

# La sécurité des smartphones

Romain Raboin - ATLAB

04 Juin 2009



# Sommaire

- ▶ Les smartphones
- ▶ Différents OS
- ▶ Windows Mobile
  - ▶ Logiciels malicieux
  - ▶ Logiciels espions
  - ▶ Méthodes d'infection
- ▶ Étude d'un spyware
- ▶ Attaques depuis un smartphone
- ▶ Conclusion

# Introduction

- ▶ Les smartphones
  - ▶ Un téléphone mobile couplé à un PDA
- ▶ Marché mondial en forte croissance
- ▶ Nombreux moyens de communication
  - ▶ Wi-Fi, Bluetooth, média amovible, ...
- ▶ Risques liés aux usages nomades
  - ▶ Perte, vol, géolocalisation, ...

# Les smartphones

## Différents OS

- ▶ Répartition par OS des ventes dans le monde fin 2008 (Gartner)
  - ▶ Symbian OS : 49.8%
  - ▶ RIM Blackberry OS : 15.9%
  - ▶ iPhone OS : 12.9%
  - ▶ Windows Mobile : 11.1%
  - ▶ Autres : 10.3%

# Les smartphones

## Symbian OS

- ▶ Système de signature depuis Symbian OS 9
- ▶ Fonctions privilégiées
- ▶ Nombreux logiciels malicieux
- ▶ Logiciels espions commerciaux
  - ▶ Signature officielle
- ▶ Présentation :
  - ▶ Symbian Exploitation and Shellcode Development

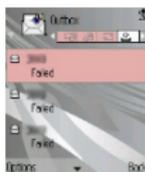
## Vecteur de fraude

### New mobile malware silently transfers account credit

Posted by Dancho Danchev @ 2:39 pm

**Categories:** [Anti Virus](#), [Hackers](#), [Malware](#), [Mobile \(In\)Security](#)

**Tags:** [Security](#), [Symbian](#), [Mobile Malware](#), [SMS Python Flocker](#), [Fraud](#), [Indonesia](#), [Dancho Danchev](#)



Kaspersky Lab today warned users of five newly found variants of the Trojan-SMS.Python.Flocker mobile malware, targeting an Indonesian mobile provider's service allowing users to transfer money or minutes to each other's accounts. SMS Python Flocker is a known mobile malware family, whose previous versions used to automatically send SMS message from the infected mobile device to premium-rate numbers operated by the malware authors.

<http://blogs.zdnet.com/security/?p=2415>

# Les smartphones

## iPhone OS

- ▶ Séparation des droits
- ▶ Système de signature
- ▶ Peu de logiciels malicieux
- ▶ Logiciel espion commercial
  - ▶ *Jailbreak*
- ▶ Vulnérabilités publiques (CVE-2006-3459)

# Les smartphones

The screenshot displays the Metasploit framework interface. The main window shows search results for the term 'iphone' under the 'Available Exploits (0)' tab. Three exploits are listed, all titled 'iPhone MobileMail LibTIFF Buffer Overflow', 'iPhone MobileSafari LibTIFF Buffer Overflow', and 'iPhone MobileSafari LibTIFF Buffer Overflow'. Each exploit description states: 'This module exploits a buffer overflow in the version of libtiff shipped with firmware versions 1.0.0, 1.0.1, 1.0.2, and 1.1.1 of the Apple iPhone. iPhones which have not had the BSD tools installed will need to use a special payload.'

The 'Available Payloads (1)' tab is also visible, showing search results for 'iphone'. It lists three payloads: 'OSX iPhone Vibrate', 'OSX iPhone Vibrate, Bind TCP Stager', and 'OSX iPhone Vibrate, Reverse TCP Stager'. Each payload description includes details about its functionality and dependencies, such as 'Causes the iPhone to vibrate, only works when the AudioToolKit library has been loaded. Based on work by Charlie Miller.'

A large, stylized watermark 'metasploit' is overlaid on the center of the screenshot.

