Mobilité, quand tout ordinateur peut devenir cheval de Troie

SSTIC 2004, 2-4 juin, Rennes

Cédric Blancher <cedric.blancher@arche.fr>
Arche, Groupe Omnetica
MISC Magazine

Agenda

1) Introduction : le concept de mobilité

2) Sécurité et mobilité

3) Scénario “catastrophe”

4) Concilier mobilité et sécurité

5) Conclusion

Introduction :
le concept de mobilité

Le concept de mobilité

- Mobilité
  - **Concept marketing récurrent**
  - **Possibilité pour l'utilisateur de se sentir chez lui n'importe où**
    - **Quel que soit le lieu**
    - **Quel que soit le terminal**
  - **“Keep connected, anywhere”**

- Déballage de moyens techniques pour rendre ce “miracle” possible

Le concept de mobilité

Méthodes de connexion entre le terminal et le réseau d'entreprise à travers l'environnement, en tenant compte de :

- **La diversité des terminaux**
- **La diversité des environnements de connexion**

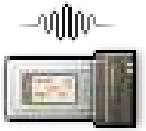
➔ Situation **très compliquée** à maîtriser

Le concept de mobilité

- Exemples de terminaux

  - **Laptop**
  - **Poste de travail fixe à la maison**
  - **CyberCafé**
  - **Ordinateur de poche**

- Exemple d'environnement
  - **Connexion personnelle à domicile (PAN)**
  - **Chez un client**
  - **HotSpot WiFi**



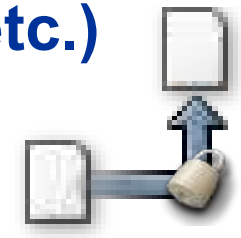
Le concept de mobilité

Exemples de moyens d'accès

- **Portail Web**
- **VPN SSL**
- **VPN classique**

Ces liens sont sécurisables :

- **Authentification (OTP, certif., tokens, etc.)**
- **Confidentialité (chiffrements divers)**



MAIS, tous ces moyens d'accès supposent un poste sain...

Mobilité et sécurité

Le poste mobile est un poste de travail, et donc une cible de choix

- Cible facile à atteindre
  - **Disponible physiquement**
  - **Souvent peu protégé**
  - **Largement connecté (web, email)**
  - **Last, but not least : opéré/administré par un “utilisateur”**

- Cible intéressante
  - **Accède au coeur du système d'information**
  - **Accède à des ressources sensibles**

Protection du poste de travail

- Protection physique
- Protection périphérique
- Antivirus local
- Pare-feu personnel
- Application des patches de sécurité
- Gestion correcte des utilisateurs et des droits

Déjà difficile en environnement fixe : protections contournables, difficultés de gestion, etc.

Mobilité et sécurité

En environnement mobile, c'est pire :

- La protection physique est trop faible
- Les protections périphériques sont inutiles
- Manque de réactivité dû à la mobilité :
  - **application des patches de sécurité**
  - **mise à jour des bases antivirus**

- Dérive par rapport à la politique de sécurité initiale

→ C'est une partie du SI qui part en vadrouille

Quelques cas intéressants

- Le cas du poste inconnu
- Le cas du poste personnel à la maison
- Le cas du laptop en voyage
- Le VPN SSL

Le cas du poste inconnu (Cybercafé, client, etc.)

- Connexion via interface HTTPS
  - **Niveau de sécurité du poste inconnu**
  - **Risque de laisser des traces (cookies, documents temporaires, etc.)**
  - **Le propriétaire est-il bien intentionné ?**

➔ Une solution à limiter au maximum, avec le moins de privilèges possible

Le poste personnel à la maison

- Connexion via un VPN (ex. IPSEC)
  - **Niveau de sécurité du poste ?**
  - **Risque de compromission non négligeable**
  - **Passerelle potentielle vers le coeur du SI**

➔ Est-il raisonnable de laisser des terminaux non contrôlés se connecter au SI ?

Le laptop en voyage

- Connexion de type VPN ou VPN SSL
  - **Problème évident de sécurité physique (vol, introduction de données)**
  - **Problème de maintient du niveau de sécurité du poste**
  - **Problème de sécurité face à l'environnement**
  - **Le poste revient avec son lot de malware au coeur du SI**

- La mobilité des autres : le laptop d'un visiteur qu'on connecte au SI

Le VPN SSL, accès supposé et simple et sûr

- **Accès via un navigateur aux ressources :**
  - Groupware
  - Documents de travail
- **Application Web ou redirection via le navigateur**

- Mais :
  - Le poste utilisé est-il sûr ?
  - Le navigateur utilisé est-il sûr ?
  - Certaines fonctionnalités supposent les droits administrateur (redirection)
  - Des traces qui restent (cookies, login/mdp, documents)

→ Est-ce bien raisonnable ?

