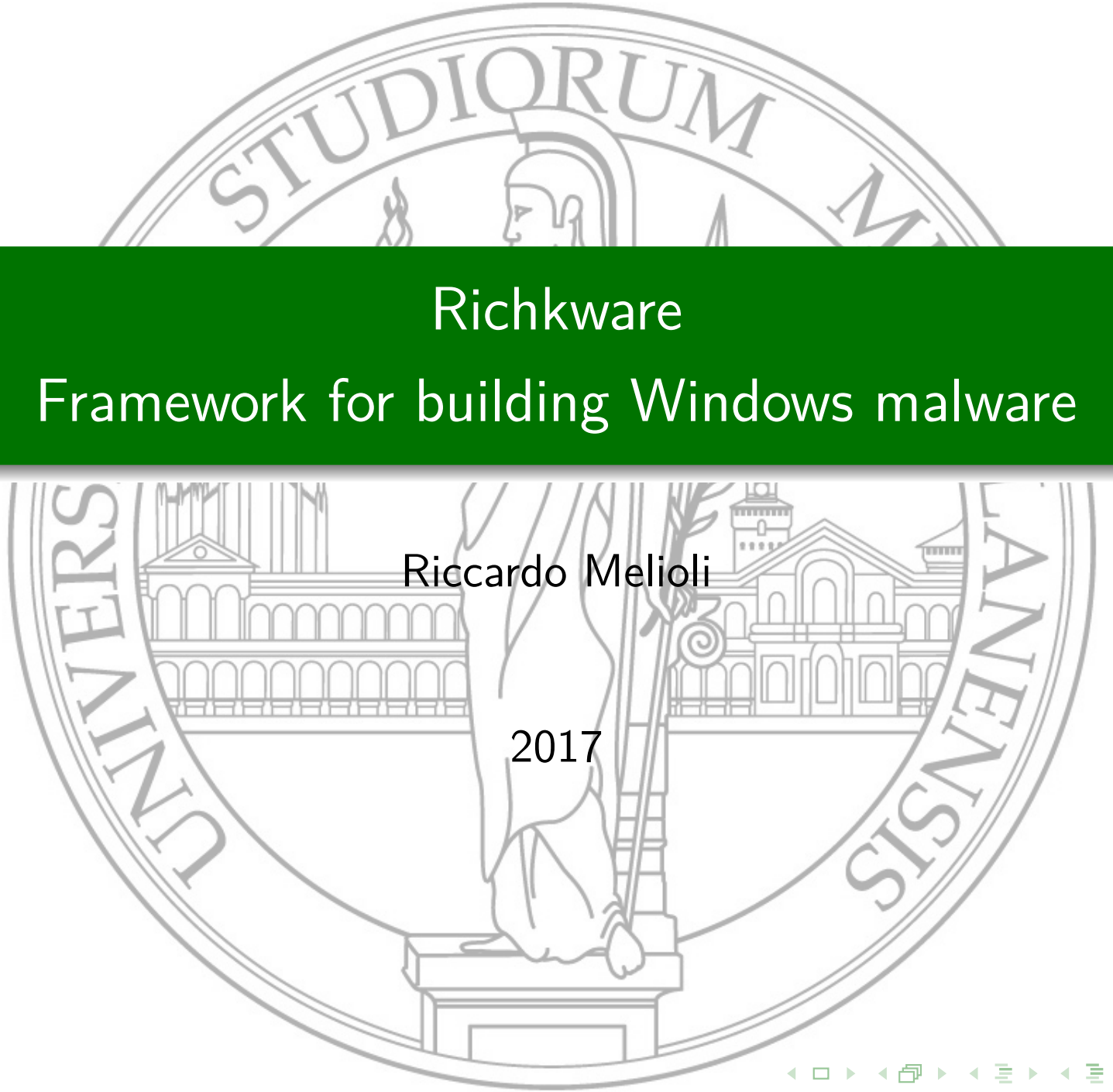


Richkware

Framework for building Windows malware

Riccardo Melioli

2017

Your Security System

Is your S.S. really reliable?

