

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







6 Concurrent « officiel » de Microsoft Office.



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



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



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

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

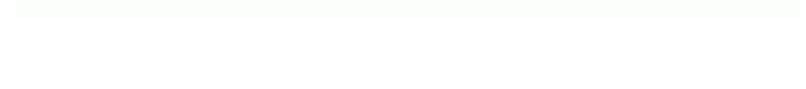


- Existence de nombreux langages de programmation intégrés : script shell, VBScript, Python, Perl, Asp, Java.
- Très grande richesse de développement des macros.
- Existence de nombreux points d'exécution détournables.

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.



- 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.

Les macros peuvent être liées à des événements ou

des services.

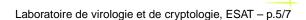
- 6 Autres mécanismes : chaînage de macros, utilisation de liens hypertexte, exécution inter applications, utilisation de lien OLE...
- Oe très nombreux mécanismes sont utilisables par une infection.

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



- 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*.
- Infection couronnée de succès quel que soit le niveau de sécurité choisi par l'utilisateur.
- 6 Certains séenarii permettent d'agir sans alerter l'utilisateur d'une quelconque manière.

L'infection OOv_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).
- Installation d'une fonction offensive \mathcal{C} dans la macro DicOOo.
- 6 La fonction C est exécutée à l'installation de *DicOO*o.

Conclusion



Conclusion



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

Conclusion



- 6 Article long à paraitre 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.