Analyse de l'antivirus OneCare

E. Filiol – P. Evrard – G. Geffart – F. Guilleminot - G. Jacob – S. Josse – D. Quenez

ESAT - Laboratoire de virologie et de cryptologie

Disclaimer

- Il s'agit de résultats de recherche et non de la position officielle du ministère de la défense !
- Cette étude n'a pas pour but de descendre un produit mais d'évaluer de manière rationnelle, indépendante et reproductible sa sécurité réelle comme pour n'importe quel autre produit.

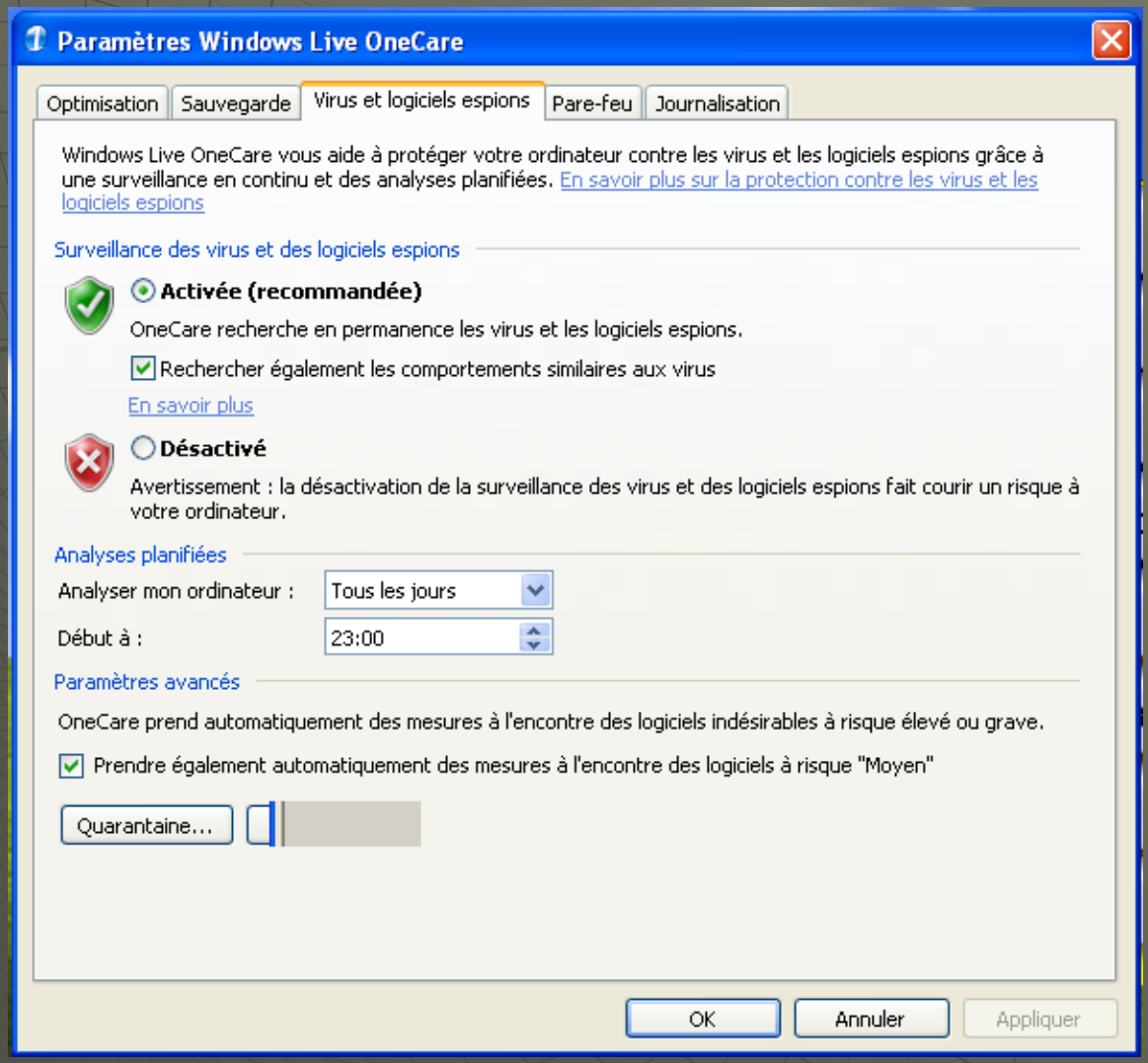
Plan

- Installation et paramétrage.
- Analyse de forme.
- Analyse comportementale.
- Conclusion.

Installation et paramétrage

- Obligation d'être connecté à Internet pour installer et activer le produit.
  - Solution inadaptée aux réseaux et systèmes devant rester cloisonnés.
- Paramétrage réduit à sa plus simple expression.
  - Impossible d'adapter à une politique locale de sécurité antivirale.

