When malwares target smartcard (eID - Belgium card ID)

@r00tbsd - Paul Rascagneres & Minilx - Julien Maladrie

malware.lu - itrust

25 October 2012

Plan

eID

Presentation of the identy card from belgium: eID.

eID

This card can be use to:

- signs documents
- pays the taxe online
- makes birth declaration
- complains to the police
- ...

More generally this card is used to sign or authenticate user.

Examples of malware

We already identified malwares that target smartcard.
For example ESET made a presentation called "Smartcard vulnerabilities in modern banking malware."
These malwares use the smart card API provides by Windows to access to the card.
We decided to develop a proof of concept with a new approach: share the USB device with the C&C.

POC

Our poc uses a driver to make USB over TCP/IP.
With this driver we are able to share in "raw" the USB device to the C&C.
The attacker can use the legitime middleware provides by the manufacturer of the samrtcard.

POC

With our poc, the attacker is able to use remotely the smartcard as it is connected.
To have the PIN code, we simply add a keylogger.

DEMO

DEMO