Mobilité, le trou dans la cuirasse... Des risques induits par le nomadisme

Cédric BLANCHER

http://sid.rstack.org/

sid@rstack.org / cedric.blancher@eads.net
Centre Commun de Recherche, EADS
Département DCR/SSI
Suresnes, FRANCE

Journée de la Sécurité des Systèmes d'Information
10 mai 2005

EADS CCR

Plan de la présentation

EADS CCR

Plan

EADS CCR

De quoi vais-je vous parler ?

Des accès distants au Système d'Information (SI) par des stations nomades

- Concept marketting très "fashion"
- Possibilité de se connecter au SI à distance
- Depuis des terminaux variés (portable, PDA, Smartphone, etc.)
- Depuis des lieus variés (réseau domestique, entreprise, hotspot WiFi, cybercafé, etc.)

Les terminaux, les moyens de connexion et de sécurisation de tels flux sont disponibles

EADS CCR

Moyens d'accès

Accéder aux ressources nécessaires disponibles sur le SI

- Accès webifié aux ressources : email, fichiers, groupware, etc.
- VPN SSL : redirection de port "clientless" (à la SSH)
- Accès VPN classique : accès "full IP" au SI

De tels liens peuvent être sécurisés

- Authentification (OTP, RSA sigs, x509)
- Confidentialité (chiffrement)

Focus sur le VPN SSL

Solution soit-disant "clientless" pour l'accès au SI
Se décline du portail Web à l'accès "full IP" sur HTTPS

Problèmes

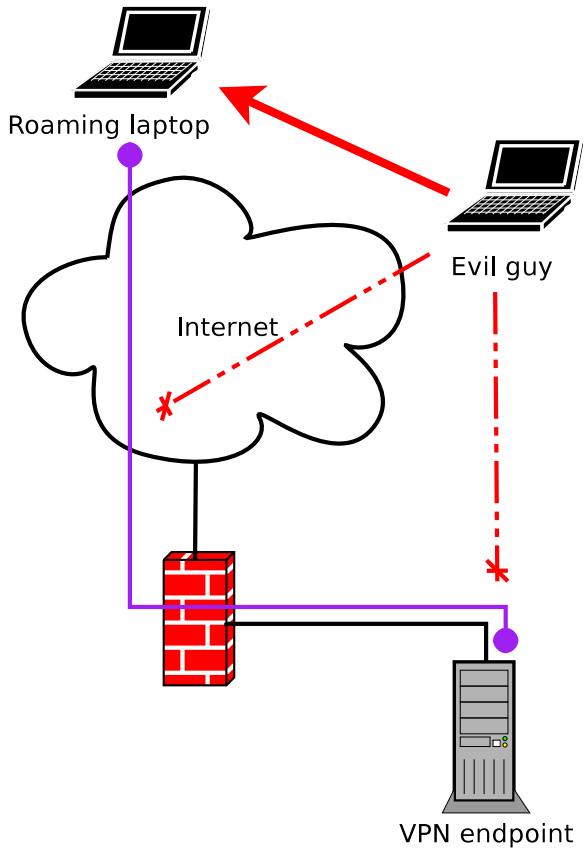
- Rediriger un port local dans un flux HTTPS nécessite l'exécution de code distant (Java, ActiveX) : la plupart des solutions nécessitent MSIE...
- La surcharge des résolutions DNS par écriture dans le fichier hosts nécessite des droits privilégiés
  $\Longrightarrow$ IE + Admin : le couple gagnant ?
- Un accès "full IP" nécessite un client dédié pour monter le lien (ex. : PPP sur SSL)

Bon... Et alors ?

Les liens sont sécurisables. Mais...

La problématique des terminaisons

Est-ce qu'on peut vraiment faire confiance à la station nomade ?
Que se passe-t-il si elle est compromise ?