Installation et paramétrage (2)



Analyse de forme

- Sur un CDROM de 89 584 malware

OneCare	26 291	29,35 %
KAV	89 584	100 %
Norton	25 593	28,57 %

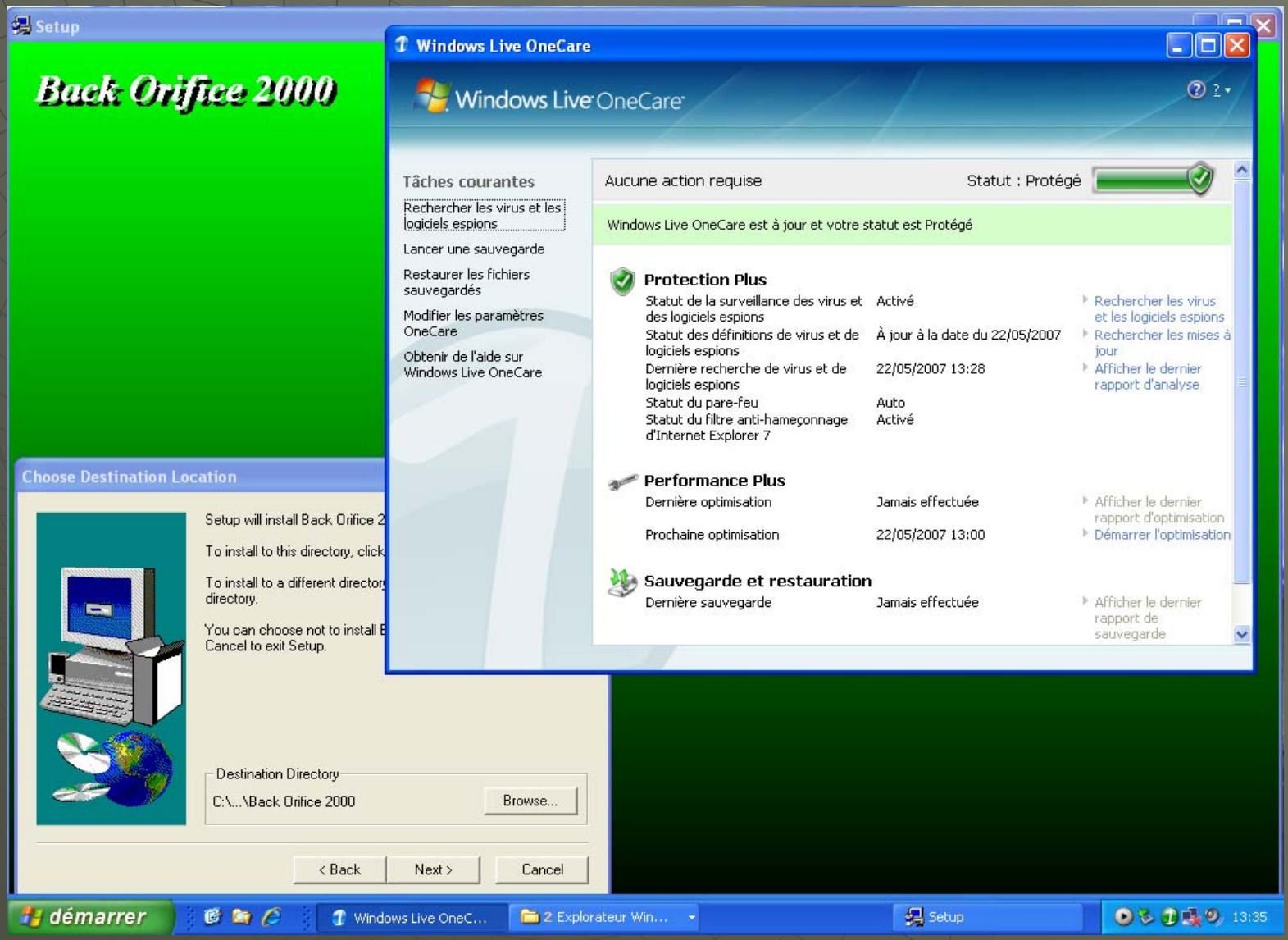
Analyse de forme (2)

- Extraction de schémas de détection
  - Schémas faibles (motifs courts et fonctions de détection triviales).
- Echec aux tests de
  - API Hook.
  - Détection de Rootkits.
  - Bad cluster NTFS.
  - Test analyse mémoire et détection Buf. Over.
  - Techniques EPO simples.
  - ...

Analyse comportementale

- Echec au test du keylogger.
- Echec aux tests de polymorphisme fonctionnel.
  - Pas de détection comportementale.
- Exécution sans alerte de codes malveillants connus.

Analyse comportementale (2)



Conclusion

- OneCare est très en retard sur ses concurrents du Top 10.
- Produit pas assez mature.
- Le produit néglige que

Lutte antivirale = politique de sécurité + antivirus.

- Quid de la version 2.0 ?
- Résultats techniques détaillés dans MISC de juillet 2007.

Conclusion (2)

- Arno Edelmann (Responsable produit sécurité produit en Europe):

« *OneCare est un nouveau produit. Ils n'auraient pas dû le sortir quand ils l'ont fait mais ils règlent les problèmes maintenant [...] Microsoft n'est pas une société de sécurité. La sécurité est importante mais ne représente qu'une petite partie de Microsoft.* »