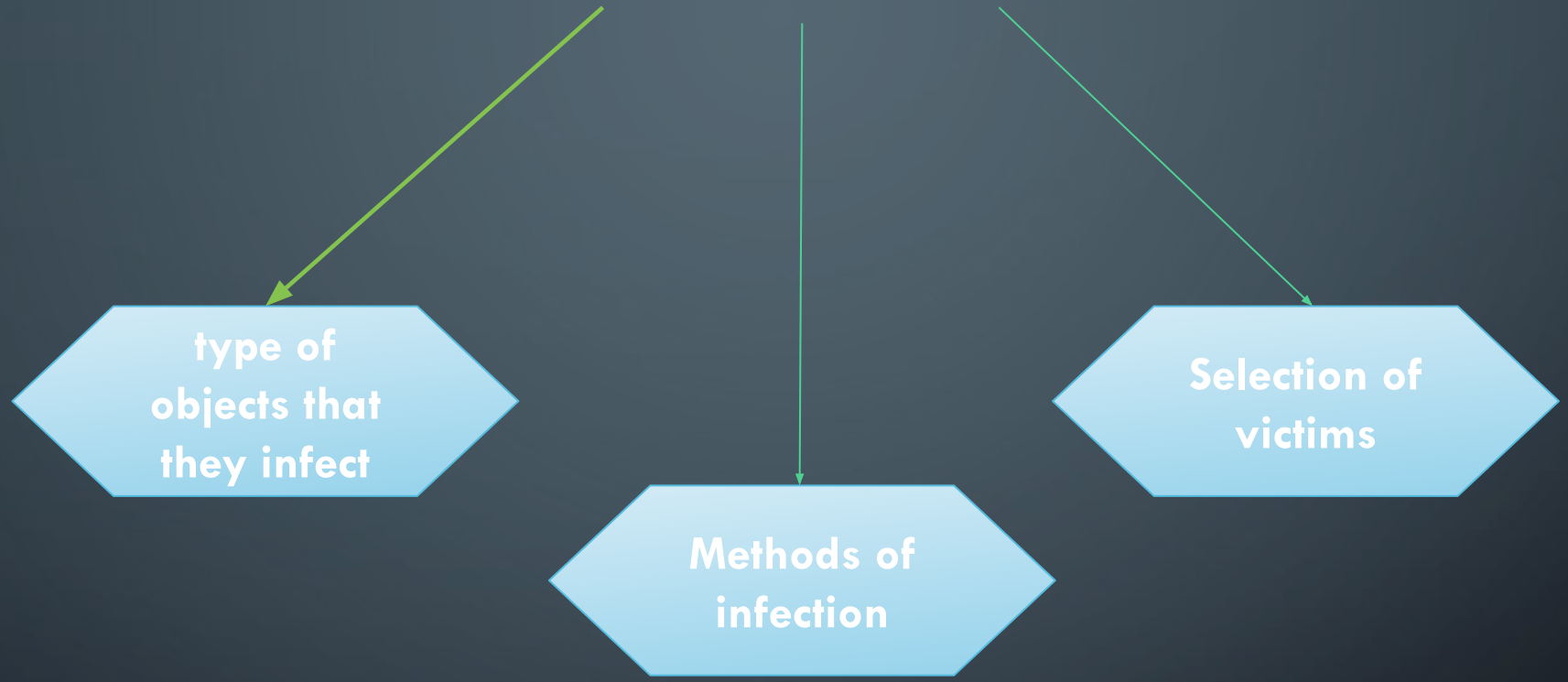

MALWARE
Loaders,8%
Worms,8%
Backdoors,23%
Trojans,31%
Rootkits
Viruses
Worms
Trojans
Rootkit
Backdoors
Loaders

VIruses

- A virus - is a self-replicating program code that is embedded in installed programs without the user's consent.



VIRUSES


type of objects that they infect
Methods of infection
Selection of victims

Worms

- is a standalone malware computer program that replicates itself in order to spread to other computers.
- Worms are in some way viruses, as they are based on self-replicating programs. However, worms cannot infect existing files.

Trojans

- By its action is the opposite of viruses and worms. It offers to download under the guise of a legitimate application, but instead of the stated functionality, it does what the attackers need.
- The current Trojans have evolved to such complex forms as, for example, backdoor and trojan loader.