Are you sure that it's checking:

- Communication Channels
- Persistance Applications
- Open Sockets
- Keylogging
- ...

Goal of Richkware

Goal

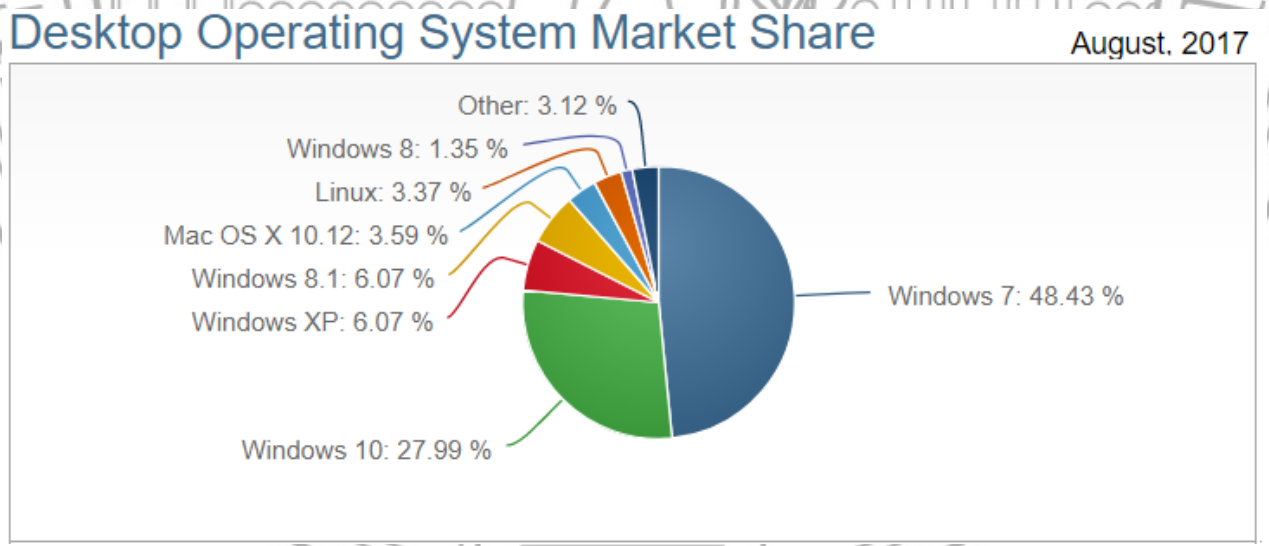
Richkware is an application that makes easier to **test your security systems**.

