Anatomy of a "polymorphic" virus

A **polymorphic virus** mutates when replicating (but keeps the original algorithm intact)

- By using cryptography
- By injecting garbage code
- By doing permutations within certain instructions or block of instructions
- By using code obfuscation technique

How to detect it?

➡ By detecting code patterns used for the self-modification

Macro Viruses

A **macro virus** is written in scripting languages used by some office applications (can be cross-platform)

- Written in VBS, embedded in a MS-office document, activated when the document is open (autoload function)

Concept (1995)

Melissa (1999)

- March 26 1999, Melissa shut down e-mail systems that got clogged with infected e-mails