Sécurité des claviers virtuels

Rump Session

SSTIC 2005

Nicolas Gregoire - nicob@nicob.net

Introduction

- Utilisé pour la banque en ligne
- Déploiement (relativement) récent en France
- Censé être sûr contre les key-loggers
- Fortes différences d'implémentation

Nicolas Gregoire - nicob@nicob.net

Contexte

- Simple PoC
- N'inclut aucune fonctionnalité « black hat »
  - Détection automatique du site bancaire
  - Administration distante
  - Remontée des infos (direct / différé / compressé / ...)
  - OCR
  - Furtivité
- Tests réalisés sur des « copies locales »
  - « Volées » sur un site de pishing

Technique

- Hook de la souris
  - WM_LBUTTONDOWN
  - Ni DLL, ni driver, via compte non privilégié
- Indépendant de la techno Web sous-jacente
  - Flash
  - DHTML
- Première version fonctionelle
  - 1h30 d'écriture
  - 220 lignes (dont 80 pour les bitmaps)
  - 8 ko non compressé (14 ko pour version de démo)

Démo

Une démo, une démo !

Nicolas Gregoire - nicob@nicob.net

Solutions ?

Il n'y en a pas !

- Idées pour « compliquer » la récupération
  - Mouse Gestures
  - Clavier clignotant ;-)
  - Overlay à la WMP
- Solution extrême côté attaquant
  - Vidéo plein écran de la session
- Vu comme un facteur de différentiation