EADS CCR

Plan

EADS CCR

Station nomade et Système d'Information

But : connecter à distance un utilisateur au SI

- Spécificités de la station nomade
- Spécificité de l'environnement de connexion

Ces spécificités imposent des contraintes

EADS CCR

La station nomade

Une station nomade est une cible intéressante

- Elle est disponible physiquement
- Elle est connectable au réseau et/ou au SI
- Elle a accès à des ressources critiques
- Elle est opérée par un utilisateur

Poste de travail vs. station nomade

La station nomade ne peut s'appuyer sur aucun dispositif de protection en dehors des siens

Poste de travail

- Protégé physiquement
- Dispose de protections réseau périphériques
- Antivirus local
- Pare-feu personnel (pas toujours)
- Mises-À-Jour (MAJ) automatiques programmées

Station nomade

- Aucune protection physique
- Aucune protection réseau périphérique
- Antivirus local (quid des MAJ ?)
- Pare-feu personnel
- Pas de MAJ lorsqu'il n'est pas connecté

L'exposition de la station nomade

Les stations nomades sont infiniment plus exposées que les postes de travails classiques

Question

Laisseriez-vous une 15e de postes de travail connectés une journée entière directement à Internet, et les remettriez-vous dans le LAN juste comme ça ?

$\Longrightarrow$ C'est pourtant ce qui se passe avec de nombreuses configuration de portable

EADS CCR

Sécurité physique

Les portables, PDA et autres terminaux mobiles sont faciles à voler
Or, ils disposent :

- De données sensibles
- De crédences d'authentification (cache de logon, stockages de mot de passe, informations de configuration, etc.)
- D'accès préconfigurés au SI via les liens sécurisés

Les PDA et les mémoires de masse portables sont particulièrement visées...

Environnement

Une station mobile est souvent connecté à un environnement non-sûr

- Réseau inconnu, ex. cybercafé, réseau domestique, etc.
- Réseau WiFi, ex. hotspot, réseau domestique "protégé" (WEP)

Des tels environnements peuvent être compromis

Accès distant

Quel confiance peut-on accorder au système qui se connecte ?

- Station personnelle : simple à compromettre ou infecter
- Portable "*personnalisé*" : quid de son niveau de sécurité ?
- Station inconnue (accès "clientless") typique du cybercafé

"Rentrer Maison"

Peut-on laisser une station nomade se reconnecter au SI après un séjour à la campagne ?

- Où[1] s'est-elle connectée ?
- Est-elle infectée ?
- Est-elle compromise ?
- Va-t-elle devenir une source d'infection pour le réseau complet ?

Ne pas oublier les stations des gens de passage sur le SI (avant-vente qui demande à télécharger ses slides)

[1] À pleins d'endroits, mais pas là

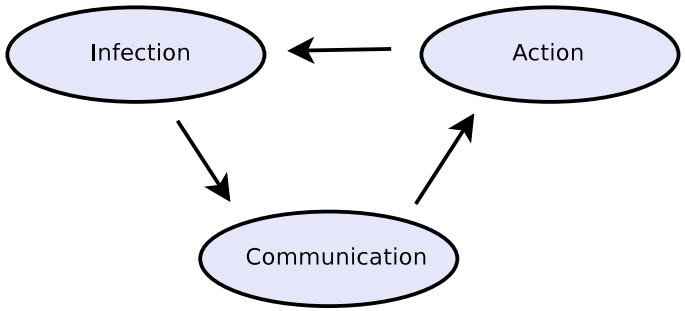
Plan

Scénarion d'intrusion

Attaque du SI via une station nomade[2]

Attaque en trois étapes :

1. Infection
2. Communication
3. Action



[2]Suite à l'adoption de la LCEN, certains outils mentionnés pourraient ne plus être disponibles en ligne...

Infection

La phase importante, mais paradoxalement la plus *simple*...

Vecteurs d'attaque

- Accès physique
- Attaque direct via un lien réseau
- Corruption des communications réseau

Accès physique

Récupération d'information

- Exploration du disque dur
- Trouver des documents sensibles
- Trouver des crédences d'authentification
- Trouver des informations de configuration

La vraie vie dot com

Extraction du disque dur et analyse sur un autre système

- Fichier batch contenant le mot de passe de groupe du concentrateur VPN
- Ce même mot de passe est sauvergardé chiffré par le client VPN dont une version vulnérable permet sa récupération en mémoire
- Les crédences d'accès au domaine du SI sont extraites du cache de logon

Conséquence

Accès complet au SI via le VPN

Accès physique

Amorcer la station sur un autre OS via CDROM, USB ou le réseau[3]

- Modification des crédences superutilisateur/utilisateur
- Accès complet au système de fichiers
- Accès à certaines parties supposées protégées

Conséquence

Accès à des informations sensibles (cf. supra)

[3] Certains BIOS de portable amorcent en PXE sans demander le mot de passe...

