

PROCEDURE			N° :		
			Créée le :	16/02/2018	
Incident antivirus février 2018 <i>(Postes administratifs EPLE)</i>			Rédacteur :	DSI	
			Nb pages :	5	
			Diffusion :	Restreinte	
Mise à jour	16/02/2018	Par :	DSI	Version :	1

Objet : Résolution d'un incident lié à l'antivirus *Trend Micro OfficeScan*.

Le 13/02/2018, le déploiement d'une sous-version de l'antivirus OfficeScan XG assurant la protection des postes administratifs en EPLE a généré des dysfonctionnements impactant plusieurs applications.

La stratégie de sécurité mise en œuvre bloque en effet le fonctionnement de :

- GFC
- PRESTO
- Outlook
- Sagesse
- TurboSelf
- etc.

À ce stade, la liste des applications impactées n'est pas exhaustive.

L'utilisateur sera amené dans la procédure qui suit à exécuter un outil visant à appliquer un paramétrage spécifique du client antivirus académique.

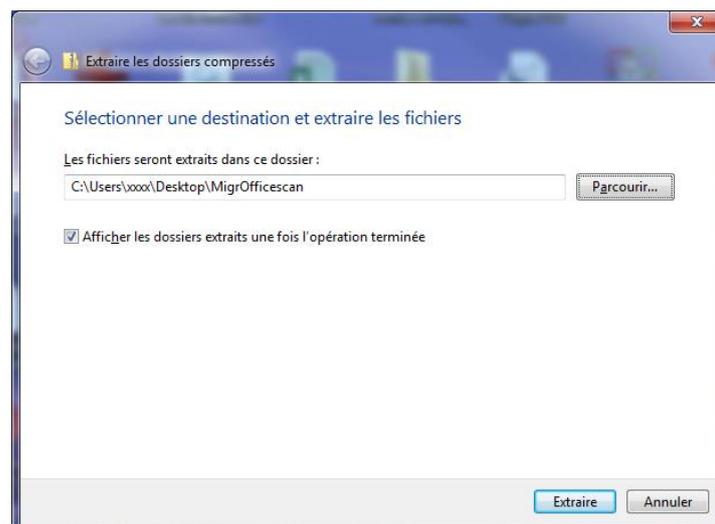
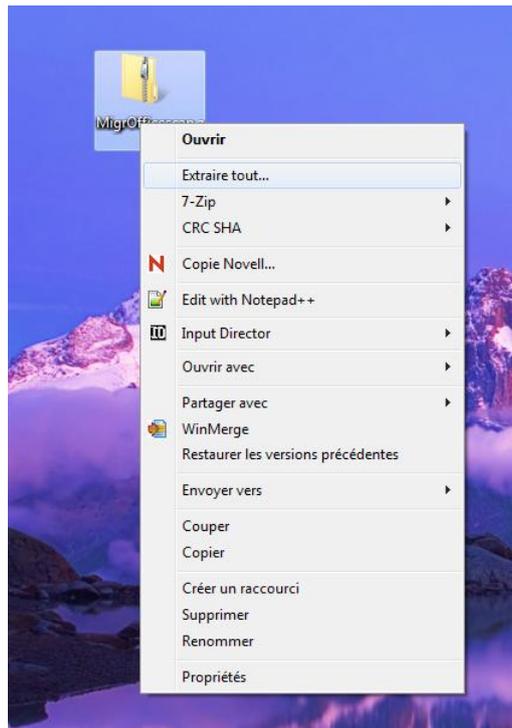
Durée estimée de la procédure: 5min

