DIAMONDS

Development and Industrial Application of Multi-Domain Security Testing Technologies

itrust consulting

Smartcards

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

© DIAMONDS Consortium 2010-2013

Case Study Characterisation

Smartcards are typically used to provide authentication, identification, and data storage. They are frequently used in banking as well as national ID cards.

A Proof of Concept (PoC) malware was developed by itrust consulting in order to demonstrate that smartcards can be attacked. The goal of the PoC is to steal the card's PIN code and remotely use that card to digitally sign a document within Microsoft Word.

© DIAMONDS Consortium 2010-2013

Smart Card Case itrust

Case study characterization

The device used for the tests were the Gemalto USB shell token V2 and the Belgian national eID. We developed on a Windows XP SP3 machine and we used Microsoft Office 2010.

The Belgian national eID is a smartcard which has the following wide range of uses:

- Identify the owner of the card
- Tax payment online
- File lawsuits online
- Sell, buy or auction real estate

BELGIË BELGIQUE BELGIEN BELGIUM

IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD

Naam / *Name* Van Der Velden

Voornamen / *Given names* Greet Hilde

Geboorteplaats en -datum / *Place and date of birth* Borsbeek 01 FEB 1985

Geslacht / *Sex* V

Nationaliteit / *Nationality* Belg

Kaartnr. / *Card No* 000-5903301-01

Geldig van - tot / *Valid from - until* 01.01.2004 - 01.01.2009

Handtekening van de houder / *Holder's signature*

© DIAMONDS Consortium 2010-2013

Smart Card Case itrust

Case study characterization

Security challenges:

To identify the weaknesses of smartcards. Many companies and countries are now using smartcards without estimating the potential security dangers.

Technical challenges:

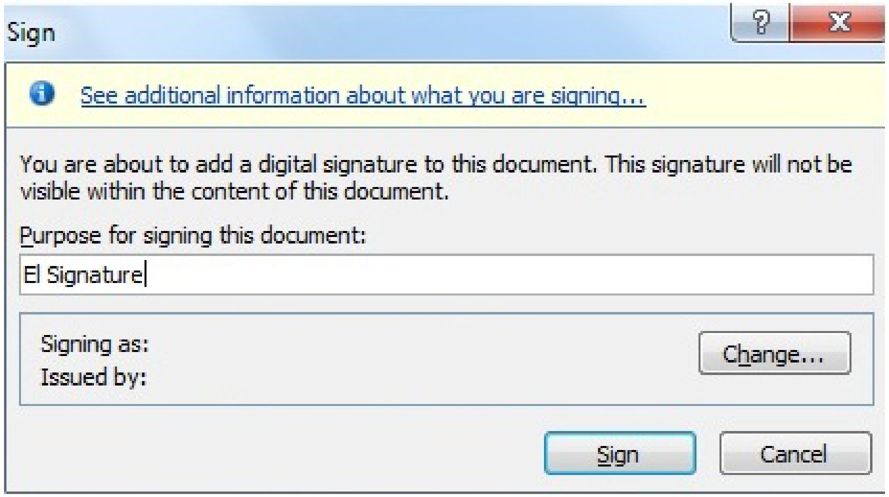
The main technical challenge was to develop a driver which could be used to share USB data.

© DIAMONDS Consortium 2010-2013

Smart Card Case itrust

Security testing appraoches

Once launched, the malware stays in an idle state until the signing dialog box appears within Microsoft Office. Once the dialog box has been detected, the malware injects code within the process and records the keystrokes in order to steal the PIN code. Once the PIN code has been recorded, it is sent through a HTTP channel to the C&C (Command & Control) server.



See additional information about what you are signing...

You are about to add a digital signature to this document. This signature will not be visible within the content of this document.

Purpose for signing this document:

El Signature

Signing as:

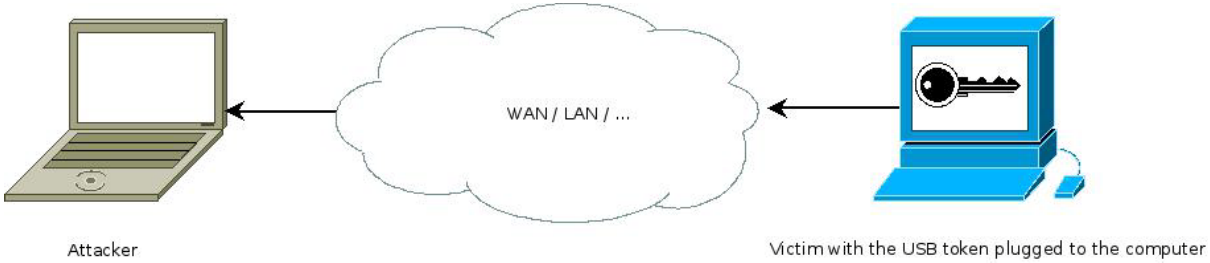
Issued by:

© DIAMONDS Consortium 2010-2013

Smart Card Case itrust

Security testing appraoches

A driver enabling us to transport USB over TCP is installed on the victim's machine (it can be installed using a remote access tool).



When the victim's USB token is plugged into their machine, we are able to remotely use the device as if it were plugged into our machine. Whilst the attacker is using the device, the user won't be able to access it. If the device has an embedded activity LED it will be visible while the attacker is using it and the victim may notice it.

© DIAMONDS Consortium 2010-2013

Smart Card Case itrust

Results and recommendations

Results:

itrust were able to develop a perfectly working sample of malware and successfully add a digital signature to the Microsoft Word document on the target computer.

Reccomendations:

We recommend to never keep the smartcard connected while it is not in use. We also recommend that smartcard providers add additional security controls e.g. the latency of a network connection is different to a USB connection. A firmware could be developed to calculate the latency and if it is too long the smartcard would be blocked.

© DIAMONDS Consortium 2010-2013

Smart Card Case itrust

Exploitaiton

The malware has been presented at two IT security conferences (Hack.lu - Luxembourg and Malcon – India). This malware has been widely presented through prestigious IT news websites such as theregister.co.uk and SC magazine.

- http://www.net-security.org/dl/insecure/INSECURE-Mag-36.pdf
- http://thehackernews.com/2012/10/new-windows-malware-can-target-smart.html#_
- http://www.computerworld.com/s/article/9233697/Proof_of_concept_malware_can_share_USB_smart_card_readers_with_attackers_over_Internet
- http://www.scmagazine.com.au/News/322969,malware-funnels-smartcard-pins-to-remote-servers.aspx
- http://archive.hack.lu/2012/when_malwares_target_smartcard_eID.pdf
- http://www.malcon.org/research/2012/05%20Paul%20Rascagneres%20-%20Smartcard.pdf
- http://threatpost.com/en_us/blogs/researchers-remotely-control-smart-cards-malware-poc-112012

© DIAMONDS Consortium 2010-2013