# Les smartphones

## RIM Blackberry OS

- ▶ Peu de logiciels malicieux
- ▶ Présentations
  - ▶ Blackjacking, Owning the Enterprise via Blackberry
  - ▶ RedBerry, Advanced Attacks via a Trojaned blackberry
- ▶ Logiciel espion commercial

# Windows Mobile

- ▶ Windows CE : Version de Windows pour les systèmes embarqués et autres systèmes minimalistes
- ▶ Windows Mobile 5.0 lancé en 2005, conçu sur Windows CE 5.1
- ▶ Windows Mobile 6.0 lancé en 2007, conçu sur Windows CE 5.2
- ▶ Signature binaire ou installeur cabinet (.cab), alerte seulement
- ▶ Sécurité faible :
  - ▶ Auto-exécution via média amovible
  - ▶ Pas de séparation des privilèges
  - ▶ Faiblesse dans la synchronisation

# Windows Mobile

## Logiciels malicieux

- ▶ Exemples :
  - ▶ Trojan WinCE/Bradord.a
  - ▶ Virus.WinCE.Duts.a
  - ▶ Trojan WinCE/Infojack
  - ▶ Rootkit Kernel
- ▶ Logiciels espions commerciaux

## Logiciel Espion

- ▶ Installation via un fichier *cab*
- ▶ Copie de fichiers dans `\Windows\VPhoneServices`, modification de la base de registre, installation d'un service
- ▶ Nécessite de redémarrer en raison du service
- ▶ Code pour accéder à l'interface de configuration
- ▶ Non visible dans l'interface *Ajout/Suppression de programmes*
- ▶ *Uninstall* dans la configuration puis *Uninstall Windows*

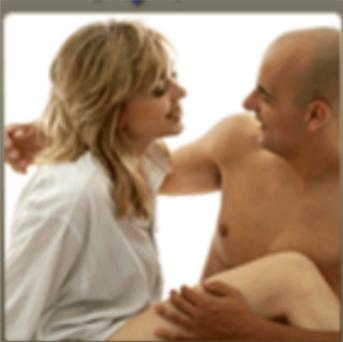
# Logiciel Espion

## Fonctionnalités :

- ▶ Interception d'appels
- ▶ Déclenchement du micro à distance
- ▶ Avertissement de changement de carte SIM
- ▶ Surveillance via GPS
- ▶ Vol de SMS, e-mails, MMS, historique d'appels, etc.
- ▶ Configuration à distance par SMS

# Logiciel Espion

## Espionnez votre femme grâce à FlexiSPY !



**This Could Be You!**

**I Knew It . . .**

Thanks to FlexiSPY I finally figured out my wife was cheating on me with my brother. I had a bad feeling about this for over a year. After the divorce, my life is so much better now.

Thanks FlexiSPY, I'm free again - Divorced

<b>FLEXISPY - PRO</b> 		
<b>PRO</b>	<a href="#">FULL DETAILS</a>	<a href="#">Supported Phones</a>
<b>MID RANGE SPYPHONE</b>		
<ul style="list-style-type: none"><li>❑ Spyphone to bug a room or person</li><li>❑ Read their SMS, EMAIL and Call Logs</li><li>❑ BUY NOW for Instant Download</li><li>❑ Change phones as often as you like</li><li>❑ Symbian, Windows and Blackberry</li></ul>		
<b>ORDER NOW: €150</b> (per year)		

# Logiciel Espion

All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help
ALL EVENTS 1 - 5 of 5 records									
Row Per Page 10									
#	Type	Direction	Duration	Contact Name	Mobile Time	Server Time			
1	E-MAIL	📧		Romain RB. RABOIN	04/11/08 10:17:11	04/11/08 09:18:15			
2	E-MAIL	📧		Romain RB. RABOIN	04/11/08 10:10:33	04/11/08 09:11:11			
3	VOICE	📞	0:00:00	*#900900900	04/11/08 09:49:31	04/11/08 08:49:04			
4	E-MAIL	📧		Romain RB. RABOIN	03/11/08 18:11:19	03/11/08 17:11:34			
5	VOICE	📞	0:00:00	2223366589	03/11/08 18:07:07	03/11/08 17:06:32			
<a href="#">Delete</a> <a href="#">Refresh</a> <a href="#">Report Settings</a>									
First   Previous   1   Next   Last									

