La sécurité des smartphones

Romain Raboin - ATLAB

04 Juin 2009

atlab
La Sécurité Offensive

Sommaire

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

atlab
La Sécurité Offensive

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, ...

atlab
La Sécurité Offensive

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%

atlab
La Sécurité Offensive

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

atlab
La Sécurité Offensive

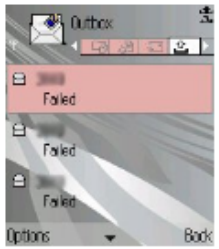
Vecteur de fraude

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

atlab
La Sécurité Offensive

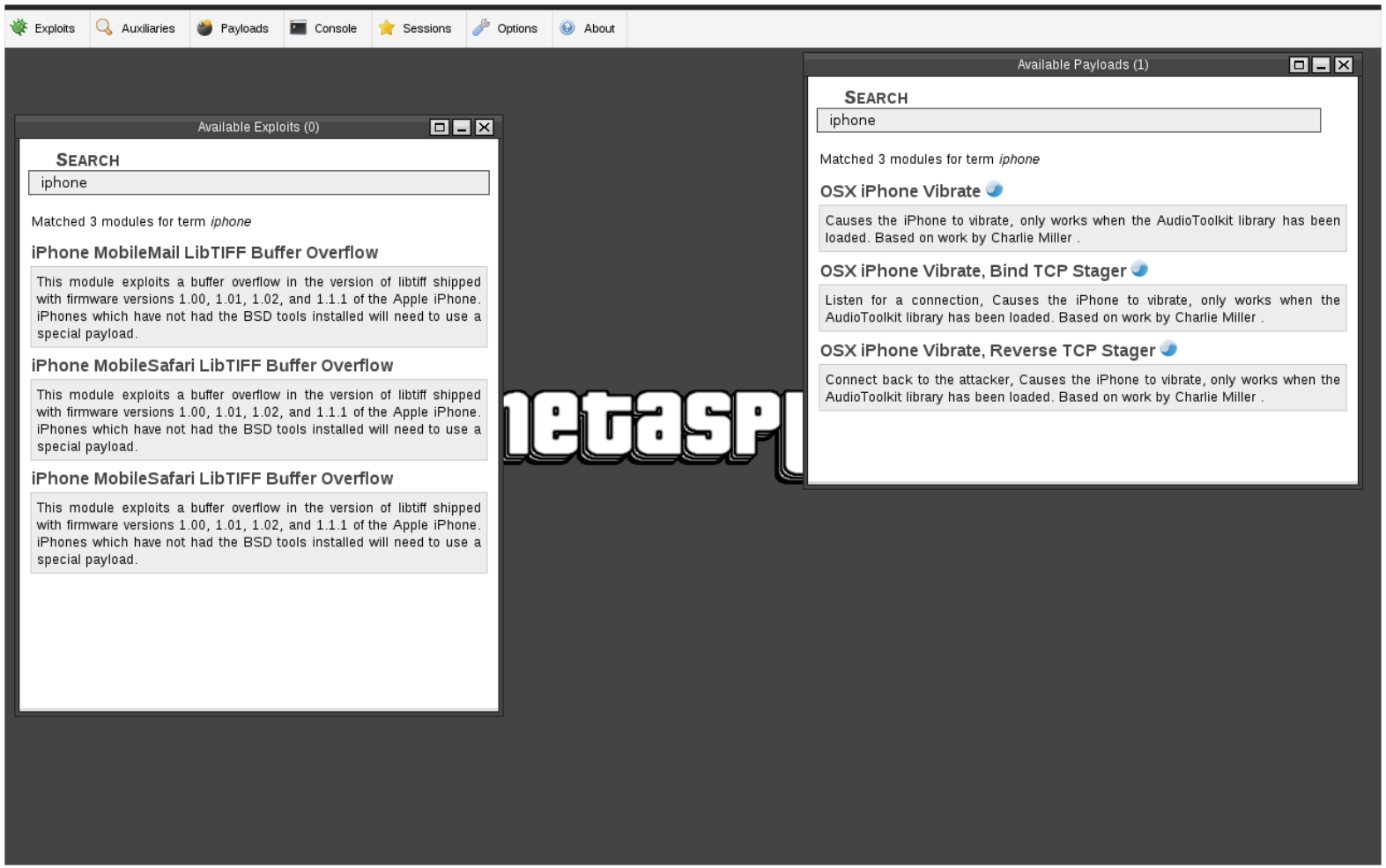
Les smartphones

iPhone OS

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

atlab
La Sécurité Offensive

Les smartphones



atlab
La Sécurité Offensive

Les smartphones

RIM Blackberry OS

- Peu de logiciels malicieux
- Présentations
  - Blackjacking, 0wning the Enterprise via Blackberry
  - RedBerry, Advanced Attacks via a Trojaned blackberry
- Logiciel espion commercial

atlab
La Sécurité Offensive

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

atlab
La Sécurité Offensive

Windows Mobile

Logiciels malicieux

- Exemples :
  - Trojan WinCE/Brador.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*

