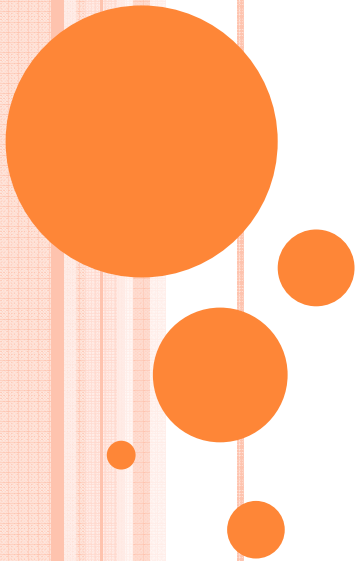

Sécurité sous Windows Mobile 6

Par Cédric HALBRONN

Contact : saidelike+sstic@gmail.com

Plan

- Téléphones actuels
- Windows Mobile 6
- Scénario SD-Card
- Scénario Rootkit
- Conclusion

Plan

- Téléphones actuels
- Windows Mobile 6
- Scénario SD-Card
- Scénario Rootkit
- Conclusion

HTC TyTN II


htc
Start
Service Provider
6/15/07
11:00
Weekly Meeting
2:30PM-5:00PM
Dinner
6:30PM-7:30PM
Notification
Contacts

Plan

- Téléphones actuels
- Windows Mobile 6
- Scénario SD-Card
- Scénario Rootkit
- Conclusion

Modèle de sécurité

- Il est tout à fait possible d'avoir une application « unsigned » qui s'exécute en « trusted » mode.

Plan

- Téléphones actuels
- Windows Mobile 6
- Scénario SD-Card
- Scénario Rootkit
- Conclusion

CONTEXTE

- Un « ami » souhaite vous montrer un nouveau jeu qu'il a découvert
- Il vous prête sa SD-Card.
  - Autorun.exe → « prompt » à l'utillisateur /!\
  - Installation en arrière plan de tout ce qu'il faut…
  - Exécution normale du jeu !

Démo

DÉTAILS

- Que s'est-il passé ?
  - Game.exe, InterceptSMS.dll
    - Signées avec un certificat
  - Autorun.exe
    - N'a nécessité aucune action de la part de l'utilisateur
    - Non signée → confirmation demandée à l'utilisateur /!\
    - Une fois confirmée, tout est possible (« privileged mode »)
      - Installation de notre certificat
      - Copie de notre DLL d'interception SMS
      - Enregistrement de la DLL dans la base de registre
    - Exécution normale du jeu
  - La DLL d'interception SMS sera exécutée par tmail.exe pour chaque SMS reçu et notre filtre d'interception permet d'exécuter les commandes souhaitées en arrière plan…

Plan

- Téléphones actuels
- Windows Mobile 6
- Scénario SD-Card
- Scénario Rootkit
- Conclusion

CONTEXTE

- APIs Windows CE ~ Windows PC
- Format PE, DLLs ~ Windows PC
- Coredll.dll ~ System32.dll
- Prefetch Abort Traps ~ appels systèmes
- Tout est là pour permettre des techniques de rootkit « similaires » au monde Windows PC

Démo

Détails

- Manque de temps, une autre fois, désolé ;-)

Plan

- Téléphones actuels
- Windows Mobile 6
- Scénario SD-Card
- Scénario Rootkit
- Conclusion

Conclusion

- Les téléphones n'ont pas autant de capacités que les PCs pour devenir de vraies cibles d'attaques
- Ils ont plus…
  - Bluetooth,
  - SMS,
  - GPS,
  - Tout ce qui vous est cher est sur vous…

Merci pour votre attention.

RESSOURCES

- Windows Mobile 5.0 Application Security - http://msdn.microsoft.com/en-us/library/ms839681.aspx
- Adding Certificates to the Privileged, Unprivileged, and SPC Stores Example - http://msdn.microsoft.com/en-us/library/bb737306.aspx
- Exemples de certificats - Windows Mobile 6 SDK\Tools\Security\SDK Development Certificates
- Configuration d'un téléphone WM6 - Mobile 6 SDK\Tools\Security\Security Powertoy
- Virtual CE - http://www.bitbanksoftware.com/VirtualCE.html
- Sample MapiRule - http://msdn.microsoft.com/en-us/library/bb158685.aspx
- Subverting Windows CE Kernel for fun and profit, Petr Matousek - http://www.fnop.org/