Windows Vista/Seven : RogueKiller en invite de commandes en mode sans échec

Une des solutions pour les virus gendarmerie/Ukash/Hadopi est l'utilisation de RogueKiller en invite de commandes en mode sans échec.
Cela peux être utile si l'invite de commandes en mode sans échec est disponible et, si par exemple, la restauration du système ne fonctionne pas.

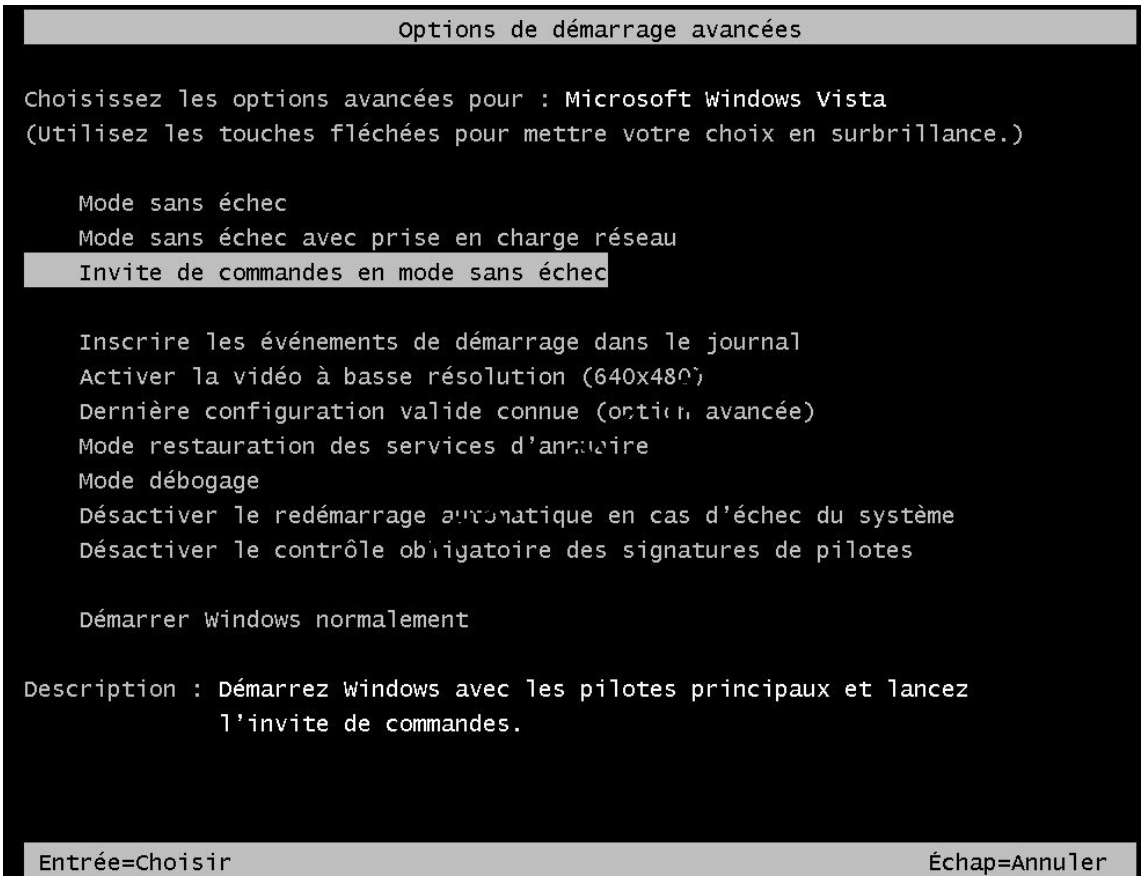
Pour cela, prenez une clef USB et téléchargez RogueKiller dessus : http://www.sur-la-toile.com/RogueKiller/
Le téléchargement de RogueKiller se fait à partir des icônes ci-dessous.

Téléchargement de RogueKiller

Une fois RogueKiller sur la clef USB, insérez la clef USB dans le PC infecté puis démarrez le PC infecté en invite de commandes en mode sans échec.

Pour cela :

Redémarrez l'ordinateur, avant le logo Windows, tapotez sur la touche F8,
Un menu va apparaître, choisissez **invite de commandes en mode sans échec**
Appuyez sur la touche entrée du clavier.