Target OS

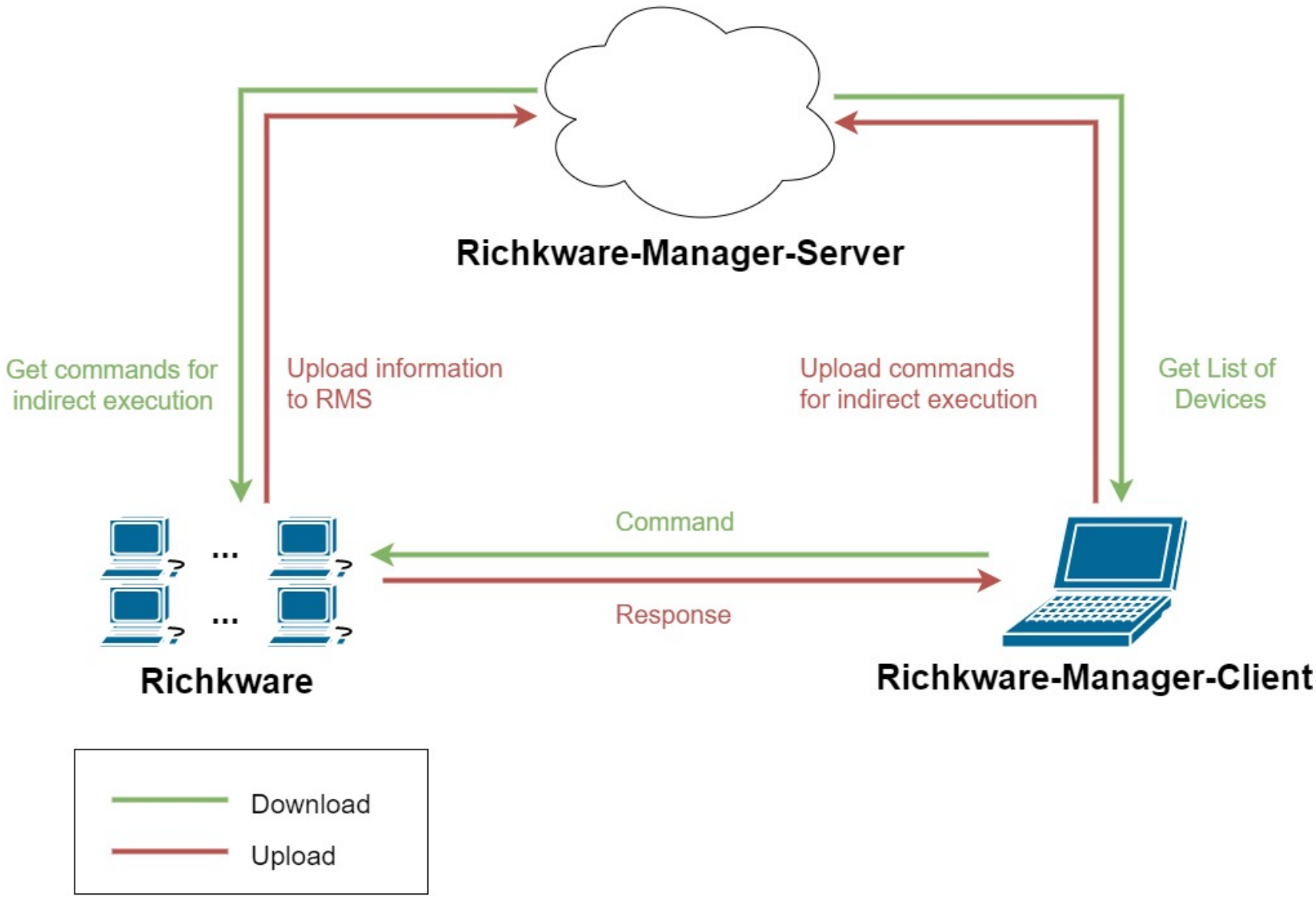
Why Windows?

The project is developed for the Microsoft Windows operating system as the target of attacks, because:

- many **vulnerabilities** are continually discovered, which could be exploited to gain more functionality.
- **popularity** of Windows, so there is more computers being infected



Project Structure



Richkware

What is it?