Accès physique

Corrompre le système

- Infection via autorun : CDROM, clé USB[MAY05], etc.
- Attaque réseau : on connecte le câble, DHCP, attaque
- Attaque Firewire[DOR04] : corruption de la mémoire du système
- Si on a accès à la console, exécution d'un binaire

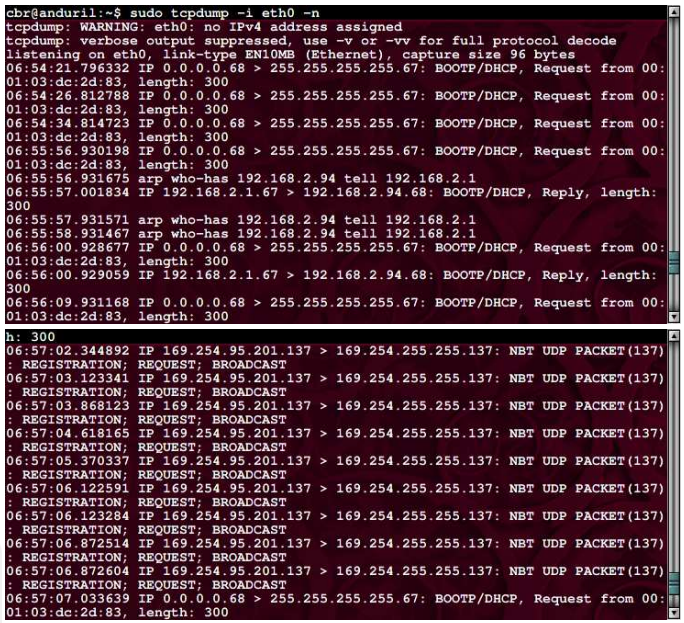
Conséquence

Compromission de la station, exécution de code malicieux

La vraie vie dot com

Un portable WinXP à jour disponible physiquement et locké

- Insertion d'une carte réseau PCMCIA
- Activation automatique de la carte par le poste
- Recherche de configuration DHCP
- Communication sur la configuration affectée ou 169.254.0.0/16



Conséquence

Lien réseau monté (réseau *local*) avec la cible

EADS CCR

Connexion réseau

Station pas forcément connectée : exploitation des liens sans-fil

- Lien IR : similaire à de l'accès physique
- Bluetooth : contre les téléphones ou les PDAs mal protégés
- WiFi : façons multiples d'associer un driver à un AP
  $\Longrightarrow$ Le coup de l'AP[MZ04] malicieux fonctionne souvent !

La vraie vie dot com

Un portable WinXP avec interface WiFi activée

- AP malicieux avec DHCP
- Exploit RPC/DCOM[a]
- Ajout d'un utilisateur et reconnexion en RDP
- Installation du port Win32 de la backddor Recub[EOS04]

[a] le pare-feu personnel a une exception pour le "réseau local"

Conséquence

Portable compromis, backdoor installée et active

Portable connecté à un environnement hostile

Une station nomade se connecte sur des réseaux propices aux attaques

- AP malicieux
- Serveur DHCP malicieux
- Corruption de cache ARP
- Corruption de réponses DNS, de cache DNS (Windows)
- Redirection et corruption de trafic réseau
- Accès aux ressources partagées
- Exploitation distante de failles

Outils : arp-sk[RAY02], rogue AP stuff[MZ04], dnsa[BET03]

EADS CCR

La vrai vie dot com

Portable connecté à un HotSpot WiFi commercial classique (= pas sécurisé)[4]

- Redirection du trafic HTTP par corruption de cache ARP
- Hotspot : authentification Web sur un portail captif
  $\Longrightarrow$ Corruption du trafic HTTP par redirection locale
- Exploitation d'une faille du navigateur par injection de contenu malicieux

Outils : arp-sk[RAY02], scapy[BIO02]

Consequence

Le code malicieux est exécuté avec le niveau de privilège de l'utilisateur
Indice : VPN SSL / MSIE / Admin / Couple gagnant...

[4] Les restrictions entre stations se contournent

Le pare-feu personnel

Quid du pare-feu personnel si présent et activé

- On peut l'exploiter : fragmentation, faille, etc.
- La *"célèbre"* exception pour le partage sur le "réseau local"
- Le pare-feu des clients VPN est activé si le VPN est monté
- On peut les contourner (gestion des broadcast UDP par XP SP2)

Conséquence

Dans pas mal de cas, la protection n'est pas aussi efficace que prévu[BLA03]...