1. Télécharger l'archive du programme de mise à jour

<http://cecoiawiki.ac-creteil.fr/wiki/images/1/18/MigrOfficescan.zip>

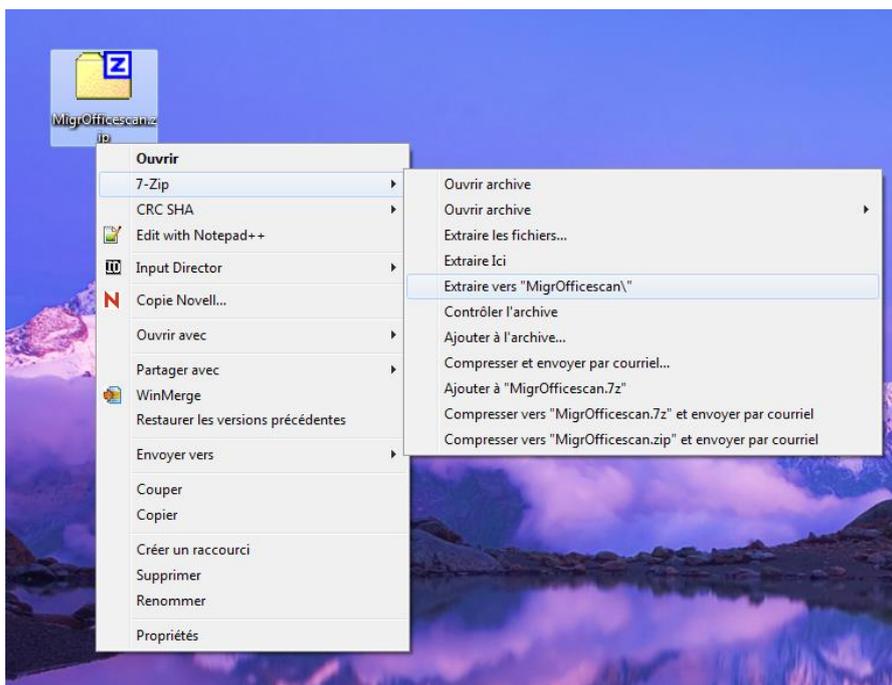
2. Décompresser l'archive

Clic droit sur le fichier puis extraire tout



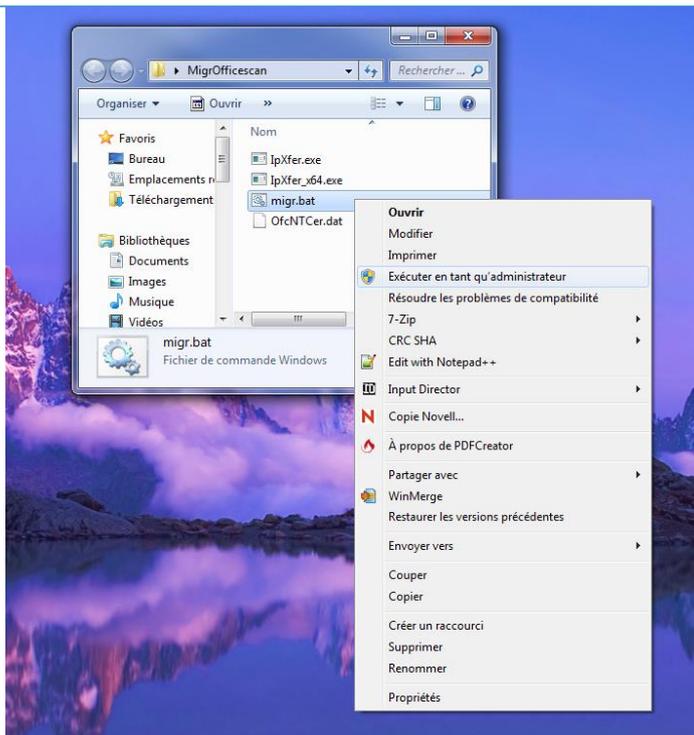
Ou si 7-zip installé

clic droit sur le fichier : puis Z-zip > extraire vers « MigrOfficescan\ »