atlab
La Sécurité Offensive

Logiciel Espion

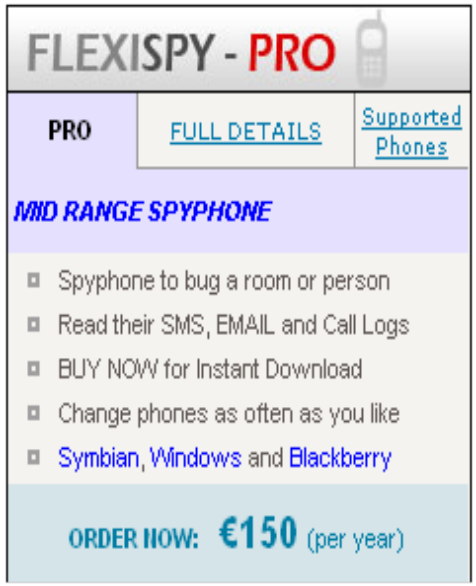
Fonctionnalités :

- 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

atlab
La Sécurité Offensive

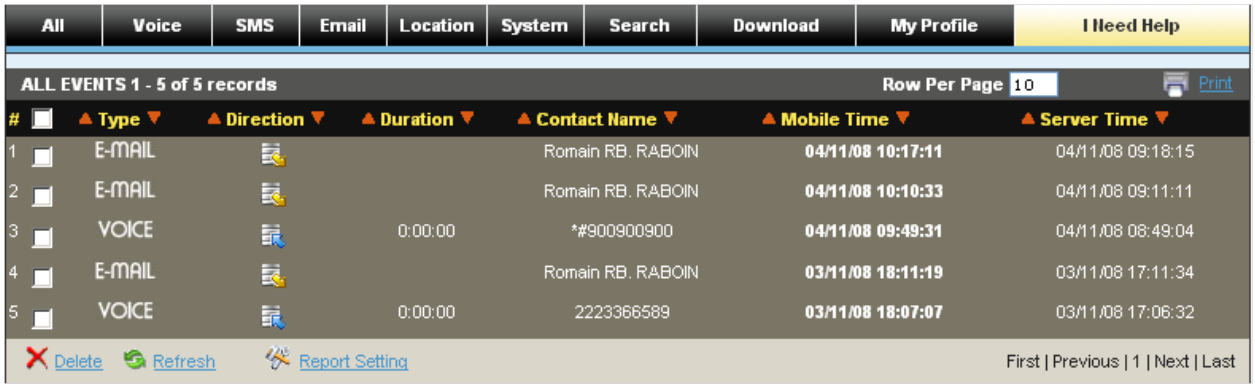
Logiciel Espion

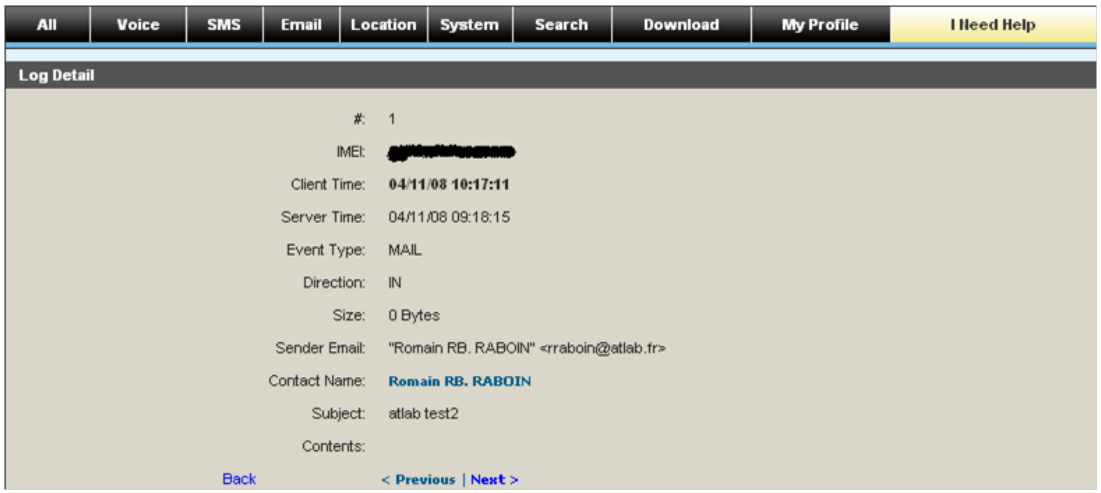
Espionnez votre femme grâce à FlexiSPY !



atlab
La Sécurité Offensive

Logiciel Espion





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

atlab
La Sécurité Offensive

Méthodes d'infection

Social engineering

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

atlab
La Sécurité Offensive

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

atlab
La Sécurité Offensive

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*

atlab
La Sécurité Offensive

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)

atlab
La Sécurité Offensive

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()**

atlab
La Sécurité Offensive

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

atlab
La Sécurité Offensive

RAPI

Exemple d'un fichier de *policies* :

