

VIRUSCAN 7.0 SE DOPE À L'EPO

LEGALIZE IT !

CHRISTIAN.RAEMY@epfl.ch, SIC



ePO, derrière cette abréviation, propulsée sous les feux de la rampe dans certains milieux sportifs, se cache également un mécanisme de contrôle et mise à jour automatique de votre programme anti-virus du célèbre McAfee, appelé: **ePolicy Orchestrator**.

Vous allez découvrir dans cet article pourquoi la solution McAfee VirusScan 7.0 Entreprise et l'agent ePO

nisme d'arrêt de tout moyen de protection installé sur la machine infectée (Anti-virus connus, Firewall, etc.). A ce jour, l'agent ePO n'est pas sensible à ce mécanisme d'arrêt.

Sachant que quelques dizaines de nouveaux virus, plus ou moins virulents, apparaissent toutes les semai-



vont vous protéger très efficacement contre ce fléau que sont les virus.

Tel un chef d'orchestre dopant votre anti-virus, ePO contrôle et paramètre celui-ci pour le maintenir le plus à jour possible, sans aucune intervention de votre part. Mais pour quelle raison me direz-vous ?

Dans un grand pourcentage de cas, les anti-virus installés ne sont presque jamais mis à jour ou pas au bon moment. En outre, et ceci depuis quelques mois déjà, une grande partie des nouveaux virus incluent un méca-

nes, **on peut facilement dire qu'un anti-virus, sans mise à jour depuis seulement 2 mois, est quasiment inutile !**

Ces mises à jour peuvent toucher quatre composants essentiels de votre mécanisme de protection des virus:

- Le programme en lui-même (**Hotfix**, corrections de bugs, améliorations diverses), avec une fréquence d'environ 1an;

SUITE EN PAGE 15

SOMMAIRE FI 6/2003

- 1 VirusScan 7.0 se dope à l'ePO
- 2 Arrêt du cache WWW
- 2 sic-info
- 3 SWITCHmobile – Loin des yeux, près du cœur
- 6 Service de backup centralisé
- 8 Simulation de robots mobiles
- 11 ERIDAN – PBS
- 17 Performances des infrastructures Web – WebStressing
- 19 L'information indexée – Méta-données et Dublin Core
- 21 Programme des cours
- 25 Le CERN accélère la transmission de ses informations
- 28 Le projet ForAll ou l'analyse d'images au service de la mode
- 32 en bref

PROCHAINES PARUTIONS

	délaI RÉDACTION	PARUTION
SP	27.06.03	26.08.03
7	04.09.03	26.09.03
8	02.10.03	21.10.03
9	30.10.03	18.11.03
10	27.11.03	16.12.03

SUITE DE LA PREMIÈRE PAGE

- Le moteur ou *engine* (améliorations des méthodes de recherche des virus, les moyens de nettoyage, nouveaux types d'analyses), fréquence d'environ 6 mois;
- Le type d'extension des documents potentiellement vulnérables (*.exe, *.com, ...), fréquence d'environ 3 mois;
- La librairie de signatures (liste continuellement mise à jour permettant de confondre ces méchants bouts de code nuisants à votre machine), fréquence ≤ 1 semaine.

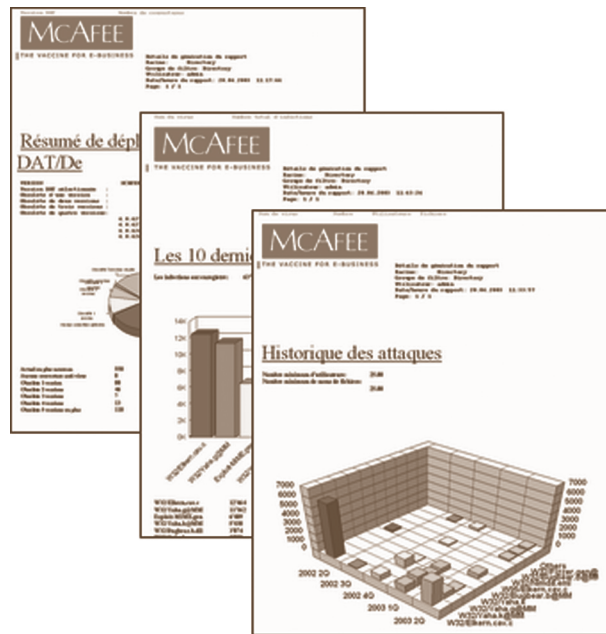
Les personnes les plus zélées, ont, je l'espère, paramétré une mise à jour de la librairie, via le site McAfee (NAI) et automatisé cette tâche. C'est un bon début mais ceci n'offre pas une protection optimale.

EN QUOI ePO PEUT-IL AMÉLIORER CETTE SITUATION ?

ePO est composé d'un serveur centralisé (actuellement au SIC, gérant toute l'EPFL) qui comporte sa propre base de données SQL ainsi que de clients (laptops, desktops ou serveurs) qui ont un agent client installé en tant que service Windows. Cet agent ePO va effectuer, à intervalles réguliers, plusieurs actions:

- Contacter le serveur central pour rapatrier les paramètres, les tâches et les installations de nouveaux produits à effectuer.
- Contrôler et appliquer les paramètres des produits McAfee présents sur la machine cliente.

