



Présentation

SystemCleaner 1.1

6, cours Edith Piaf

77144 MONTEVRAIN

Tél. : 01 60 36 07 81

Mail: root@nolme.com

Site : <http://www.nolme.com>

Sommaire

| | <u>Pages</u> |
|---------------------------------|--------------|
| I. Introduction | 3 |
| II. Solutions existantes | 4 |
| III. Le logiciel | 6 |
| IV. But principal | 7 |
| V. Ses fonctionnalités | 8 |
| VI. La version de base | 9 |
| VII. La version professionnelle | 10 |
| VIII. Mise à jour du logiciel | 11 |
| IX. Son positionnement | 12 |
| X. Démonstration | 13 |

Introduction

- De plus en plus de virus et autres malwares 2.000 signatures par mois environ (source Symantec / Panda Software)
- Machines toujours plus lourdement infectées par des programmes toujours plus discrets et performants :
 - 700 malwares sur un ordinateur professionnel derrière un routeur, monté en Norton Internet Security 2003,
 - Démontage du disque dur pas toujours possible (ordinateur portable, garantie, etc.),
 - Disquette de secours de moins en moins utilisable du fait de l'absence de lecteur 3 1/2,
 - Première source d'appel Hot Line Dell (source PC Expert – janvier 2005)

Solutions existantes (1/2)

- Merijn Hijack This! 1.99
- Lavasoft AdAware SE 1.05
- Spybot – Search & Destroy 1.3
- Antispy 4
- Antispyware 1.0
- Spy Sweeper 3.2i
- Spykiller 2005
- Spysubtract 2.51
- X-Cleaner
- Xoftspy 3.45
- Panda Platinum Internet Security 8

Solutions existantes (2/2)

| | Editeur | Taux de reconnaissance | Taux d'éradication | Taux d'utilisation du processeur | Durée de l'analyse |
|------------------------------|------------------|------------------------|--------------------|----------------------------------|--------------------|
| | | % | % | % | min:sec |
| Ad-Aware SE | Lavasoft | 13,00 | 11,00 | 42,00 | 02:03 |
| Antispy 4 | Omniquad | 7,10 | 3,30 | 62,00 | 13:42 |
| Antispyware 1.0 | Mc Afee | 14,30 | 10,40 | 55,00 | 01:27 |
| Pestpatrol 4 | Pestpatrol | 52,00 | 44,20 | 40,00 | 03:34 |
| Platinum Internet Security 8 | Panda Software | 100,00 | 98,10 | 55,00 | 03:27 |
| Spy Sweeper 3.2i | Webroot | 64,90 | 60,40 | 16,00 | 01:53 |
| Spyboot Search & Destroy 1.3 | Patrick M. Kolla | 13,00 | 7,10 | 100,00 | 02:20 |
| Spykiller 2005 | Swanksoft | 14,90 | 6,50 | 100,00 | 02:48 |
| Spysubstract 2.51 | Intermute | 11,70 | 5,80 | 35,00 | 01:48 |
| X-Cleaner | Xblock.com | 16,20 | 13,00 | 50,00 | 03:00 |
| Xoftspy 3.45 | Paretologic | 13,00 | 2,00 | 100,00 | 01:26 |

légende :

| | |
|--|---------------------|
| | le moins performant |
| | le plus performant |

Source PC Expert – décembre 2004

Le logiciel

- Début du développement en avril 2004.
- Langage utilisé : C#.Net 2003.
- Mystification (« obfuscation ») du code : Xenocode 2005.
- Système d'exploitation : Microsoft Windows 98, Me, NT, 2000, XP, 2003, Longhorn.
- Langues : français / anglais.
- Taille : 4Mo.
- Pré-requis :
 - Microsoft .Net framework 1.1 ou ultérieur (22Mo), installé par défaut sur tout Windows à partir de Microsoft Windows 2003 Server.

But principal

- Accéder à la Base des Registres lorsque RegEdit ne peut-être lancé :
 - Exemple :
 - RegEdit terminé automatiquement par le ver Gaobot.
- Déceler les malwares résidents, rapidement, afin de pouvoir nettoyer le reste de l'ordinateur.
- Le logiciel évolue régulièrement afin de déceler les parasites les plus coriaces.

