



# ***Analyse du risque viral sous OpenOffice.org 2.0.x Les virus OOv\_x***

E. Filiol

`efiliol@esat.terre.defense.gouv.fr`

Laboratoire de virologie et de cryptologie  
Ecole Supérieure et d'Application des Transmissions



# ***Introduction***



# *Introduction*

- ⑥ Concurrent « officiel » de Microsoft Office.

# ***Introduction***

- ⑥ Concurrent « officiel » de Microsoft Office.
- ⑥ Parts de marché en progression constante.

# *Introduction*

- ⑥ Concurrent « officiel » de Microsoft Office.
- ⑥ Parts de marché en progression constante.
- ⑥ Coût direct négligeable mais ...

# Introduction

- ⑥ Concurrent « officiel » de Microsoft Office.
- ⑥ Parts de marché en progression constante.
- ⑥ Coût direct négligeable mais ...
- ⑥ Quid de la sécurité réelle d'OpenOffice ?

# Introduction

- ⑥ Concurrent « officiel » de Microsoft Office.
- ⑥ Parts de marché en progression constante.
- ⑥ Coût direct négligeable mais ...
- ⑥ Quid de la sécurité réelle d'OpenOffice ?
- ⑥ Analyse du risque viral et validation par codes *proof-of-concept*.

# *Analyse du risque*



# *Analyse du risque*



- ⑥ Existence de nombreux langages de programmation intégrés : script shell, VBScript, Python, Perl, Asp, Java.
- ⑥ Très grande richesse de développement des macros.
- ⑥ Existence de nombreux points d'exécution détournables.

# *Analyse du risque*



- ⑥ Pas de mécanismes de protection prévus pour les macros.
- ⑥ Le format type ZIP offre une grande facilité de pénétration virale.

# *Analyse de risque (2)*



## Analyse de risque (2)

- ⑥ La sécurité des macros est très facilement contournable. Des répertoires dits « de confiance » sont définis. Toute macro placée dans ces répertoires est *ipso facto* de confiance.
- ⑥ La signature du document ne prend pas en compte réellement les macros. Possibilités de contournement.

## *Analyse de risque (2)*

- ⑥ Les macros peuvent être liées à des événements ou des services.
- ⑥ Autres mécanismes : chaînage de macros, utilisation de liens hypertexte, exécution inter applications, utilisation de lien OLE...
- ⑥ De très nombreux mécanismes sont utilisables par une infection.

## *Analyse de risque (2)*

- ⑥ Toutes les techniques virales connues pour Microsoft Office sont transposables sous OpenOffice.org.
- ⑥ Tous les types d'infections informatiques sont réalisables (infections simples et auto-reproductrices).

## *Analyse de risque (2)*

- ⑥ Globalement, la suite OpenOffice représente un risque plus grand en terme d'infections que la suite Microsoft.
- ⑥ Absence de véritables concepts de sécurité.

# Les virus OOv\_s1, OOv\_s1\_f, OOv\_s2...



# Les virus OOv\_s1, OOv\_s1\_f, OOv\_s2...



- ⑥ Réalisation de plusieurs souches virales opérationnelles comme *preuve de concept*.
- ⑥ Infection couronnée de succès quel que soit le niveau de sécurité choisi par l'utilisateur.
- ⑥ Certains scénarii permettent d'agir sans alerter l'utilisateur d'une quelconque manière.

# *L'infection* 00v\_s1\_f



# *L'infection OOv\_s1\_f*



- ⑥ Envoi d'un mail avec pièce jointe (document OpenOffice.org).
- ⑥ A l'ouverture, la macro associée à cet événement est exécutée (phase de primo-infection).
- ⑥ Installation d'une fonction offensive  $\mathcal{C}$  dans la macro *DicOOo*.
- ⑥ La fonction  $\mathcal{C}$  est exécutée à l'installation de *DicOOo*.

# ***Conclusion***



# Conclusion

- ⑥ Nombreuses possibilités identifiées et testées.
- ⑥ Le risque infectieux sous OpenOffice est actuellement maximal.
- ⑥ OpenOffice est à déconseiller d'un point de vue de la sécurité.

# Conclusion

- ⑥ Article long à paraître prochainement :
  - △ D. de Drézigué, J.- P. Fizaine, N. Hansma, *In-depth Analysis of the Viral Threats with OpenOffice.org Documents*, Journal in Computer Virology, 2006.