

Supprimer des clés coriaces dans la base de registre

■ de [Aski](#) » 24 Fév 2009 12:34

Attention, réservé aux utilisateurs expérimentés

Certaines clés de la base de registre, non supprimées par des désinstallations mal programmées, ne peuvent pas être désinstallées par les moyens classiques. Il existe un moyen pour les détruire en lançant REGEDIT en mode SYSTEM. Pour prendre ces droits, on peut utiliser PSEXEC, un des utilitaires de la boîte à outils PSTOOLS de Microsoft. Cet utilitaire est décrit en détail dans [cet article](#).

Le problème s'est posé lorsque j'ai tenté vainement de supprimer une clé créée par Phantom CD et non détruite à la désinstallation. Cette clé était :

Code: [Tout sélectionner](#)

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_PHNTMBLT&
Prod_PHANTOM_CD&Rev_
```

J'ai pu tester cette méthode, sous Windows 7 de mon PC et sous Windows 7 installé sur une machine virtuelle.

La méthode consiste donc, avant la suppression proprement dite :

- à désactiver l'UAC si elle est activée, sans oublier de relancer le système
- à télécharger PSTOOLS comme indiqué ci-dessus et à le copier dans un dossier
- à en extraire PSEXEC et à le placer dans le dossier X désiré
- à lancer l'invite de commande en mode Administrateur
- à lancer REGEDIT depuis l'invite de commande, par

Code: [Tout sélectionner](#)