Ses fonctionnalités

- Analyse le système sous différents aspects et compare chaque fichier potentiellement dangereux avec sa base de signatures (125.000).
- 23 langues de Microsoft Windows reconnues :
 - Français, anglais, arabe, brésilien, chinois, tchèque, danois, allemand, espagnol, finlandais, grecque, hébreu, hongrois, italien, japonais, coréen, hollandais, norvégien, polonais, portugais, russe, suédois, turc.
- Microsoft Windows 98, Me, 2000, XP, 2003, NT4.

La version de base

- Zones analysées :
 - Base des Registres et les différentes options de lancement d'un programme,
 - Menu Démarrer,
 - Processus en mémoire,
 - Threads en mémoire,
 - Service Systèmes
 - Différents dossiers Systèmes,
 - Internet Explorer :
 - BHO : Browser Helper Object
 - DPF : Downloaded Program File
 - Barre d'outils
 - Boutons
 - Cookies Internet Explorer (Firefox / Mozilla en-cours de développement)

La version professionnelle

- Zones analysées :
 - Idem que la version de base,
 - Analyse des fichiers systèmes :
 - Hosts,
 - Win.ini
 - System.ini
 - Autoexec.bat
 - Config.sys,
 - Winnt.ini
 - Copie et isolement des fichiers
 - Analyse du disque dur complet
 - Analyse de la Base des Registres
 - Suppression multiple de processus, entrées dans le Registre, etc.,

Mise à jour du logiciel

- Mise à jour via Internet plusieurs fois par semaine.
- La base de données, comme pour tout antivirus, accuse toujours un léger retard du fait du temps d'apprentissage des nouvelles signatures.
- Par contre, sa reconnaissance poussées des éléments validés, qui eux varient moins souvent, permet par déduction de trouver les nouveaux parasites.

Son positionnement

- <http://www.nolme.com/logiciels.htm>
- <http://www.softpedia.com/get/Internet/Popup-Ad-Spyware-Blockers/SystemCleaner.shtml>
- http://www.echu.org/portail/modules/newbb/viewtopic.php?topic_id=137&forum=3&viewmode=flat&order=ASC&start=5
- <http://www.01net.com/telecharger/windows/Utilitaire/systeme/fiches/31338.html>

Démonstration

- SystemCleaner 1.1, exemple :

The screenshot displays the SystemCleaner application interface. The left pane shows the Windows Registry tree, with the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` selected. The right pane shows the properties of the file `c:\program files\chiers communs\cmeii\cmesys.exe`.

| Propriétés | Valeurs |
|-------------------------------|---|
| Informations générales | |
| Clé | SOFTWARE\Microsoft\Windows\CurrentVersion\Run |
| Sous-clé | CME Sys |
| Valeur | "C:\Program Files\Fichiers communs\CMEII\CME Sys.exe" |
| Fichier extrait | c:\program files\chiers communs\cmeii\cmesys.exe |
| Arguments extraits | |
| Fichier | |
| Emplacement | c:\program files\chiers communs\cmeii\cmesys.exe |
| Taille du fichier | 90 112 octets |
| Date de création | 16/02/2005 23:59:04 |
| Date de dernier accès | 10/04/2005 00:33:50 |
| Dernière écriture | 16/02/2005 23:59:04 |
| Produit | CME |
| Version | 7.1.0.6 |
| Editeur | 'GAIN Publishing' |
| Description | CME II Client Application |
| Version du fichier | 7.1.0.6 |
| Langue | Anglais (États-Unis) |
| Copyright | Copyright © 1999-2005 GAIN Publishing |
| Attributs | Archive |
| Base de données | |
| Editeur | GAIN Publishing |
| Description | - |
| Nom de l'application | CME II Client Application |
| Niveau de risque | risque moyen |
| Empreinte numérique | |
| MD5 trouvée | C44878D8BB5428C8AC2E5F089CBB1F5D |