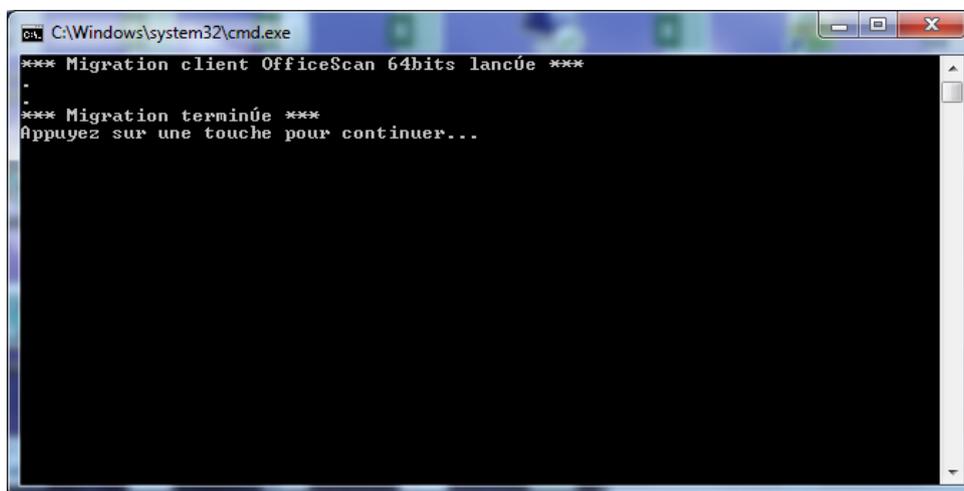
3. Exécution du correctif

Dans le dossier «MigrOfficescan » créé lors de la décompression, cliquer droit sur le fichier migr.bat puis sélectionner « **exécuter en tant qu'administrateur** ».



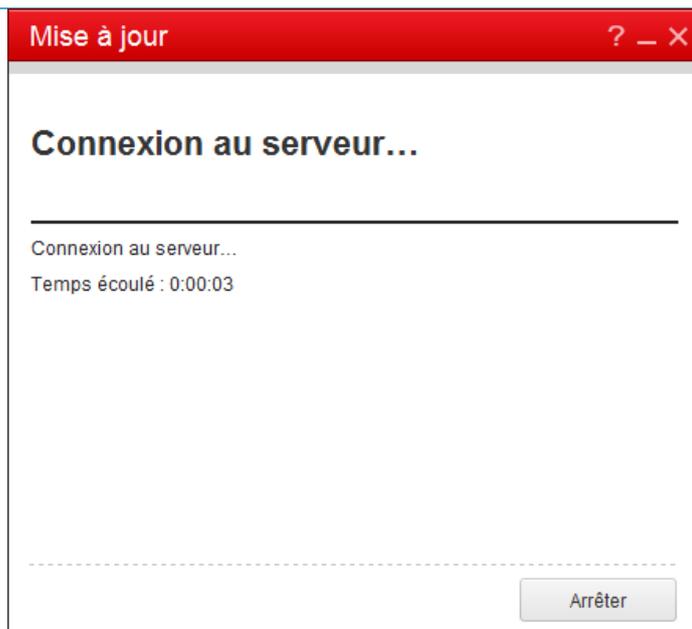
Le programme se lance dans une fenêtre.

Il faut attendre que le message « **Appuyez sur une touche...** » apparaisse.

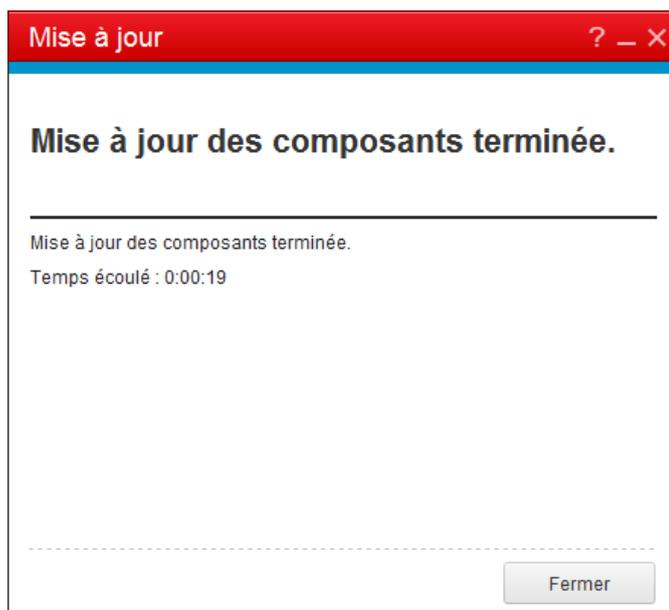


Important : le client antivirus se décharge et un message signalant qu'il est désactivé pourrait apparaître. L'icône bleue dans la barre des tâches passe en rouge puis disparaît momentanément le temps de la prise en compte de la nouvelle connexion. Puis il réapparaît en bleu.

Afin de vérifier la descente des autorisations pour GFC, Presto et autres vous pouvez lancer une mise à jour immédiate en cliquant droit sur l'icône bleue, puis sélectionner « **mettre à jour** ».



Vous devez aboutir au message suivant : « **Mise à jour des composants terminée** »



Tester les applications.

La procédure est terminée.