Le pare-feu personnel

Quid du pare-feu personnel si présent et activé

- On peut l'exploiter : fragmentation, faille, etc.
- La *"célèbre"* exception pour le partage sur le "réseau local"
- Le pare-feu des clients VPN est activé si le VPN est monté
- On peut les contourner (gestion des broadcast UDP par XP SP2)

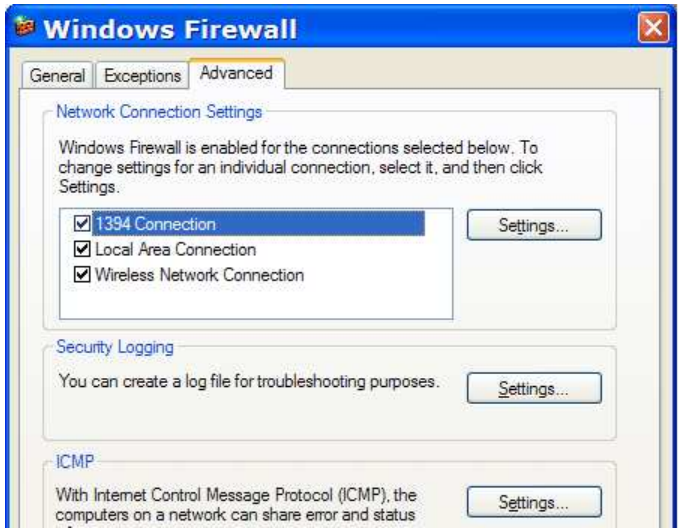
Conséquence

Dans pas mal de cas, la protection n'est pas aussi efficace que prévu[BLA03]...

Le pare-feu personnel

Quid du pare-feu personnel si présent et activé

- On peut l'exploiter : fragmentation, faille, etc.
- La *"célèbre"* exception pour le partage sur le "réseau local"
- Le pare-feu des clients VPN est activé si le VPN est monté
- On peut les contourner (gestion des broadcast UDP par XP SP2)



Conséquence

Dans pas mal de cas, la protection n'est pas aussi efficace que prévu[BLA03]...

Code malicieux

Exécution de la backdoor

- La backdoor est écrite sur le système de fichiers
- Elle modifie le démarrage du système (BDR, Start menu)
- Elle s'attache aux processes courants (API hooking) et meurt

Outils : Casper[DD04], Recub[EOS04]

Consequence

Station compromise, backdoor/trojan actif

Établissement du canal de communication

La backdoor doit communiquer avec le monde extérieur en passant le pare-feu personnel et les protections périmétriques éventuelles

- Les threads sont attachés à des applications autorisées (ex. navigateur)
- La communication est déclenché par un trafic spécifique (ex. requête HTTP)
- L'utilisation d'une API HTTP/HTTPS native permet la récupération automatique de la configuration réseau (proxy, crédences)
- Mise en place d'un canal caché sur HTTP/HTTPS

Outils : Casper[DD04], Recub[EOS04]

Conséquence

La backdoor communique à travers un protocole autorisé

Établissement du canal de communication

On peut également exploiter des API "Designed for Microsoft® Windows®"...

- API pour permettre aux applications de générer leurs propres exceptions sans notification de l'utilisateur
- API UPnP qui permet aux applications de générer des autorisations et redirections de port sur les routeurs compatibles

Conséquence

La backdoor se rend joignable à travers le firewall XP SP2 et le NAT

Les actions de la backdoor

La backdoor peut agir sur demande

- Vol de données sur le poste compromis ou ceux disponibles sur le réseau
- Extensions possibles par upload de modules
- Découverte de l'environnement réseau
- Escalade de privilèges locale
- Attaque de l'environnement réseau

Outil : JAB[GRE03]

Les actions de la backdoor

Dans le cas d'une backdoor hookée sur un process

- Vol de crédences
- Vol de clés et certificats[5]
- Interception de trafic réseau
- Détournements de fonctionnalités
- Etc.