RootkitS

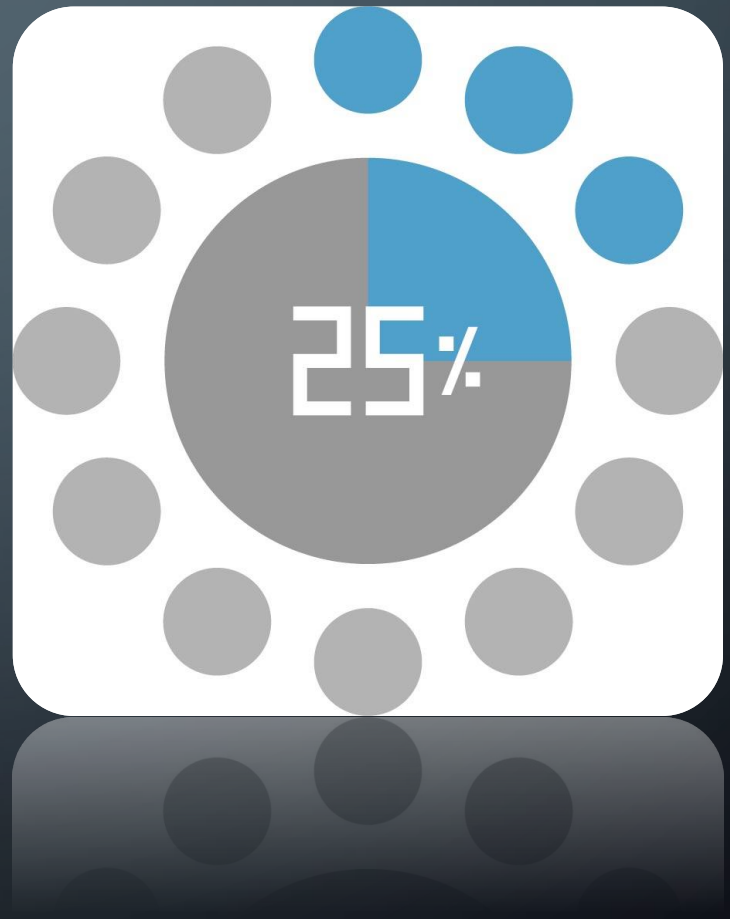
- In the modern world, a rootkit is a special part of malicious programs designed specifically to hide the presence of malicious code and its actions from the user and the installed security software. This is possible due to the tight integration of the rootkit with the operating system.

BACKDOORS

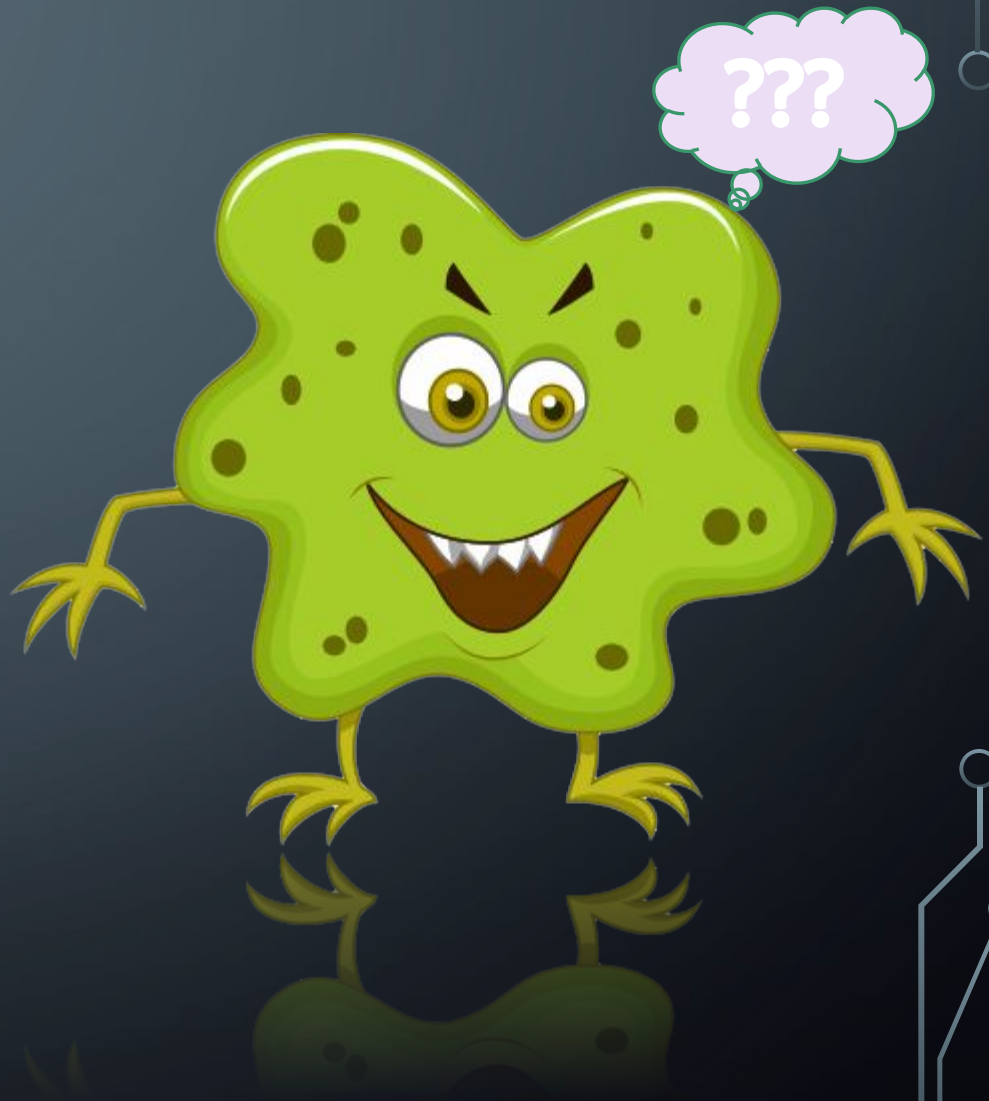
- is an application that allows a system administrator or an evil intruder to control your computer from a distance. Depending on the functional features of the specific backdoor, a hacker can install and run any software on the victim's computer, save all keystrokes, download and save any files, turn on a microphone or a camera.