All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help
Log Detail									
# 1									
IMEI: ██████████									
Client Time: 04/11/08 10:17:11									
Server Time: 04/11/08 09:18:15									
Event Type: MAIL									
Direction: IN									
Size: 0 Bytes									
Sender Email: "Romain RB. RABOIN" <raboind@atlab.fr>									
Contact Name: Romain RB. RABOIN									
Subject: atlab test2									
Contents:									
<a href="#">Back</a> < Previous   Next >									

# Logiciel Espion

## Points forts

- ▶ Riche en fonctionnalités
- ▶ Multiplate-formes : Symbian, Blackberry, Windows Mobile, iPhone

## Points faibles

- ▶ Toutes les données sont envoyées non chiffrées sur les serveurs de l'éditeur
- ▶ Aucune utilisation d'une méthode d'infection spécifique
  - ▶ Nécessite une interaction physique avec le téléphone

# Méthodes d'infection

## *Social engineering*

- ▶ e-mails
- ▶ Bluetooth
- ▶ *Installeur* PocketPC
  - ▶ Fichier cabinet (.CAB)
  - ▶ Modification d'un installeur existant
  - ▶ Ajout d'un logiciel malveillant

## Méthodes d'infection

- ▶ Auto-exécution via media amovible
  - ▶ \Carte de stockage\type-de-processeur\autorun.exe
  - ▶ \windows\Carte de stockage\autorun.exe
- ▶ Bluetooth et OBEX FTP
  - ▶ *Directory traversal - Bugtraq ID: 33359*
  - ▶ \Mes documents\Partage Bluetooth
  - ▶ Exécution de logiciels malicieux et vol d'informations

# Méthodes d'infection

- ▶ Exploitation de vulnérabilités sur des outils natifs à Windows Mobile
  - ▶ Buffer overflow Outlook (<http://www.mulliner.org/pocketpc/>)
  - ▶ Microsoft Windows Mobile Overly Long Bluetooth Device Name Denial of Service Vulnerability - *Bugtraq ID: 31420*

# ActiveSync

- ▶ ActiveSync : logiciel de communication entre Windows Mobile et le poste de travail
- ▶ Installé sur tous les postes pour la synchronisation
- ▶ RAPI : API puissante pour utiliser le canal de communication (<http://msdn.microsoft.com/en-us/library/aa457105.aspx>)

# RAPI

## Version de Windows Mobile

- ▶ Différenciation WM5, WM6, etc.
- ▶ CeGetVersionEx()

## Lecture / écriture de fichiers

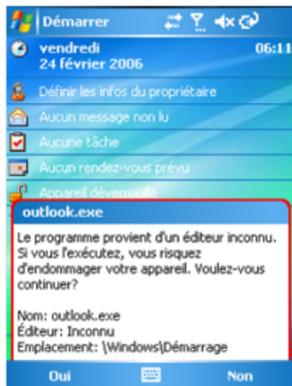
- ▶ Copie de la backdoor
- ▶ CeWriteFile(), CeReadFile()

## Création de processus

- ▶ On exécute la backdoor
- ▶ CeCreateProcess()

## RAPI

- ▶ Demande de confirmation par défaut
- ▶ Configuration des *policies* dans la base de registre
- ▶ Modification de la base de registre impossible
- ▶ Utilisation de rapiconfig.exe pour modifier les *policies*
- ▶ Fonction non documentée **CeRapiConfig()**



# RAPI

## Policies

- ▶ Règles permettant de limiter l'accès à certaines fonctions de la RAPI
  - ▶ *Closed mode* : Accès via RAPI interdit
  - ▶ *Restricted mode* : Fonctions privilégiées interdites
  - ▶ *Open mode* : Aucune restriction

## Policy ID

- ▶ Unsigned Prompt Policy, ID: 4122
- ▶ Unsigned Applications Policy, ID: 4102

# RAPI

Exemple d'un fichier de *polices* :

```
<wap-provisioningdoc>  
  <characteristic type="SecurityPolicy">  
    <parm name="4097" value="1" />  
    <parm name="4102" value="1" />  
    <parm name="4122" value="1" />  
  </characteristic>  
</wap-provisioningdoc>
```

