]Hacking**Team**[

RCS BlackBerry

BlackBerry

- Always connected

- Push technology

- BlackBerry Internet Service: BIS

- Enterprise solution: BES

- Information Integration

Security

- Ssl proxy through RIM servers

- Applications in java sandbox

- Signature with capabilities

- No access to kernel

- Exploit existing API

RCS BlackBerry

- Backdoor

- Stealth application

- Starts automatically

- Low power consume

- Works on any OS >= 4.5 (>85% installed)

Installation vectors

- By web

- By wap push

- By wire (*)

* Under development

Agents

- Application

- Callist

- Device information

- Messages (EMail, SMS)

- Position (Wifi,Cell,GPS)

- Mic

- AddressBook

Actions

- Sync : wifi, apn, cdma

- Uninstall

- Sms

- Agent

Events

- Timer

- AC

- Process

- StandBy

- Battery

- Call

- Position (Cell, GPS)

The End

- DEMO

- Questions?