```
psexec -i -s regedit
```

Cordialement

Aski

PsExec v1.82

Par Mark Russinovich

Paru le 05 mars 2007

Introduction

Les utilitaires tels que Telnet et les programmes de contrôle à distance tels que PC Anywhere de Symantec vous permettent d'exécuter des programmes sur des systèmes distants, mais ils peuvent être difficiles à configurer et nécessitent que vous installiez le logiciel client sur les systèmes distants auxquels vous souhaitez accéder. PsExec est un substitut léger à Telnet qui vous permet d'exécuter des processus sur d'autres systèmes, avec une interactivité totale pour les applications de console, sans avoir à installer manuellement le logiciel client. Les utilisations de PsExec les plus puissantes incluent le lancement d'invites de commande interactives sur des systèmes distants et des outils activables à distance, tels qu'IpConfig qui sinon n'ont pas la possibilité d'afficher les informations sur les systèmes distants.

Remarque : certains logiciels d'analyse antivirus signalent qu'un ou plusieurs des outils sont infectés par un virus « d'administration à distance ». Aucun des outils PsTools ne contient de virus, mais ils ont été utilisés par des virus, c'est pourquoi ils déclenchent des notifications de virus.

Installation

Il vous suffit de copier PsExec sur votre chemin exécutable. La saisie de « Psexec » affiche sa syntaxe d'utilisation.

PsExec fonctionne sous Windows Vista, NT 4,0, Win2K, Windows XP et Server 2003 y compris les versions x64 de Windows.

Utilisation

Reportez-vous au numéro de juillet 2004 de Windows IL Pro Magazine pour l'[article de Mark](#) couvrant l'utilisation avancée de PsExec.

Utilisation : psexec [\\ordinateur[,ordinateur2[,...]] | @fichier][-u utilisateur [-p mot de passe]][-ns][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w répertoire][-d][-<priorité>][-a n,n,...] cmd [arguments]

ordinateur

Demande à PsExec d'exécuter l'application sur le ou les ordinateurs spécifiés. Si vous omettez le nom de l'ordinateur, PsExec exécute l'application sur le système local et si vous entrez un nom d'ordinateur semblable à « * », PsExec exécute les applications sur tous les ordinateurs du domaine actuel.

@file

Indique à PsExec d'exécuter la commande sur chaque ordinateur répertorié dans le fichier texte spécifié.

-a

Sépare les processeurs sur lesquels l'application peut s'exécuter avec des virgules, où 1 correspond au processeur avec le numéro le plus bas. Par exemple, pour exécuter l'application sur le processeur 2 et le processeur 4, tapez : « -a 2,4 »

-c

Copie le programme spécifié sur le système distant pour l'exécution. Si vous omettez cette option, l'application doit se trouver dans le chemin du système sur le système distant.

-d

N'attend pas que l'application se termine. Utilisez uniquement cette option pour les applications non interactives.

-e

Ne charge pas le profil du compte spécifié.

-f

Copie le programme spécifié sur le système distant même si le fichier existe déjà sur le système distant.

-i

Exécute le programme pour qu'il interagisse avec le bureau de la session spécifiée sur le système distant. Si aucune session n'est spécifiée, le processus s'exécute dans la session de console.

-l

Exécute le processus en tant qu'utilisateur limité (sans le groupe Administrateurs et autorise uniquement les privilèges attribués au groupe Utilisateurs). Sur Windows Vista, le processus s'exécute avec une intégrité faible.

-n

Spécifie l'expiration en secondes de la connexion aux ordinateurs distants.

-p

Spécifie le mot de passe en option pour le nom d'utilisateur. Si vous omettez ceci, vous serez invité à entrer un mot de passe masqué.

-s

Exécute le processus à distance dans le compte System.

-u

Spécifie le nom d'utilisateur facultatif pour se connecter à l'ordinateur distant.

-v

Copie le fichier spécifié uniquement s'il a un numéro de version plus élevé que celui sur le système distant.

-w

Détermine le répertoire de travail du processus (relatif à l'ordinateur distant).

-x

Affiche l'interface utilisateur sur le bureau Winlogon (système local uniquement).

-priority

Spécifie -Faible, -Inférieure à la normale, -Supérieure à la normale, -Élevé ou -Temps réel pour exécuter le processus à une priorité différente.

programme

Nom du programme à exécuter.

arguments

Les arguments à transmettre (notez que les chemins de fichiers doivent être des chemins absolus sur le système cible)

Vous pouvez inclure des applications avec des espaces dans leur nom en utilisant des guillemets par ex. "psexec \\marklap "c:\nom long\app.exe". L'entrée est uniquement transférée au système distant lorsque vous appuyez sur la touche Entrée et l'activation des touches Ctrl-C termine le processus distant.

Si vous omettez un nom d'utilisateur, le processus distant s'exécute dans le même compte que celui à partir duquel vous exécutez PsExec, mais étant donné que le processus distant n'est pas imité, il n'aura pas accès aux ressources réseau sur le système distant. Lorsque vous spécifiez un nom d'utilisateur, le processus distant s'exécute dans le compte spécifié, et aura accès à toutes les ressources réseau auxquelles le compte a accès. Notez que le mot de passe est transmis en texte non codé au système distant.

Vous pouvez utiliser la version actuelle de PsExec en tant que remplacement de Runas lorsque vous ciblez le système local étant donné que PsExec ne nécessite pas que vous soyez un administrateur.

↑ [Haut de page](#)

Exemples

Cet article que j'ai écrit décrit le fonctionnement de PsExec et fournit des conseils sur son utilisation :

<http://www.winnetmag.com/Windows/Issues/IssueID/714/Index.html>

La commande suivante lance une invite de commande interactive sur \marklap :

```
psexec \\marklap cmd
```

Cette commande exécute IpConfig sur le système distant avec le commutateur /all et affiche le résultat localement :

```
psexec \\marklap ipconfig /all
```

Cette commande copie le programme test.exe sur le système distant et l'exécute de manière interactive :

```
psexec \\marklap -c test.exe
```

Spécifiez le chemin complet à un programme qui est déjà installé sur un système distant s'il ne se trouve pas sur le chemin de système :

```
psexec \\marklap c:\bin\test.exe
```

Exécutez Regedit de manière interactive dans le compte System pour afficher le contenu des touches SAM et SECURITY :

```
psexec -i -d -s c:\windows\regedit.exe
```

Pour exécuter Internet Explorer avec des privilèges utilisateur limités, utilisez cette commande :

```
psexec -l -d "c:\program files\internet explorer\iexplore.exe"
```

↑ [Haut de page](#)

PsTools

PsExec fait partie d'un kit d'outils de ligne de commande Sysinternals en pleine croissance appelé *PsTools* aidant à la gestion des systèmes Windows NT/2K distants.



[Télécharger PsTools \(1 Mo\)](#)