Par exemple, il est possible de créer un MiM SSL universel et transparent[DR05]

[5] Passphrase comprise

Périmètre d'action

La backdoor peut agir depuis :

- Le SI lui-même
- Un accès VPN

Backdoor asynchrone et adaptative

- Actions réalisable sans connexion avec un master
- S'appuie sur des applications configurée
- Délivre ses résultats et récupère ses ordres dès qu'une connexion est disponible

La vraie vie dot com

Souvenez-vous : le ver Blaster[6] (été 2003)

- Portables compromis pendant les vacances en se connectant à Internet
- Le ver se propage également par des liens VPN
- Le ver se propage quand les gens reviennent au bureau (syndrôme du lundi pourri)

Conséquence

Des réseaux entiers protégés par leurs 3 couches de firewalls/proxies/antivirus/etc. sont compromis

[6] On aurait pu également citer Slammer (mai 2004)

Plan

EADS CCR

Réduction des risques

Il n'existe pas de solution *sur étagère* prête à l'emploi
Cependant, les risques peuvent être fortement réduits

- Protection physique de la station
- Protection du système
- Intégration dans l'architecture existante
- Protection du Système d'Information

Protection physique

Empêcher le vol de la station si possible, ou au moins empêcher la récupération d'informations

- Dispositifs antivol : marquage, câble antivol[7]
- Choix de la plate-forme matérielle (ex. : fonctionnalités du BIOS)
- Mise en place du mots de passe BIOS et verrouillage de l'amorçage sur le HDD
- Mot de passe sur le HDD ATA[8]
- Espace de stockage chiffré

[7] Attention, crochetage au stylo...
[8] Disponible depuis ATA3

Protection du système

Appliquer des mesures strictes

- Choisir un OS approprié
- Choisir des applications appropriées
- Durcir la configuration : comptes non privilégiés, gestion des droits, politique de MAJ, etc.
- Mise en place d'outils de sécurité : au minimum antivirus et pare-feu personnel
- Outils "nouvelle génération" : interception des appels systèmes, mise en place de politique de sécurité, etc.

EADS CCR

Intégration à l'architecture du SI

Réfléchir à deux fois avant d'intégrer un solution nomade dans l'architecture existante

- Ne pas traiter les stations nomades comme les postes internes : ils ne sont pas exposés de la même manière
- Restreindre l'accès des stations nomades au SI
- Dépasser le discours commercial *"Happy World"*

EADS CCR

Protection du Système d'Information

Contrôler l'accès au réseau

- Interdire les stations inconnues
- Mettre en place du contrôle d'accès physique et/ou logique (ex. 802.1x)
- Penser à la segmentation et aux zones de "quarantaines"
  - VLANs dédiés isolés pour les invités
  - Vérification manuelle ou automatique[9] des stations nomades avant connexion

[9] Si disponible

Plan

EADS CCR

Conclusion

Les accès nomades apportent beaucoup, mais peuvent réduire à néant la sécurité du SI

Les solutions miracle n'existent pas (encore ?)

Cependant, la réduction des risques reste possible, mais passe par une politique stricte, spécifique et adaptée pour les stations nomades

Remerciements

Merci à...

-  ...
- L'équipe **Rstack.org**
  `http://www.rstack.org/`
- **MISC Magazine**
  `http://www.miscmag.com/`
- **French Honeynet Project**
  `http://www.frenchhoneynet.org/`

Vous pouvez télécharger cette présentation sur
`http://sid.rstack.org/contrib.html/`

EADS CCR

Plan

EADS CCR

Bibliographie I

- [BET03] Pierre Bétouin, dnsa, `http://securitech.homeunix.org/dnsa/`
- [BIO02] Philippe Biondi, scapy, `http://www.secdev.org/projects/scapy.html`
- [BLA03] Cédric Blancher, Atouts et limites du concept de sécurité du pare-feu personnel, SSTIC 2003
- [DD04] Éric Detoisien & Eyal Dotan, API Win32 ancestrale pour chevaux de Troie hyper furtifs, Black Hat Europe 2004 & JSSI 2004
- [DR05] Éric Detoisien & Nicolas Ruff, Malwares la menace de l'intérieur, JSSI 2005

EADS CCR

Bibliographie II


[DOR04] Maximillian Dornseif, "0wn3d by an iPod - Firewire/1394 Issues", Cansecwest/core05


[EOS04] EOS India, Recub Win32 port, `http://www.eos-india.net/misc/main.html`


[GRE03] Nicolas Grégoire, JAB - Une backdoor pour réseau Win32 inconnu, SSTIC 2003


[MAY05] David Maynor, "0wn3d by everything else - USB/PCMCIA Issues", Cansecwest/core05


[MZ04] Shane "K2" Macaulay & Dino Dai Zovi, "Rogue Access Points", Cansecwest/core05

EADS CCR

Bibliographie III

 [RAY02] Frédéric Raynal, arp-sk, `http://www.arp-sk.org/`