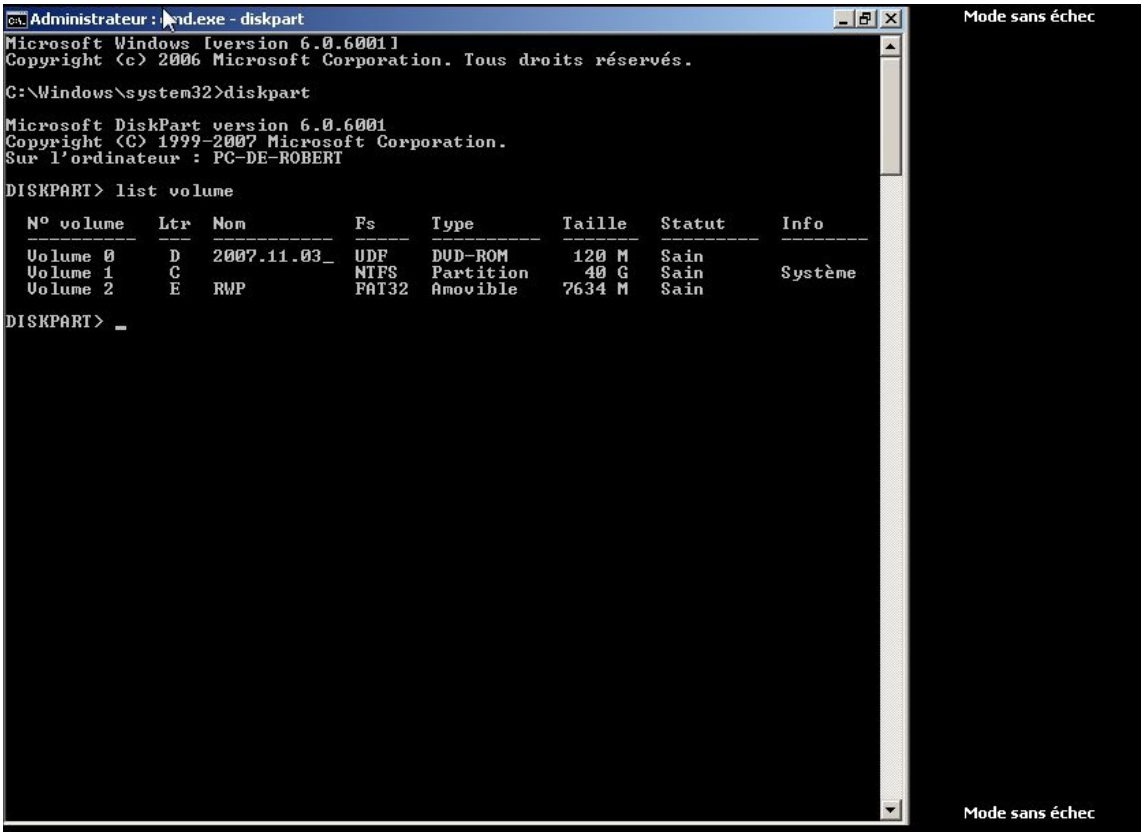


Un rappel rapide du fonctionnement de l'invite de commandes pour une meilleur compréhension.
Lorsque vous arrivez sur l'invite de commandes en mode sans échec, vous devez avoir C:/Windows/system32>
Cela indique que vous êtes dans le répertoire system32

Le but du jeu est donc d'aller sur la clef USB.
Pour changer de lecteur, il faut taper lettre: et appuyer sur entrée
Par exemple, si on veux aller sur le lecteur D, il faut taper d: et entrée

Si vous ne connaissez pas la lettre de votre USB, tapez **diskpart**
Une fois dans diskpart, saisir : **list volume**

Dans la capture ci-dessous, on peux voir comme type Amobile le lecteur E
La lettre de la clef USB est donc E.



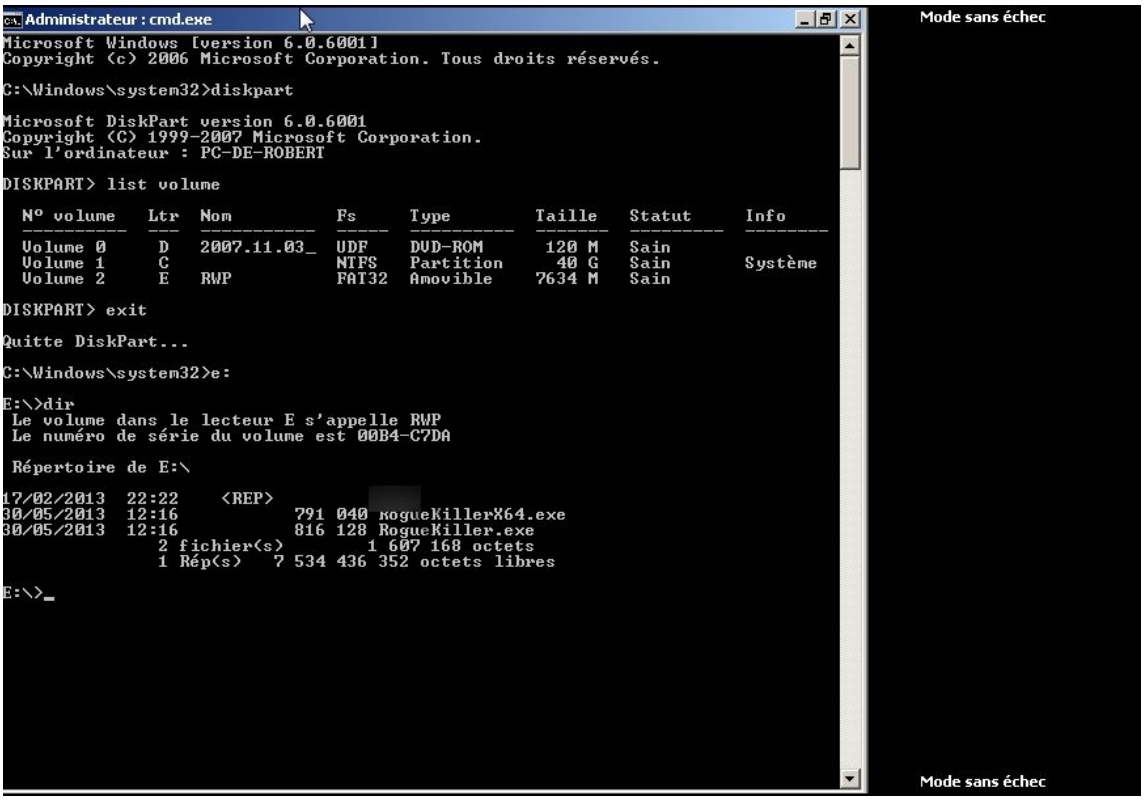
tapez exit pour quitter Diskpart, on revient sur C:/Windows/system32>