## Création d'un logiciel malveillant

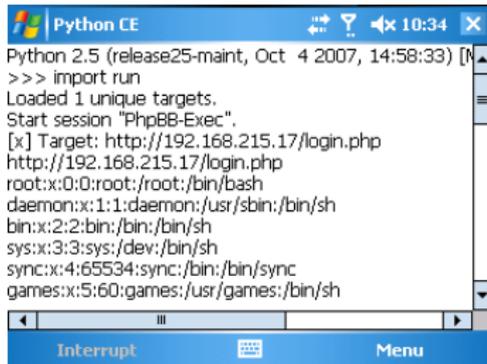
- ▶ Exemple avec l'historique des appels
- ▶ Réception des informations sur un serveur Web
- ▶ API existante :
  - ▶ PhoneOpenCallLog
  - ▶ InternetOpenA
- ▶ Envoi d'informations lors d'un accès Internet
  - ▶ via Wi-Fi
  - ▶ via GPRS
  - ▶ via ActiveSync

# Création d'un logiciel malveillant

## Démonstration

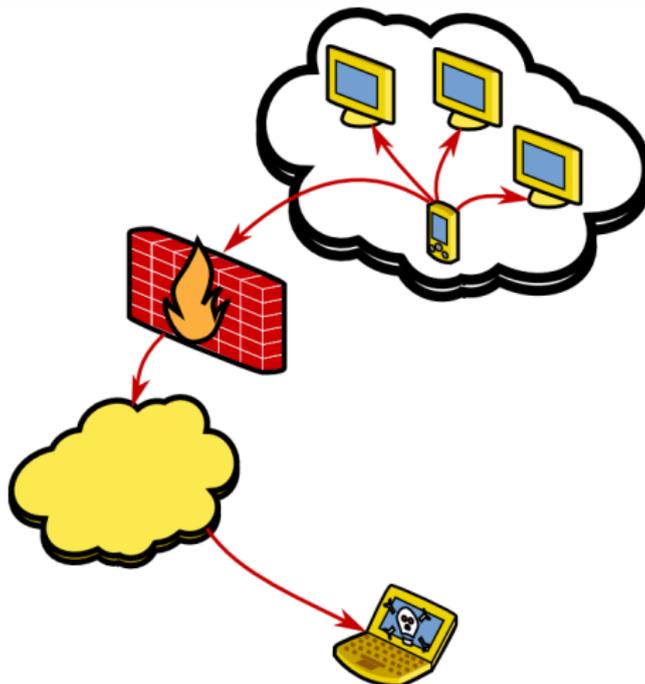
## Attaques depuis un smartphone

- ▶ Blackjacking - Owing the Enterprise via Blackberry
- ▶ Framework d'exploitation
  - ▶ Exploitation Web
  - ▶ Payloads génériques, Transformations (*LFI to exec*), ...
  - ▶ Développé en Python



```
Python CE
Python 2.5 (release25-maint, Oct 4 2007, 14:58:33) [M
>>> import run
Loaded 1 unique targets.
Start session "PhpBB-Exec".
[x] Target: http://192.168.215.17/login.php
http://192.168.215.17/login.php
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

# Attaques depuis un smartphone



## Faiblesses

- ▶ Nombreux vecteurs d'échange (y compris Micro SD, SD Cards), envoi de fichiers et exécution
- ▶ Aucune notion de privilèges
- ▶ Aucun outil "système"
- ▶ API puissantes (fonctionnalités proches des postes Windows)
- ▶ Synchronisation au bureau et/ou au domicile
- ▶ Faible sensibilisation des utilisateurs
- ▶ Plusieurs méthodes d'infection
- ▶ Facilité de vols d'informations confidentielles

## Sécuriser son smartphone

- ▶ Intégration officielle de tous les smartphones dans le SI
- ▶ Sécuriser les postes de travail
- ▶ Respecter les politiques de sécurité
- ▶ Sensibiliser tous les utilisateurs
- ▶ Gestion de parcs de téléphones mobiles
- ▶ Antivirus, pare-feux
- ▶ Chiffrement
  - ▶ Utimaco SafeGuard PDA
  - ▶ Check Point Mobile Encryption
  - ▶ FreeOTFE

## Questions

- ▶ Merci de votre attention
- ▶ Contacts :
  - ▶ Romain Raboin : [rraboin@atlab.fr](mailto:rraboin@atlab.fr)
  - ▶ [www.atlab.fr](http://www.atlab.fr)
  - ▶ [www.lasecuriteoffensive.fr](http://www.lasecuriteoffensive.fr)