Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 08 janvier 2001
N° CERTA-2001-INF-001

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Surveillance avec spector

Gestion du document

Référence	CERTA-2001-INF-001
Titre	Surveillance avec spector
Date de la première version	08 janvier 2001
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

– vol de mots de passe, ... ;
– surveillance de l'activité à l'insu des utilisateurs.

2 Systèmes affectés

Windows

3 Résumé

`spector` est un logiciel qui enregistre l'activité d'un utilisateur à son insu sous la forme d'une succession de copie d'écran. Il peut aussi intercepter ce qui est frappé au clavier.

4 Description

Une *industrie de la méfiance* se répand de plus en plus. Cette industrie fait le commerce de différents outils destinés à pratiquer la surveillance des individus. Un discours malsain est utilisé pour justifier ce commerce :

les individus sont par nature malveillants, il faut donc les surveiller pour les empêcher de nuire. En particulier, l'époux ou l'épouse trompe son conjoint, la baby sitter maltraite les enfants qu'on lui confie, le futur gendre est probablement un repris de justice, si ce n'est pas un dangereux toxicomane, les internautes en veulent aux enfants, les employés profitent de toutes les occasions pour gaspiller le temps qu'ils sont censés occuper à travailler pour faire des activités à la limite de la légalité... Il serait donc nécessaire, parce que justifié par la menace omniprésente, de tout entreprendre pour surveiller ces personnes. Les publicités s'appuient sur les témoignages de personnes décrivant des anecdotes plus horribles les unes que les autres qui auraient pu (nous dit-on) être évitées si toutefois elles avaient été dotées des outils vendus par cette industrie.

Outre le discours discutable sur la nature humaine que développe cette industrie qui pousse tout le monde à se surveiller mutuellement, outre l'aspect naïf qui consiste à imaginer qu'un logiciel sauvera un couple, protégera les enfants ou identifiera les paresseux, *l'utilisation d'un outil de surveillance à l'insu des personnes surveillées est illégale en France*.

Cette note d'information décrit comment découvrir si l'on fait l'objet d'une surveillance menée par le moyen de l'outil `spector`.

`spector` est un des outils vendus par la société `SpectorSoft`. Cet outil fonctionne dans un environnement Windows et enregistre l'activité de l'utilisateur sous la forme de copies d'écran prises à intervalle régulier. Par ailleurs, il serait possible de demander l'interception de séquences de touches frappées au clavier. Cette dernière fonctionnalité permet notamment à un pirate d'obtenir les mots de passe, numéro de carte bleue, texte de documents confidentiels, ...

Cet outil peut être installé de sorte à être *furtif*, c'est à dire difficile à détecter. Dans ce cas, il n'y a pas d'icône, les fichiers sont cachés et portent des noms relativement anodins pouvant laisser penser à des composants légitimes de Windows.

Curieusement cet outil ne semble pas être détecté par certains antivirus.

Ce programme tourne sous la forme d'un service sous le nom `mswnsrvx.exe`. Sa configuration est située dans le fichier `C:\WINNT\mswnsrvx.INI`. Les journaux enregistrant l'activité de l'utilisateur sont rangés dans le répertoire `C:\WINNT\System32\WebExt` sous la forme de fichiers à l'extension `.TPS`. On trouve aussi les fichiers :

- `C:\WINNT\System32\mswnsrvx.gid`
- `C:\WINNT\System32\WebExt\mswebext.ocx`
- `C:\WINNT\System32\WebExt\_MSFILEA.TXT`

Suivant l'installation on peut aussi trouver les fichiers suivants :

- `C:\WINNT\Profiles\All Users\Start Menu\Programs\Spector`

Ces fichiers et répertoires sont cachés. Par défaut, ils ne sont pas affichés par l'explorateur de fichiers sauf si l'option « afficher les fichiers cachés » est activée.

Le logiciel `Spector` définit aussi quelques entrées dans la base de registre :

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\systrayex`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersionRun\_systray`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersionRun\sysbot`
- `HKLM\SOFTWARE\SpectorSoft`
- `HKLM\SOFTWARE\SpectorSoft\Spector`
- `HKLM\SOFTWARE\SpectorSoft\Spector\MSExplorerBitmap`

Une séquence de touches permet de faire apparaître la fenêtre de configuration de `spector`. Par défaut cette séquence de touche est `CTRL+ALT+SHIFT+S`. Cependant cette séquence de touche est configurable.

Les enregistrements de l'activité sur la machine sont par défaut dans le répertoire `C:\WINNT\System32\WebExt`. On peut configurer `spector` pour qu'il utilise un autre répertoire.

Les fichiers d'enregistrement de l'activité ont par défaut l'extension `.TPS`. On peut configurer `spector` pour qu'il utilise une autre extension.

La configuration permet de modifier d'autres paramètres comme l'intervalle de temps entre deux copies d'écrans.

5 Solution

La façon la plus propre de retirer ce cheval de Troie est de lui demander de se désinstaller lui-même. Ceci n'est possible que si l'on connaît la séquence de touches permettant d'appeler l'interface utilisateur de `spector` (par défaut `CTRL+ALT+SHIFT+S`). La procédure à suivre est la suivante :

1° taper la séquence de touches (par défaut `CTRL+ALT+SHIFT+S`) ;
2° une fenêtre de configuration s'affiche ;
3° choisir par le menu l'option `File->Unistall spector` ;
4° redémarrer la machine ;
5° si l'exécutable `mswnsrvx.exe` existe encore cliquer dessus et reprendre à l'étape 2.

Il existe quelques produits qui offrent de désinstaller `spector`. Aucun de ces produits n'est diffusé avec ses sources, si bien qu'il est difficile de se faire une idée de leur inocuité.

La façon manuelle pour supprimer ce logiciel est :

1° effacer le fichier `C:\WINNT\System32\mswnsrvx.exe` ;
2° redémarrer la machine (pour vider la mémoire si toutefois ce logiciel était en train de tourner) ;
3° effacer les fichiers `.TPS` générés par `spector`. (La conservation d'une interception de l'activité d'un utilisateur à son insu est interdite).

Gestion détaillée du document

08 janvier 2001 version initiale.