

## eole-fichier - Scénario #14880

### Whitelister les outils Eole/Windows dans scannedonly

02/02/2016 16:52 - Klaas TJEBBES

<b>Statut:</b>	Terminé (Sprint)	<b>Début:</b>	16/02/2016
<b>Priorité:</b>	Normal	<b>Echéance:</b>	04/03/2016
<b>Assigné à:</b>	force verte	<b>% réalisé:</b>	100%
<b>Catégorie:</b>		<b>Temps estimé:</b>	0.00 heure
<b>Version cible:</b>	sprint 2016 07-09 - Equipe MENESR	<b>Temps passé:</b>	1.50 heure
<b>Description</b>			
Pour éviter que Clamav/scannedonly ne détecte cliscribe-setup.exe, joineole.exe et autres comme des virus, on pourrait les ajouter comme fichiers à exclure du scan.			
Pour ce faire, créer un fichier <b>/etc/default/scannedonly</b> contenant :			
<pre>DAEMON_ARGS="--exclude (/home/[a-z]/[a-z]+/perso /home/client_scribe)/client/(cliscribe-setup.exe cliscribe-updater-setup.exe) /home/a/admin/perso/IntegrDom/joineole.exe"</pre>			
<b>Sous-tâches:</b>			
Tâche # 15041: Réactivation du template de configuration scannedonly			<b>Fermé</b>
<b>Demandes liées:</b>			
Lié à eole-antivirus - Proposition Scénario #14994: ACTION EAD3 : pouvoir ajo...			<b>Classée sans suite</b>

### Historique

#### #1 - 04/02/2016 14:30 - Klaas TJEBBES

Clamav utilise deux bases de données :

1. une base appelée **local.fp** située dans **/var/lib/clamav/** . Elle contient la signature MD5, la taille et le nom du fichier.
2. une autre base appelée **local.ign2** située dans **/var/lib/clamav/** . Elle contient seulement le nom du fichier.

Nous prendrons pour exemple le fichier **MSRA-TLPU176.exe** :

1 - La première chose à faire est de créer une signature pour le fichier en question :

```
root@srv-scribe # sigtool --md5 /chemin_du_fichier/MSRA-TLPU176.exe >> /var/lib/clamav/local.fp
```

2 - Il faut ensuite renseigner la base local.ign2 avec la commande :

```
root@srv-scribe # echo 'MSRA-TLP176.exe' >> /var/lib/clamav/local.ign2
```

On peut bien entendu exécuter les 2 commandes en même temps :

```
root@srv-scribe # sigtool --md5 /chemin_du_fichier/MSRA-TLPU176.exe >> /var/lib/clamav/local.fp && echo 'MSRA-TLP176.exe' >> /var/lib/clamav/local.ign2
```

Au prochain scan, Clamav devrait considérer les fichiers comme non vérolés et ne pas les déplacer dans **/var/virus**.

Si le fichier avait déjà été déplacé par Clamav, exécuter en premier la commande suivante pour déplacer le fichier du dossier **.var/virus** vers son dossier d'origine :

```
mv /var/virus/MSRA-TLPU176.exe /home/workgroups/commun/logiciels/
```

**#2 - 12/02/2016 15:39 - Scrum Master**

- Tracker changé de Proposition Scénario à Scénario
- Echéance mis à 04/03/2016
- Version cible mis à sprint 2016 07-09 - Equipe MENESR
- Release mis à EOLE 2.5.2
- Points de scénarios mis à 3.0

**#3 - 12/02/2016 15:43 - Joël Cuissinat**

- Assigné à mis à force verte

**#4 - 16/02/2016 10:11 - Daniel Dehennin**

- Projet changé de Scribe à eole-fichier

**#5 - 16/02/2016 11:02 - Daniel Dehennin**

Paquet 2.5.2 compilé et branches de backport poussées mais non intégrées.

**#6 - 18/02/2016 09:38 - Scrum Master**

- Statut changé de Nouveau à Terminé (Sprint)