Returning trust against the user

Jonathan Dechaux,
Jean-Paul Fizaine

May 8, 2010

1 Presentation

2 Introduction

3 Review on Openoffice
- General aspect on the format
- Configuration file
- Trusted macro

4 Attack scheme & Demonstration
- Description of the attack
- Where are the difficulties ?
- Demonstration

5 Conclusion

How we are ?

- Jonathan Dechaux, fourth year at ESIEA (dechaux@et.esiea-ouest.fr)
- Jean-Paul Fizaine, fourth year at ESIEA (fizaine@esiea-recherche.eu)

What do we first need to know

- Office document as main vector of attack.
- $k-$ary code.

Definition (k-ary code)

Attack that is performed by a cooperation of k malicious codes, dependently or indepedently.

Problems

How can we bypass securities settings of macro and how can we gain the trust of our victim?

Definition (Solution)

We are going to use Openoffice format as a vector of infection. And use a binary that will adapt Openoffice settings to enable our macro to execute.

Quick description of the Openoffice format

Definition (Openoffice format)

- It is a archive format,
- contain directory and file,
- describes by the **META-INF/Manifest.xml**

Definition (Macro's location)

Macro or either on the host, they are them embedded in the application. Or them are within the document. By default, the execution of macro is deactivated.

Where are the configuration files ?

- It is the same organization and the same files on each operating system.
- When there are no personal configuration, Openoffice takes it default setting. Otherwise a file on the user root directory is updated.
- Setting files of Openffice are **not protected** at all !!!

What it is ? Where are they?

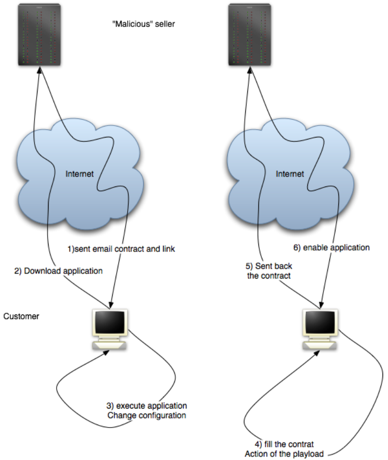
Definition (Trusted macro)

Trusted macro, is a concept that permits some macros to be executed in the a totally with trusted of the user.

They can be every way, embedded in the document, or on the host.

- Customer by our software and fill up a form.
- Download the software.
- He receive by email the agreement in Openoffice document, that is numericaly signed by the seller.
- He must first launch the application that gives a code he must sent back to activate the software.
- He must sent back the agreement with the previous number that must be numericaly signed.
- Now it can use his software.

Description of the attack



The Website

- It is the first step of the attack, and the the fist contact with the victim.
- It is a website that sales for example security software.
- We need the faith of the customer, and make him by our software.

Email & The infected contract

- It is an Openoffice document that contains a malicious macro.
- It goal is to perform the final attack from the document.

The malicious application

- It must first modify the Openffice settings, to enable the execution of our macro.
- After it can perform his own attack.
- At this point we have a binary attack which can be used has the attacker wants on depending his goal.

Not so difficult as we can imagine

- Bypassing security in Openoffice...

Definition

A stage attack that where the first code has the objective to modify the configuration file.

- How to you acquire user's faith ?

Definition

- By using cryptography,
- agreement, procedure...

Demonstration

Let’s rock ! ;)

- Office document is the central part of the attack.
- We manage to introduce three malwares instead of only **ONE !!!**
- The attack can be extended to k malwares, on depending the goal.
- Out attack uses results that was publish last year at **Black Hat Europe 09** ...
- The Antivirus community do not make any security survey.

Take you for you attention.
Do you have any questions ?