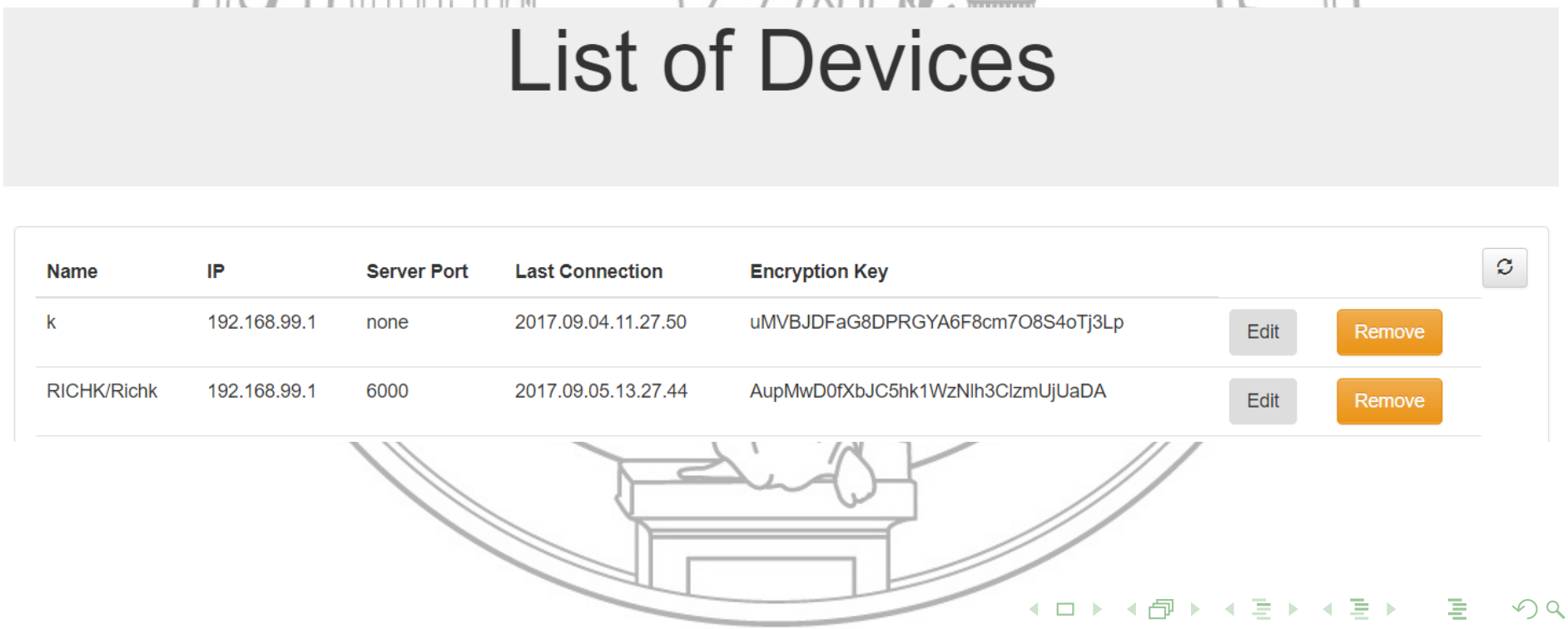
It's a library of network and OS functions, that you can use to create malware like:

- Virus
- Worm
- Spyware
- Keylogger
- ...

RMS - Richkware-Manager-Server

What is it?