Scénario “catastrophe” sur mesure

Scénario “catastrophe”

Attaque d'un SI via ses postes nomades

- Contexte :
  - **Utilisateur mobile pourvu de son laptop**
- Vecteur d'attaque :
  - **Backdoor asynchrone**
- Attaque en quatre étapes :
  1. **Infection**
  2. **Implantation**
  3. **Communication**
  4. **Actions**

Étape paradoxalement la plus simple

- Actions physique
  - **Périphérique de stockage avec autorun (CDROM, USB, etc.)**
  - **Prise en main du poste (reboot éventuel)**

- Exécution d'un malware par l'utilisateur (ou ses outils)

  - **Par courrier électronique**
  - **Via Web**
  - **Exploitation de failles de logiciels (IE, OE, etc.)**
  - **Mise à profit du contexte (détournement, etc.)**

- Compromission du poste
  - **Utilisation d'une faille pour implanter du code malveillant**

- La compromission suppose la connexion, mais pas forcément volontaire...
  - **Le poste peut être connecté en environnement hostile (ex. HotSpot Wifi, Cybercafé)**
  - **Les capacités wireless peuvent être mises à profit (WiFi, BlueTooth, IR) par un pirate**

La backdoor doit pérenniser son accès

- Écriture sur le disque pour ré-exécution
- Modification de la BDR ou lien dans le menu “Démarrer”
- Infection des process existants par API Hooking

Furtivité : éviter de rester en mémoire

- ➔ Tuer le processus père de la backdoor

La backdoor doit communiquer :

- Transmettre des données (documents, résultats d'action, etc.)
- Recevoir des données (ordres, modules d'attaque, etc.)

Furtivité : ne pas communiquer directement, ne pas altérer les objets (exe, dll) existants

- ➔ Utilisation d'applications tierces (ex. IE) pour relayer les messages
- ➔ Utilisation de l'API Hooking pour communiquer via des applications valides

L'action d'initier une communication peut-être conditionnée

- Activité réseau
- Disponibilité de sites de référence
- Utilisation d'un protocole (HTTP)

La communication sera banalisée

- Utilisation de HTTP
- Chiffrement des données

4. Actions

La backdoor est à même de mener des actions :

- Vol de documents (.doc, .xls, .pdf, etc.) sur le poste et le SI environnant
- Vol d'identifiants (keylogger)
- Élévation de privilèges
- Infection d'autres éléments du SI
- Etc...

Ces actions peuvent être menées

- Depuis une connexion nomade à travers le VPN
- Depuis le cœur du SI lorsque le laptop revient

La backdoor est asynchrone

- Elle n'a pas besoin de connectivité pour agir
- S'adapte à l'environnement

Conclusion

- Le SI est corrompu
  - **Les protections périphériques du SI n'ont servi à rien**
  - **Les liens VPN ont été exploités pour atteindre le SI, sans être attaqués**

- Un cas réel ? Blaster
  - **Postes nomades infectés en vacances**
  - **Entrée du ver via les liens VPN**
  - **Entrée du ver au retour de vacances**

Concilier mobilité et sécurité

Concilier mobilité et sécurité

Sécuriser le poste de travail (fixe ou itinérant)

- Choix des applications (IE vs. Mozilla)
- Choix du système d'exploitation (on aurait vu des gens travailler efficacement sous GNU/Linux)
- Renforcer l'administration : gestion des utilisateurs, droits, updates, etc.
- Outils de sécurité : antivirus, pare-feu personnel
- Outils “nouvelle génération” : interception des appels système, application de politique dynamique

Concilier mobilité et sécurité

Réfléchir sur l'intégration de la mobilité

- Intégration à l'architecture existante
- Compartimentation : ne pas traiter les terminaux mobiles comme les terminaux fixes
- Utilisation de zones de quarantaines :

  - **Network Access Quarantine Control de Microsoft**
  - **Self-Defending Networks de Cisco**
    - **Examen du terminal avant accès au réseau**
- Résister au discours technico-commercial !

Concilier mobilité et sécurité

Contrôler l'accès à ses ressources

- Bannir les terminaux non contrôlés ?
  - **À l'intérieur du SI**
  - **À l'extérieur, pour l'accès aux ressources “mobiles”**
- Contrôler l'accès physique au SI
  - **Prises réseau, accès WiFi**
  - **Utilisation de 802.1x**

➔ Mettre en place une politique d'accès stricte

Conclusion

Conclusion

- La mobilité n'est pas une fonctionnalité triviale qui s'ajoute facilement au SI
- La mobilité peut ruiner l'efficacité des dispositifs de sécurité

- → À l'heure actuelle, il n'y a pas de solution vraiment adaptée à la mobilité, mais elles arrivent
- → La mobilité demande des règles strictes, une surveillance accrue et une forte réactivité

Greetings

- rstack.org
  - http://www.rstack.org/

- Everybody at MISC
  - http://www.miscmag.com/
- French Honeynet Project
  - http://www.frenchhoneynet.org/
- Guys at Pirateur.net
  - http://www.pirateur.net/

Questions ?