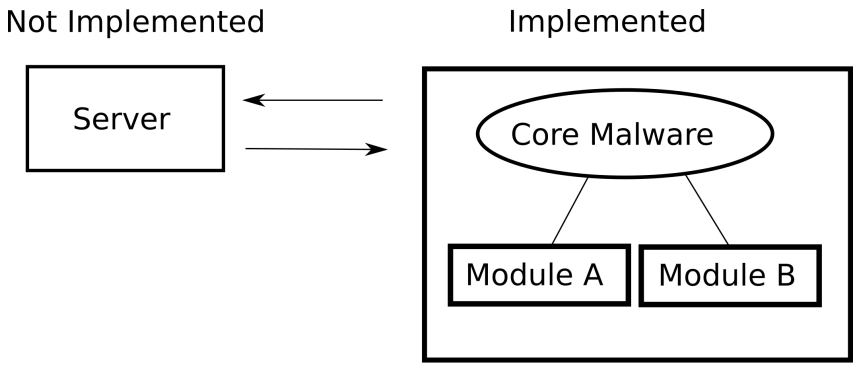
Malware Project

Rafsun Islam, Jeremias Eppler

DSU

April 28, 2015

Basic Idea



- basic idea: Malware is modularized
- server-agent principle
- server controls agent (Core Malware)
- agent executes server commands
  - start/stop modules
  - download new modules
  - uploading information

Implemented

Core Malware features:

- executes other modules (Keylogger, ReverseShell)
- parses and interprets commands
- checks for internet connection
- assign it self to to the registry

Modules:

- PSExecutor - executes PowerShell commands
- Keylogger
- Reverse Shell (reused)

Additional:

- Obfuscator
- sensless strings/functions (make analysis more difficult)