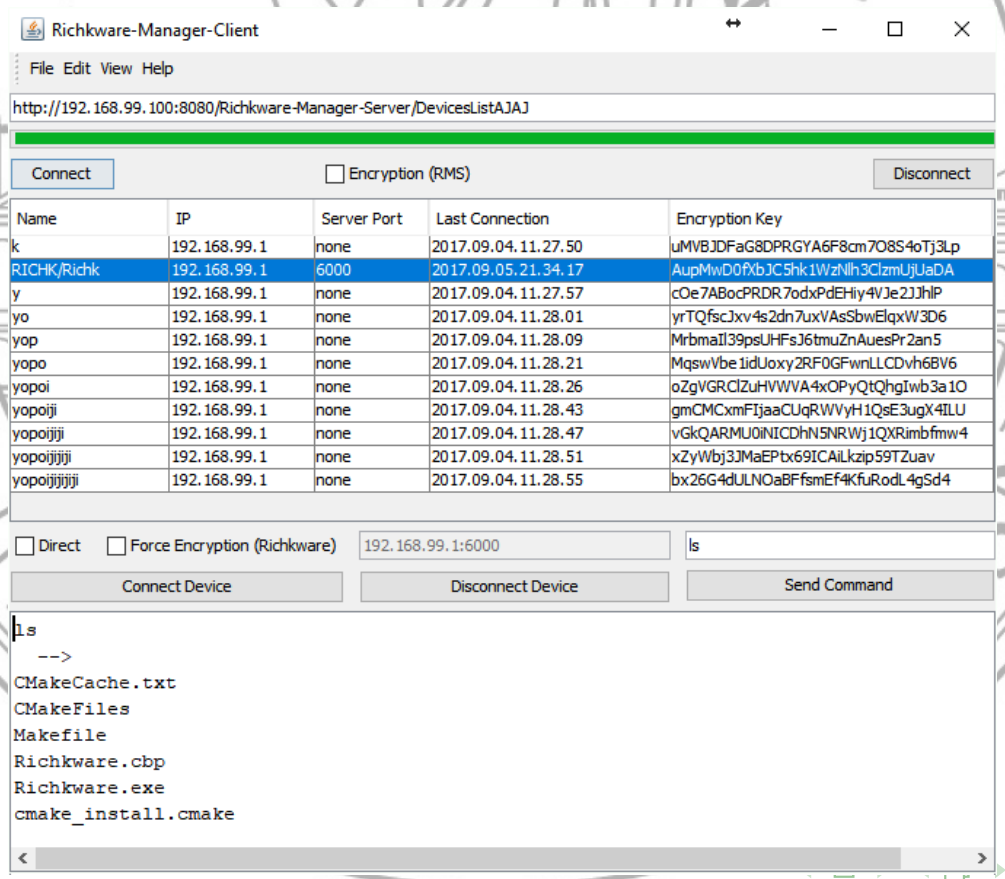
Service for **management** of hosts where is present a malware developed using Richkware framework. It **stores** all malware information in a SQL database.



RMC - Richkware-Manager-Client

What is it?

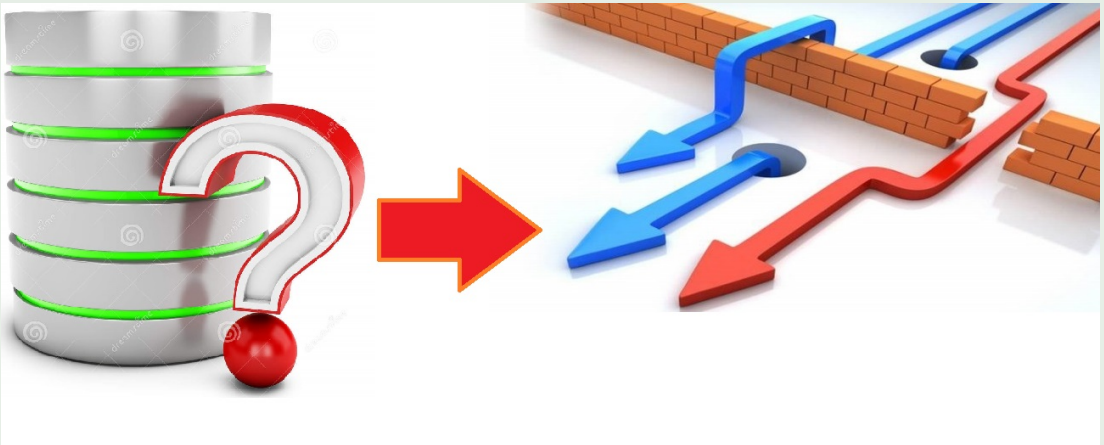
Richkware-Manager-Server Client, **gets the list** of all hosts from the server and allows to **send commands** to run on the infected pc, by safe communication.



Antivirus

Detection

In generally, the malicious applications developed with Richkware are **not detected** from Security Systems signature-based.



