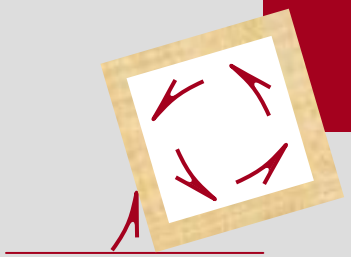
Le progrès est technique,

l'évolution est humaine

Le contrôle d'intégrité et ses limites.



SSTIC

Cyril Leclerc

03 Juin 2005

ARSeO Conseil

Agenda

- Pourquoi contrôler l'intégrité ?
- Panorama du contrôle d'intégrité actuel
- Les contraintes du contrôle en production
- Les différents vecteurs d'injection
- Démo d'infection
- Conclusion et pistes de solutions

Pourquoi contrôler l'intégrité ?

Intégrité : l'intégrité du système et de l'information traitée garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est à dire à la garantie de son origine et de sa destination. [IGI n°900].

Panorama du contrôle d'intégrité actuel

- **L'intégrité réseau**
  - Les checksums classiques (MD5/SHA,etc.) sont insuffisants
  - HMAC:

```
H(K XOR opad, H(K XOR ipad, text))
```

- **Au niveau système**
  - WPF, signature des modules kernel
  - Tripwire (& similaires)
  - Surveillance temps réel

Panorama du contrôle d'intégrité actuel

- **Pour les applis**
  - **Vérification de vraisemblance : La donnée est comparée a une donnée « vraisemblable » dans le contexte (plages de valeurs, seuils).**
  - **Contrôle de format : on vérifie que l'on est en présence d'un nombre à 6 chiffres, une chaîne de 10 caractères alphanumérique, un booléen, etc.**
  - **Principe des 4 yeux**

Les contraintes du contrôle en production

Dynamisme du système

- *les répertoires temporaires*
- *les queues de mails*
- *les caches applicatifs*

Gestion du changement

- Application des patchs
- Mise à jour de la base d'intégrité

Manipulation de la base d'intégrité

-Gestion de la base d'intégrité

- **Scellement**
- **Mise à jours, emplacement**

-Modification du contrôleur d'intégrité lui-même

Les différents vecteurs d'injection et la dissimulation

- ***Hooking Non volatile***

Injection

- **Kernel Hooking**
- **System-wide Windows Hooks**
- **Injection via la fonction CreateRemoteThread()**
- **Injection via la base de registre.**
  - HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Windows\AppInit_DLLs
- **Hook spécifiques à certaines applications**
  - BHO (browser helper object)
  - les applications MS Office.

Les différents vecteurs d'injection et la dissimulation

Hooking volatile

- Injection via la fonction CreateRemoteThread() sans Loadlibrary
  - *fnVirtualAllocEx*
  - *WriteProcessMemory*

- Interception en insérant des jmp.
- Modification de l'IAT

Les différents vecteurs d'injection et la dissimulation

Furtivité sur les I/O disques/registry/etc.

- *NtCreateFile (Cacher tout les fichiers créés par un processus particulier)*
- *ZwOpenFile (Renvoyer une erreur lorsque l'on tente d'ouvrir un fichier caché)*
- *ZwQueryDirectoryFile (cacher un fichier dans un répertoire)*
- *ZwOpenKey (renvoyer une erreur lors de l'ouverture d'une clé dans la base de registre)*
- *ZwQueryValueKey (Modifier le contenu d'une clé)*
- *ZwEnumerateKey (cacher des clés…)*

Hookings des IRP (I/O request packet)

Le risque résultant

« Doit-on réinstaller un serveur à chaque nouvelle vulnérabilité publique exploitable ? »

Critères de choix:

- *Existence d'un outil (ou pire d'un vers) permettant l'exploitation,*
- *Simplicité de son utilisation,*
- *Exposition de l'équipement (la machine est en frontal sur Internet, ou est située au fond d'un lan surprotégé),*
- *Durée de l'exposition de l'équipement*
- *D'autres équipements ont déjà été touchés (dans le même SI ou dans d'autres entreprises)*
- *L'absence ou la présence d'outils permettant de limiter les risques (stack non executable, un reverse proxy en frontal d'un web, un mécanisme d'Intelligence Applicative dans le firewall, une sonde de détection, etc.).*

Démo d'infection

Conclusion et pistes de solutions

- ***Un système ou une application peuvent difficilement s'autocontrôler.***

Pistes de solutions :

- Ne pas être vulnérable.
- L'outil d'intégrité peut ré implémenter la lecture des partitions (ntfs/fat/extfs) lui-même
- les protections empêchant la modification de l'exécution du noyau
- Détection des incohérences entre un fs accédé directement et les appels systèmes ou noyau

Contact

Cyril Leclerc

Ph. : +33 6 61 34 63 23

Mail : cleclerc@arseo.com

03 Juin 2005

SSTIC 2005

ARSeO

8 rue de Valmy

93100 Montreuil

France

www.arseo.com