LOADERS

- Loader - a small part of the code used to further download and install the full version of the malware

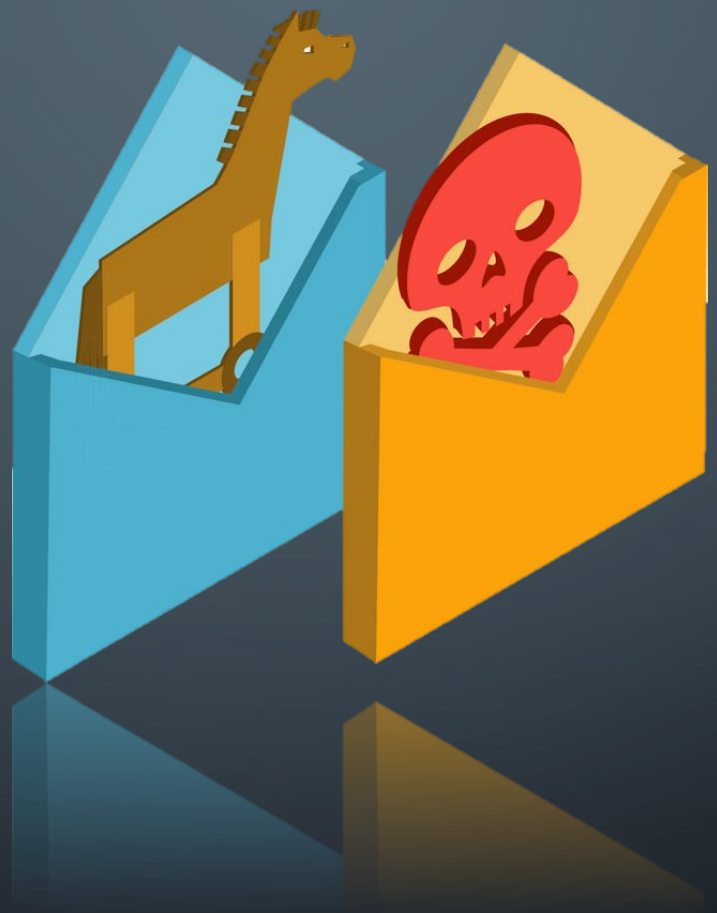


How malware can get on your computer?