Exceptions

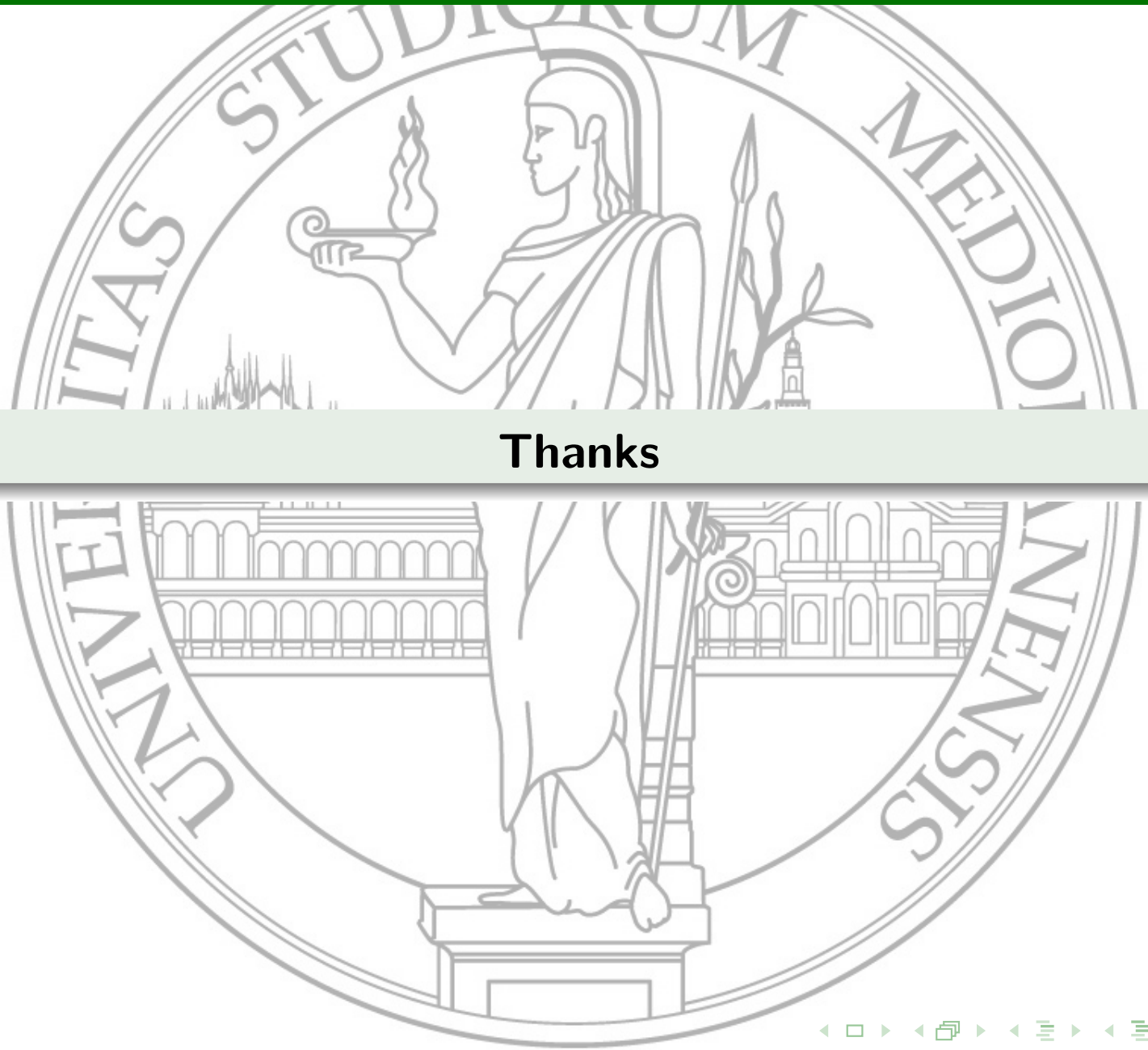
Depending of to the Richkware functions used, some security systems, that they use **applications behavior analysis**, they could mark your application as malware.

Future developments

Possible future developments

- creating a **smart main** that applies artificial intelligence concepts, such as hiding itself by antivirus and it takes decisions based on the external situation.
- extend the library with **new features**, such as creating a ransomware.

End



Thanks