A2IMP - Particularité de Windows

Boris Valera
(boris.valera@insa-toulouse.fr)
d'après Christophe Dubois

31 mars 2009

Un système graphique

- Administration via des applications graphiques
  - dispersions des configurations et logs
  - exécutions de tâches invisibles
- L'intrus ne lance pas de commande mais télécharge des outils de contrôle à distance ou des malwares
- Objet d'une intrusion :
  - vol de la base de login/password
  - exécution d'un shellcode provoquant un téléchargement
  - installation d'outils de téléadministration (DameWare, RAdmin, etc)
  - installation de codes malveillants (chevaux de troie en tout genre)

Démarrage automatique de programme

Il existe plusieurs façons :

- Base de registre
- Services
- Certains répertoires (dossier Démarrage du menu Démarrer)
- Certains fichiers (`.ini`, `.sys`)

Journaux systèmes

- Peu de fichiers de journalisation pour le système
- Journaux éclatés sur le système
- Erreurs parfois incompréhensibles : nécessité d'aller sur des sites comme `http://www.eventid.net`

Processeurs x86 : notion de ring

- Hiérarchie
  - Ring 3 userland (niveau applicatif)
  - Ring 2 inutilisé
  - Ring 1 inutilisé (sauf par certains malwares)
  - Ring 0 kernelland (niveau noyau)
- Chaque *ring* ne peut communiquer qu'avec ses voisins directs
- Les outils de diagnostics s'exécutent souvent en *ring* 3 et ne détectent donc pas ce qu'il y a dans les rings en dessous

NTFS et ADS (1)

- Origine : permettre l'interopérabilité avec HFS (Système de fichiers de Macintosh)
- Spécifications disponibles sur `http://www.ntfs.com`

NTFS et ADS (2)

- Problèmes
  - Fonctionnalité peu connue
  - Flux additionnel perdu si on quitte le contexte NTFS
  - Peu d'outils pour consulter les ADS (tous en *ring 3*) : lads, StreamDir, Stream Find et ADS Check
  - Peut être attaché sur des dossier
  - Ne modifie pas les sommes MD5 et SHA1
- Surtout utilisé par les malwares.

Exemple réel : `explorer.exe:malware`

NTFS et ADS (3)

- Accessible via ":" suivi d'un nom

  fichier.txt flux principal
  fichier.txt:info flux additionnel
- Accès en lecture à un flux ADS :
  `notepad fichier.txt:info`
- Écriture d'un flux ADS :
  `type malware.exe > fichier.txt:malware`
- Les *rootkits* utilisent souvent les flux ADS pour dissimuler des fichiers

NTFS et ADS (4)

- Bien pris en comptes par les anti-virus et outils de protection
- De plus en plus d'outils pour les détecter et les supprimer
  - LADS (`http://www.heysoft.de/`)
  - Streams de sysinternals
  - Stream Explorer (`http://www.rekenwonder.com/streamexplorer.htm`)

Détecter une intrusion

- C'est assez difficile car :
  - Les outils de diagnostic sont en *ring 3* et les malwares parfois en *ring 0*
  - Le nombre normal de processus lancés est élevé et on ne connait pas toujours leur utilité (par ex. svchost)
  - Le nom des processus est en relatif et pas en absolu $\rightarrow$ impossibilité de distinguer deux processus de même nom

Quelques signes

- Fenêtre de commande qui s'ouvre et/ou se ferme toute seule
- Messages d'erreur au démarrage (pop-up)
- Navigation sur des sites web non souhaités
- Surcharge du processeur

Détection d'anomalies

- Plusieurs points vérifier régulièrement :
  - l'espace disque
  - Les clés dans la base de registre (en particulier les clés "run")
  - les noms de processus
  - la charge d'un processus
  - les flux alternatifs

Diagnostic

- Peu d'outils de diagnostic de base :
  - Gestionnaire des tâches
  - `netstat -ano`
  - `netstat -ban`

  NB : Windows utilise des sockets réseau pour la communication interne de ses processus
- Nécessité d'utiliser des outils externes :
  - le Windows debugger (téléchargeable sur le site de Microsoft) : permet de "lire" les fichiers de dump des BSOD
  - SysInternals (`http://www.microsoft.com/technet/sysinternals/`) : filemon, regmon, handle, tcpview, etc.

Rootkits sous Windows (1)

- Vbootkit
  - Rootkit pour Vista
  - infection de la machine par un secteur de boot spécial
- Hacker Defender
  - très performant
  - retrouvé dans de nombreux incidents du CERTA il y a quelques temps
  - indétectable par des outils de niveau *ring 3*
  - détectable par le réseau ou les partages
- Blue Pill
  - en vogue
  - niveau *ring 1*
- Utilisation des ADS de NTFS

Rootkits sous Windows (2)

- Plusieurs outils de détection
  - Rootkit Revealer de Sysinternals
  - Icesword (`http://mail2.ustc.edu.cn/~jfpan/`)
  - Blacklight de F-Secure (`http://www.f-secure.com/en_EMEA/products/technologies/blacklight/`)
  - RKDetector (`http://www.rkdetector.com/`)

Démarche

- Utiliser la boîte à outils
- Isoler la machine du réseau
- Collecter les traces réseau

Ces opérations peuvent s'effectuer dans n'importe quel ordre mais chacune peut avoir des conséquences. En particulier, isoler la machine du réseau peut provoquer l'arrêt de certains processus.

- Copier le disque dur
- Déclarer l'incident

Isoler la machine du réseau

Une fois les informations volatiles récupérées à l'aide de la boîte à outils, isoler la machine du réseau puis l'éteindre proprement

- Cette étape doit venir après la récupération des processus

Copie du disque

- Démarrer avec une distribution de type LiveCD et faire une image via dd par exemple.
- Copier tout le disque d'un coup pour permettre de rebooter la machine virtuellement
  - ceci permet de tester des codes malveillants dans leur environnement d'origine
- Calculer la signature de l'original

Questions