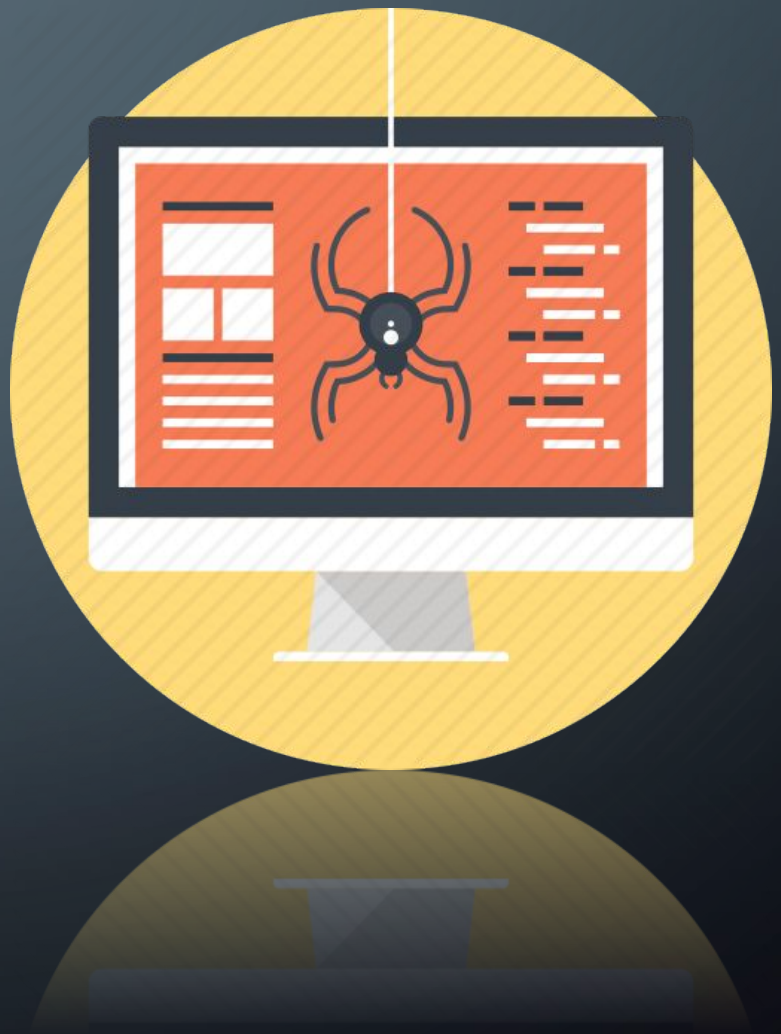
E-mail with an attachment

- Often, people out of curiosity open an incoming message, after which problems begin



