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

Metamorphic Virus

A **metamorphic virus** can reprogram itself

- by using different instructions
- and by using different strategies to implement a functionality

Zmist (2000)

- First metamorphic virus

Simile (2001)

- First a multi-OS metamorphic virus