- Effectuer les différentes mises à jours programmées dans le planning reçu du serveur.
- Centraliser toutes les alertes et détections de virus dans la base SQL du serveur.



L'agent est robuste (monté comme un service), ne demande pas d'intervention de la part de l'utilisateur, n'occupe que très peu de ressources système, transmet tous les changements

de configurations du poste au niveau IP, nom, domaine et peut très bien être intégré à une image de *postmaster* dans la cas d'un déploiement d'une salle de PC.

En outre, dans le cas où le serveur devait être inatteignable (crash, migration, ...) l'agent continuera à appliquer les derniers paramètres et les tâches reçus depuis sa dernière connexion avec le serveur. **La mise hors service du serveur ne met en aucun cas, en péril la mise à jour des anti-virus des clients.**

Le serveur est administré à distance, via une console de commande MMC à installer sur un ou des postes d'administration. Il regroupe plusieurs informations:

- la liste de toutes les machines clientes avec leurs caractéristiques (IP, RAM, OS...);
- propriétés et configurations des différents produits McAfee;
- package d'installation à distance des produits McAfee;
- tâches et planning à effectuer par les agents clients;
- gestion des chemins réseaux pour la mise à jour des clients;
- une multitude de rapports sur le parc de machines et sur les infections subies;
- la possibilité d'envoyer un réveil des agents pour déployer un patch ou une signature de manière urgente.

Les machines clientes du serveur ePO sont classées dans des groupes et c'est sur ces groupes que les différentes configurations et tâches sont attribuées. A l'EPFL, la structure des différents groupes de machines est volontairement calquée sur la représentation de l'Active Directory (AD).

Toutes les machines ne faisant pas encore partie de la forêt AD de l'EPFL sont mises dans un groupe spécifique (Zautres).

Si besoin est, des sous-groupes peuvent être créés et gérés par des administrateurs d'instituts ou de labo. Cette option n'est utile que si les machines appartenant à ces sous-groupes doivent recevoir des paramètres ou tâches différentes de leur groupe parent.

La communication entre l'agent et le serveur est établie par l'agent lui-même, à une fréquence définie et, bien évidemment, celle-ci est cryptée au moyen de clé publique / clé privée pour être à l'abri d'un mécanisme hostile perturbant ou usurpant la communication.

EN PRATIQUE, DEUX CAS S'OFFRENT À VOUS SELON VOTRE STATUT

VOUS ÊTES UN ADMINISTRATEUR EN CHARGE D'UN GROUPE DE MACHINES WINDOWS:

Dans ce cas, suite à une petite formation d'une demi-journée et à l'installation sur un de vos postes d'administration de la console de management d'ePO, vous serez en mesure de déployer VirusScan sur la totalité de votre parc de machines, d'ajouter des tâches de contrôle, d'avoir une vision globale de votre protection virale grâce aux multiples rapports offerts par ePO.

La procédure se trouve ici: <http://winsec.epfl.ch>

VOUS ÊTES UN UTILISATEUR NE FAISANT PAS PARTIE DE L'AD ET SANS ADMINISTRATEUR

Commandez alors simplement l'agent ePO dans DistriLog, installez-le et vous serez automatiquement ajouté au serveur, dans le groupe réservé aux machines hors AD.

Vous recevrez alors, de manière automatique l'installation du dernier VirusScan 7.0, paramétré et mis à jour quotidiennement.

En cas d'attaque, votre anti-virus recevra automatiquement la mise à jour urgente, déployée de manière centralisée et ceci sans intervention de votre part.

A l'heure actuelle, la totalité des machines gérées par les services centraux (SCX) sont protégées par ce système. Si vous ne savez pas si votre machine est déjà protégée grâce à ePO, contactez votre administrateur informatique qui vous renseignera volontiers.

Finalement, je ne saurais donc que vous encourager vivement à opter pour cette solution qui me paraît être la



meilleure protection anti-virale à ce jour afin de diminuer drastiquement les risques de contamination globale du site de l'EPFL et les conséquences désastreuses qui en découleraient. La bataille n'est pas terminée mais nous disposerons alors, d'un outil efficace pour ce combat de plus en plus d'actualité.

REMARQUE:

Vu la rapidité de propagation des virus récents et la vitesse avec laquelle il est nécessaire de réagir, il devient impératif, pour minimiser les risques d'infections, de déployer au maximum cet agent offrant des moyens de réaction rapide sur la globalité des machines Windows de l'EPFL. C'est dans cette optique qu'il ne sera pas proposé de version autonome de McAfee VirusScan 7.0, mais uniquement conjointe avec l'installation de l'agent ePO. Le team agent ePO et VirusScan 7.0 offrant actuellement la meilleure réponse en terme de protection contre les virus. ■