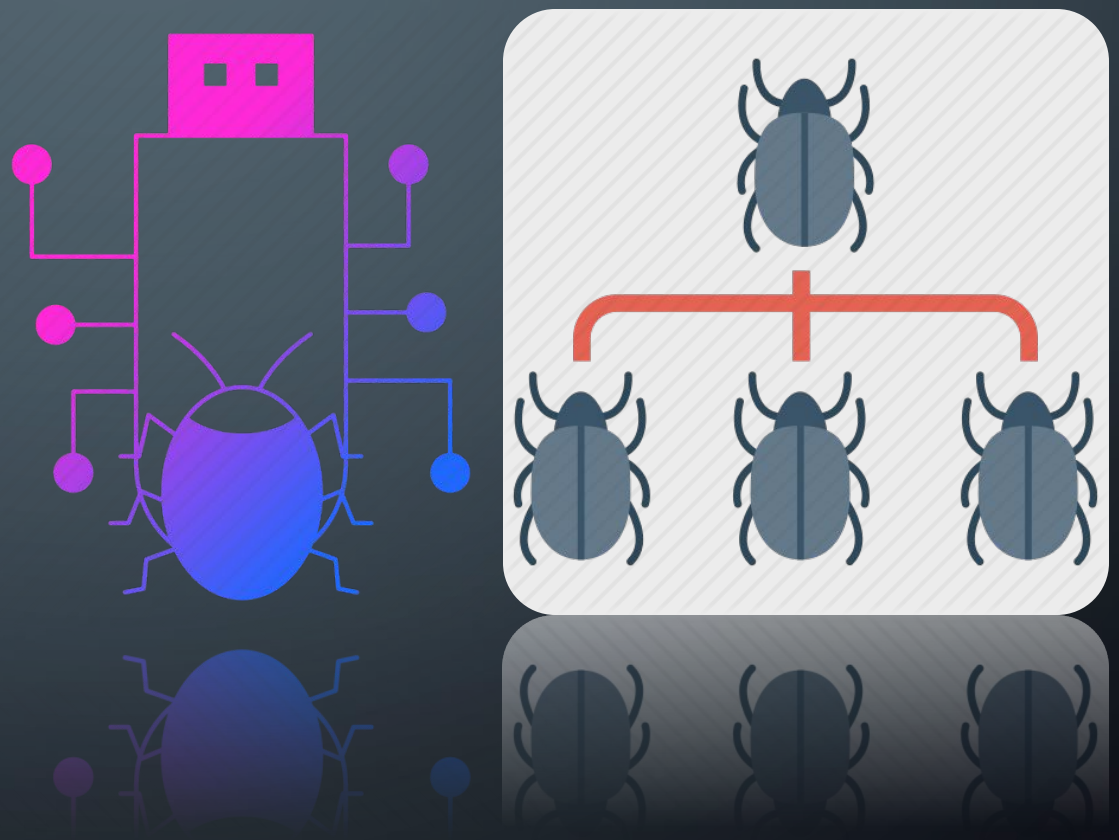
Web sites

- As you know, there are sites whose target audience are mostly adults. These sites are inherently unreliable, and also often spread computer viruses



Network

- If the computer is connected to a home network, or is part of a large network, you can easily get the virus through no fault of your own. One of the network members receives a virus and within a few minutes is the distributor of this virus.



Phishing

- Data loss as a result of phishing is a frequent occurrence, but it is also easy to infect a computer with viruses. When visiting fake sites, spyware programs often automatically install viruses on computers.

How to avoid infecting your computer with malware?

- As you can see, there are a lot of ways to spread computer viruses. To prevent infection, you can download any antivirus for free and install it in the system. At the same time, observe the elementary precautionary measures:

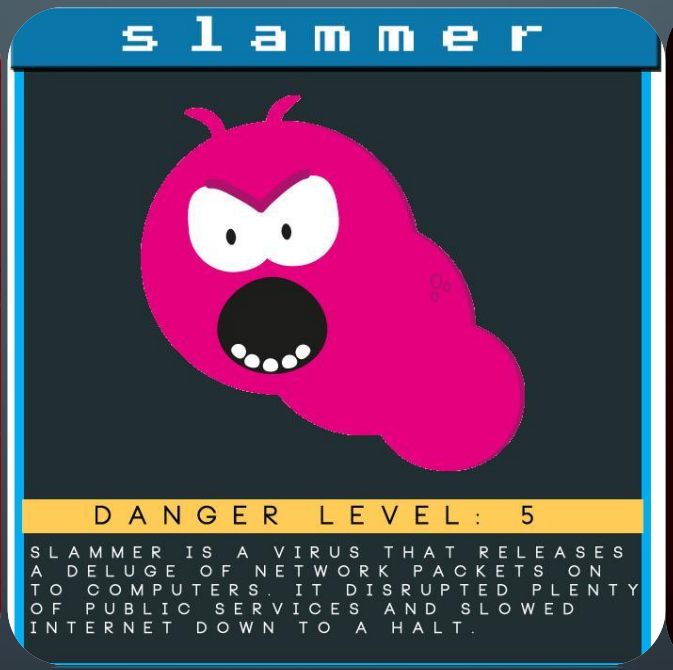
✔ 1. Use licensed antivirus

✔ 2. Check loaded programs before launch.

✔ 3. Avoid visiting sites of questionable content.