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

atlab
La Sécurité Offensive

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

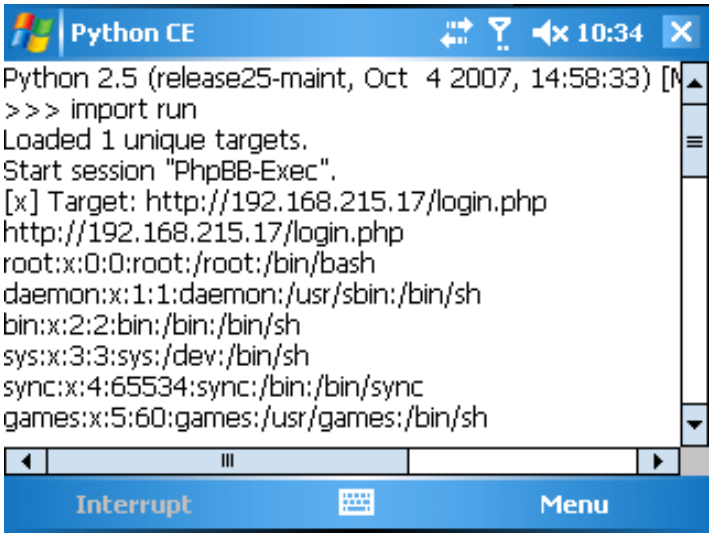
atlab
La Sécurité Offensive

Création d'un logiciel malveillant

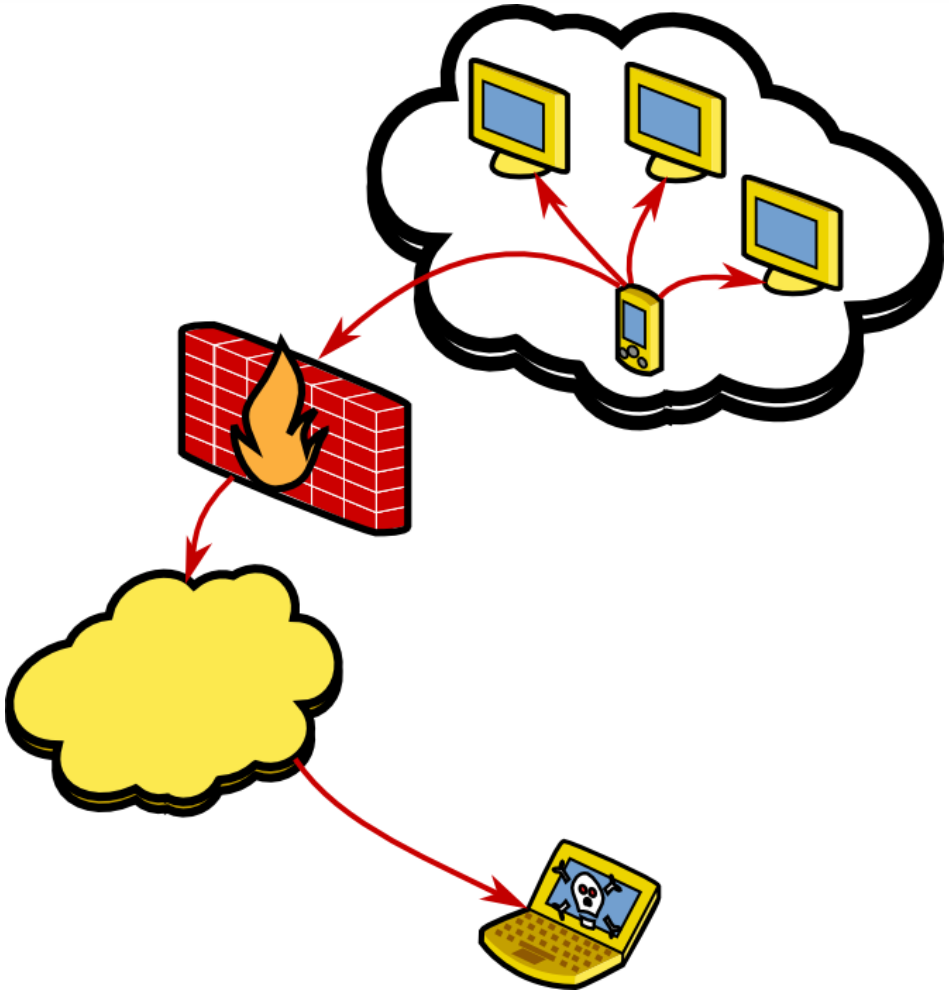
Démonstration

Attaques depuis un smartphone

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



Attaques depuis un smartphone



Faiblesses

- Nombreux vecteurs d'échange (y compris Micro SD, SD Cards), envoi de fichiers et éxecution
- 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

atlab
La Sécurité Offensive

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

atlab
La Sécurité Offensive

Questions

- Merci de votre attention
- Contacts :
  - Romain Raboin : rraboin@atlab.fr
  - www.atlab.fr
  - www.lasecuriteoffensive.fr

atlab
La Sécurité Offensive