Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 8 septembre 2000
N° CERTA-2000-ALE-012

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Mauvaise compatibilité des scanners de virus avec NTFS

Gestion du document

Référence	CERTA-2000-ALE-012
Titre	Mauvaise compatibilité des scanners de virus avec NTFS
Date de la première version	08 septembre 2000
Date de la dernière version	–
Source(s)	Avis du CERT-IST Sophos NAI F-Secure
Pièce(s) jointe(s)	Aucune

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

1 Risque

Prolifération de virus non détectés par les analyseurs antivirus.

2 Systèmes affectés

Windows NT et 2000 utilisant le système de fichiers NTFS.

3 Résumé

Le système de fichier NTFS permet de créer des Flux de Données Additionnels (Alternate Data Streams) associés ou non à un fichier. Il a été relevé dès 1998 que cela permettait de dissimuler de l'information pour 2 raisons essentielles :

– Cette fonctionnalité est très mal documentée par Microsoft et peu d'administrateurs la connaisse,
– Beaucoup d'outils de Windows n'ont même pas la capacité de gérer ces flux.

C'est ainsi que la commande *dir* ou l'*explorateur* de Windows ne sont pas capables de les afficher, ni même d'indiquer le changement de taille d'un fichier auquel on aurait adjoint un flux additionnel.

Les analyseurs antivirus n'échappaient jusqu'alors pas à la règle, et ne recherchaient donc pas de signatures caractéristiques dissimulées dans un flux additionnel.

Un premier virus est apparu sous Windows 2000 : *Win2K.Stream*, *Win2k_Stream* ou simplement *Stream*. Ce n'est qu'une version expérimentale qui n'est pas nocive aujourd'hui. Cependant il faut noter qu'il est apparu seulement quelques jours après une alerte du "SANS Institute" expliquant le danger potentiel des flux additionnels pour les antivirus.

4 Description

L'ensemble du système de fichier NTFS est géré comme une base de données relationnelle composée uniquement de fichiers. Chaque fichier a une liste d'attributs (nom de fichier, descripteur de sécurité, données,...) de longueur variable. Tout fichier accepte de nouveaux attributs caractérisés par leur nom. Un attribut est divisé en 2 parties : l'entête et le contenu, ce dernier étant composé du nom de l'attribut et d'un flux de données.

Un flux de données addtionnel peut donc être créé par la simple ligne de commande *echo "Test de flux de données addtionnel" >fichier_existant:flux1.txt*, où *fichier_existant* est un fichier présent dans le répertoire courant (on ajoute un nouvel attribut de nom *flux1.txt* au fichier *fichier_existant*). Ni la commande *dir* ni l'*explorateur de fichiers* ne révèlent son existence. Il peut en revanche être ouvert par la commande *notepad fichier_existant:flux1.txt*. D'autres flux additionnels peuvent évidemment être ajoutés. La commande *del*, incompatible, n'est pas en mesure de les supprimer. Cependant un tel flux est inerte, il ne peut être directement exécuté.

Dans l'optique d'une utilisation malicieuse, cette restriction peut être facilement contournée : l'essentiel du code du virus est masqué dans un flux additionnel, et il est simplement appelé par un code minimal depuis le flux "normal" (script vba sous Word, scriptlet vbs, modification d'un exécutable,...). Le peu de code qui estalors visible par les antivirus ne permet pas de générer une signature : il est trop peu caractéristique pour ne pas générer de nombreuses fausses alarmes.

5 Solution

Depuis la publication du bulletin du "SANS Institute" et l'apparition du virus *Stream,* il est impératif que les éditeurs d'antivirus rendent les moteurs d'analyse compatibles avec les flux de données additionnels.

Il est donc essentiel de mettre à jour les bases de signature de vos antivirus (détection de *Stream*), de prendre contact avec vos éditeurs pour connaître les modalités d'évolution des moteurs d'analyse (achat, mise à jour,...) et de prendre en compte dès aujourd'hui le déploiement.

6 Documentation

- Copie du bulletin d'alerte du "SANS Institute" :
  http://securityportal.com/topnews/sans20000907.html
- Analyse de Stream par F-Secure :
  http://www.datafellows.fi/v-descs/w2kstrm.htm
- Analyse de Stream par Symantec :
  http://www.symantec.com/avcenter/venc/data/w2k.stream.html
- Analyse de Stream par Sophos :
  http://www.sophos.com/virusinfo/analyses/w2kstreams.html
- Analyse de Stream par NAI :
  http://vil.nai.com/villib/dispvirus.asp?virus_k=98803

Gestion détaillée du document

08 septembre 2000 version initiale.