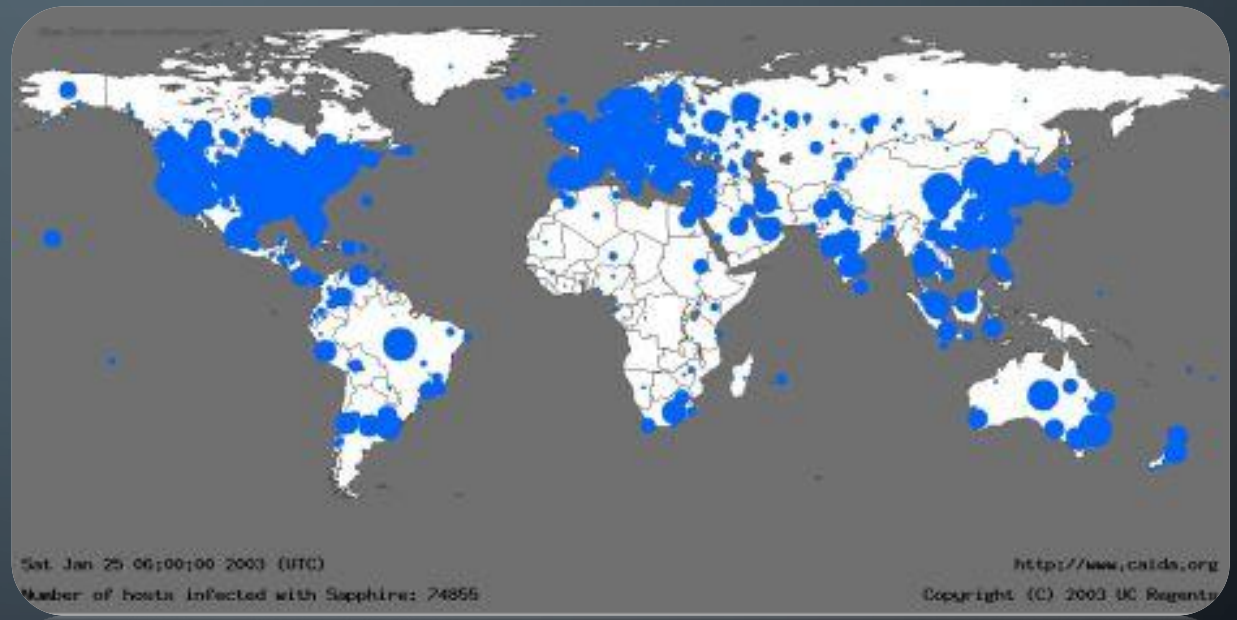
✔ and then you can easily avoid infection.

The most dangerous malware (͡° ͜ʖ ͡°)



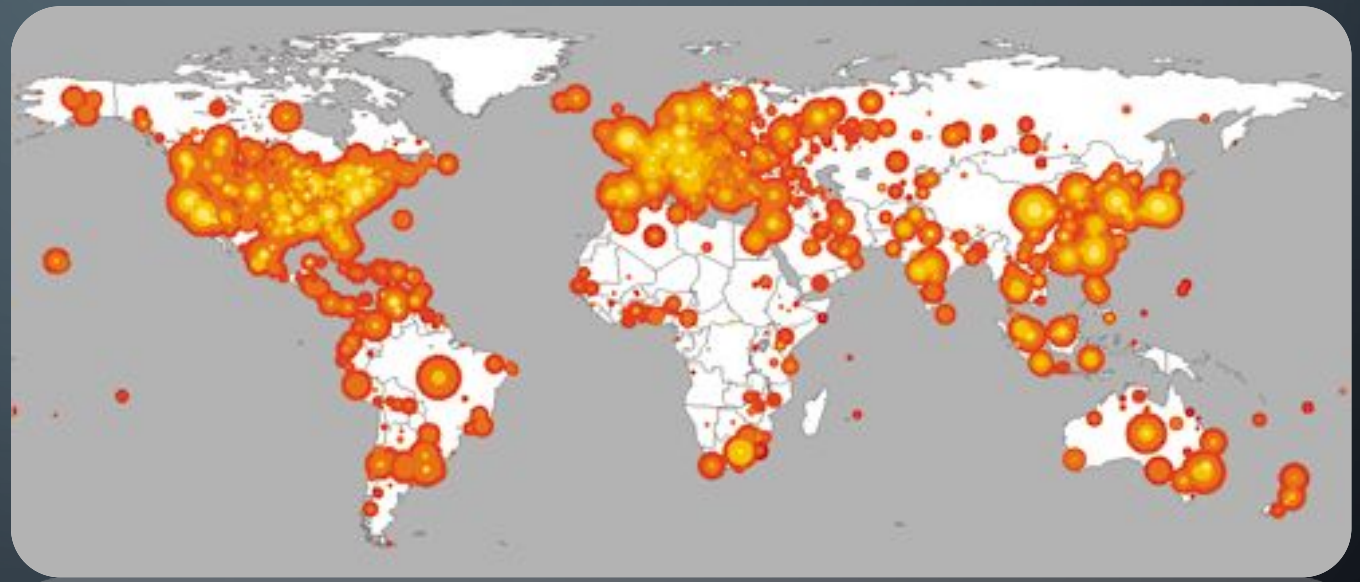
5. SLAMMER

- TYPE: WORM
- YEAR: 2003
- TARGET: SQL SERVERS
- DAMAGE: 1.2 BILLION
- ORIGIN: USA



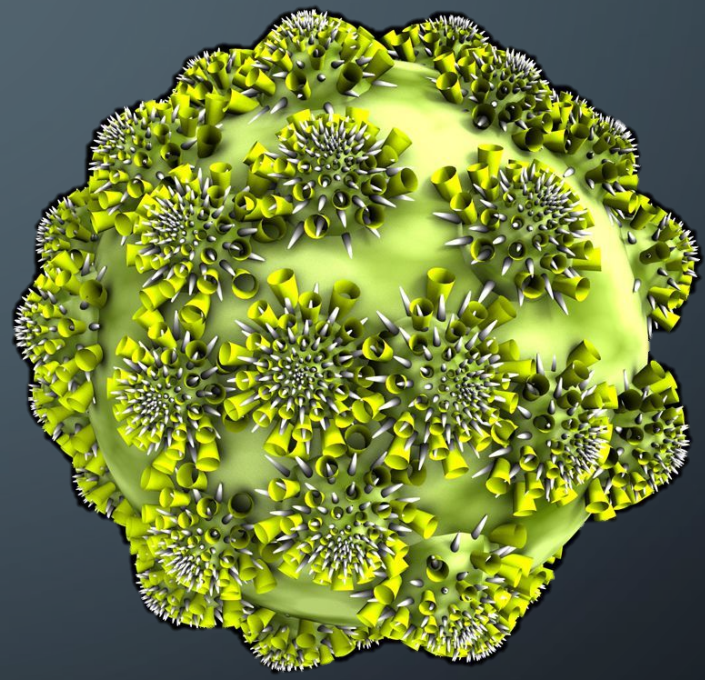
4. CODE RED

- TYPE: WORM
- YEAR: 2001
- TARGET: SERVERS
- DAMAGE: 2.6 BILLION
- ORIGIN: USA



3. ILOVEYOU

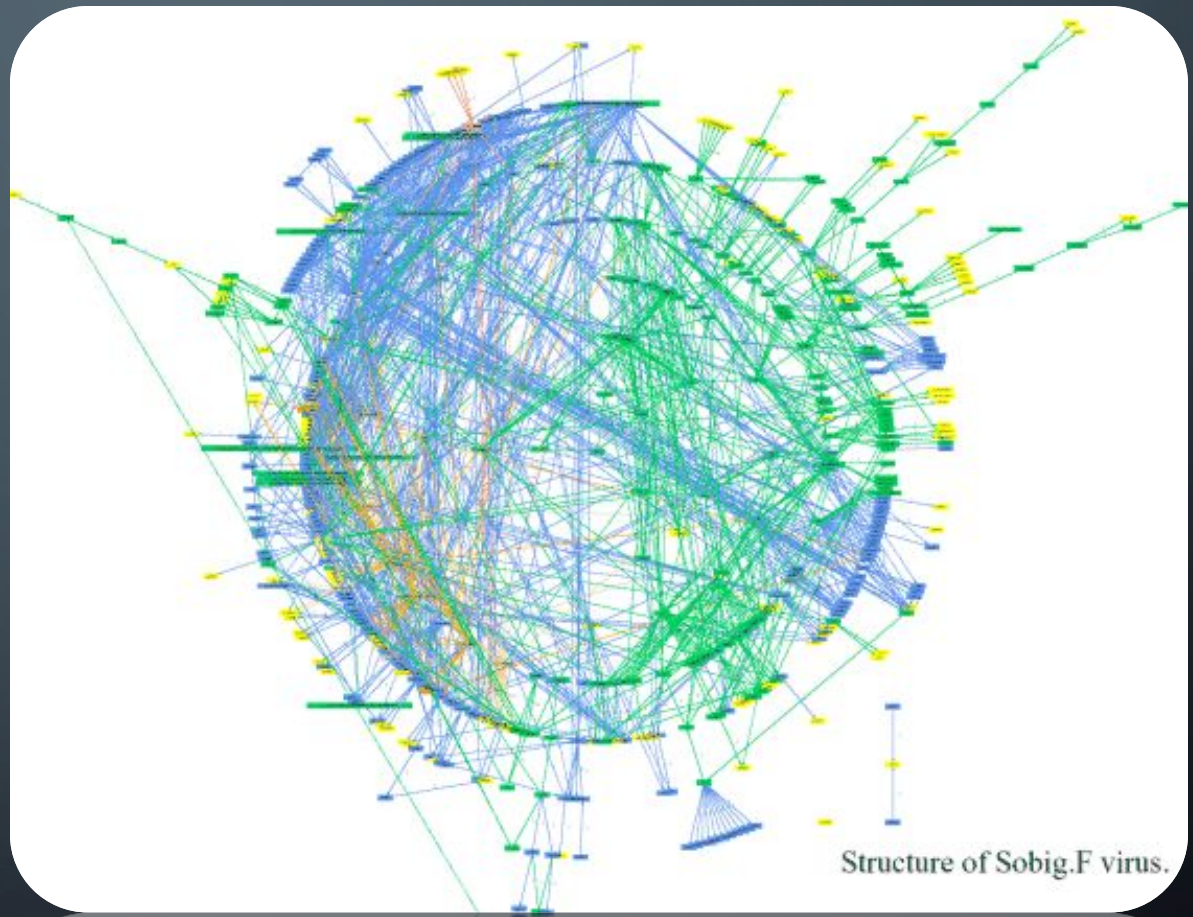
- TYPE: WORM
- YEAR: 2000
- TARGET: E-MAIL
- DAMAGE: 15 BILLIONS
- ORIGIN: Philippines



ILOVEYOU'S MODEL

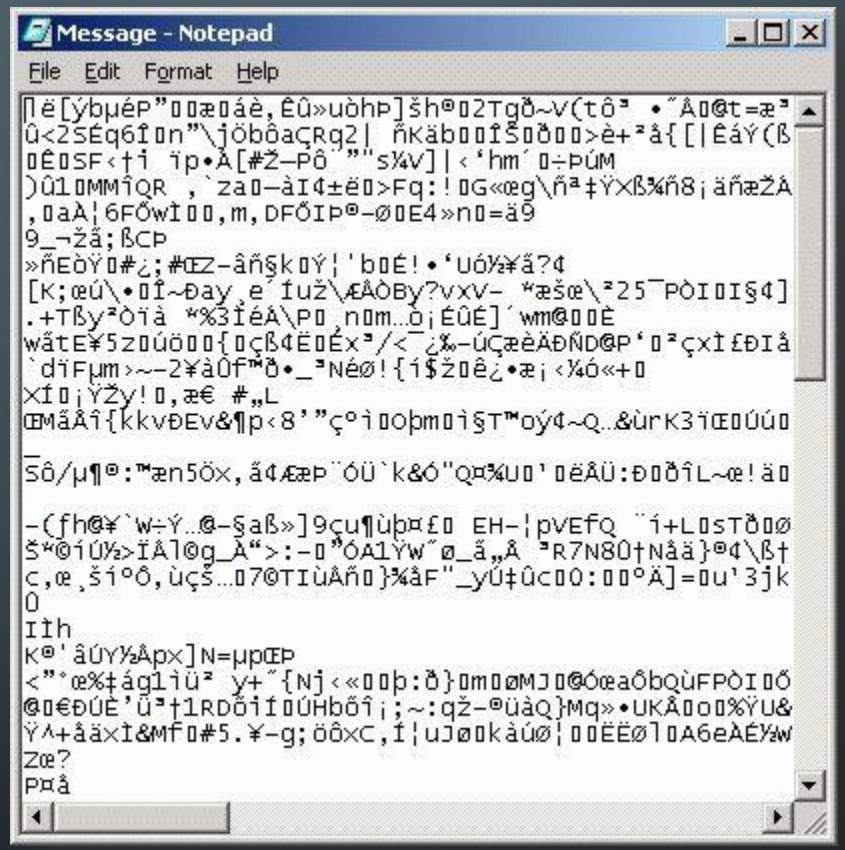
2. SOBIG.F

- TYPE: WORM | TROJAN
- YEAR: 2003
- TARGET: E-MAIL
- DAMAGE: 37 BILLIONS
- ORIGIN: UNKNOWN



MYDOOM

- TYPE: WORM
- YEAR: 2004
- TARGET: NDN
- DAMAGE: 38 BILLIONS
- ORIGIN: UNKNOWN



THX FOR
WATCHING!