Tapez la lettre de votre clef usb suivi de :
Dans mon cas donc E: et valider par entrée

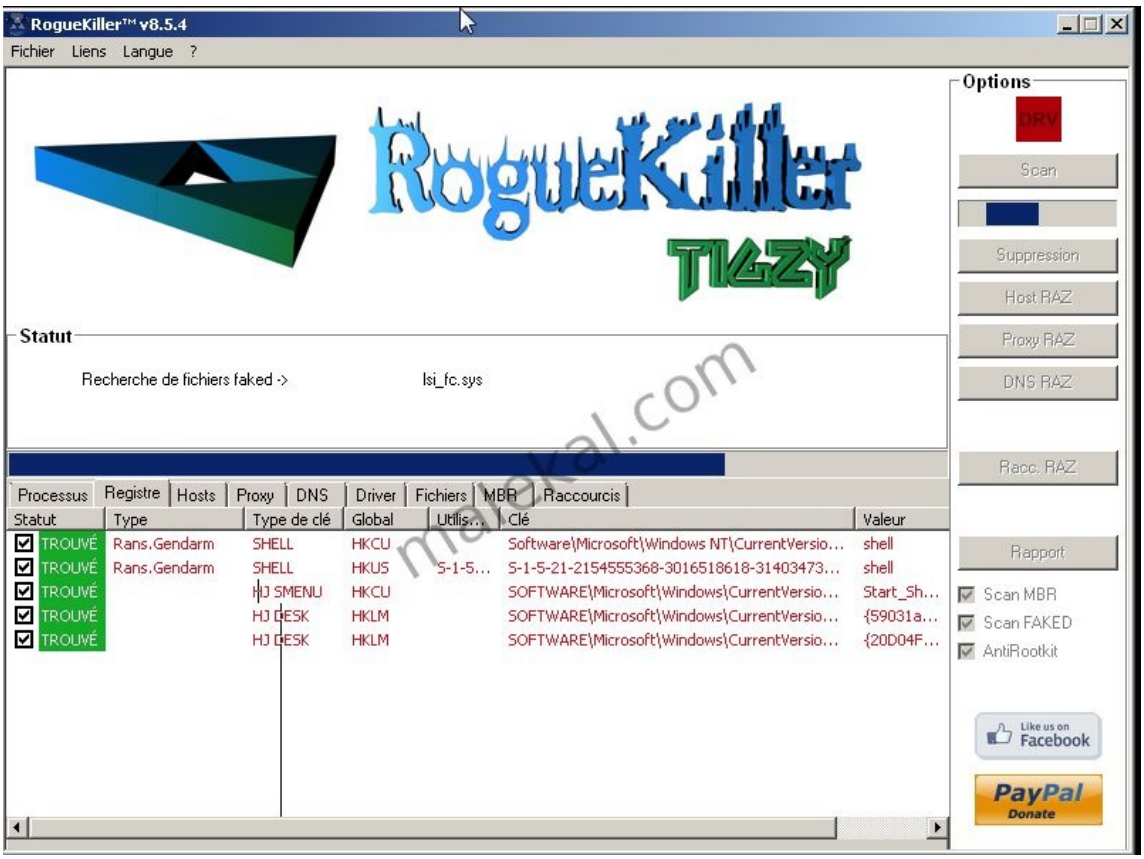
On arrive sur la clef USB E:/>

La commande dir permet de lister les fichiers.
Vous devez avoir le fichier de RogueKiller soit donc RogueKiller.exe

Tapez **roguekiller** (aucune importance pour les majuscules/minuscules et pas besoin de saisir le .exe à la fin) et validez par entrée.
RogueKiller doit se lancer.

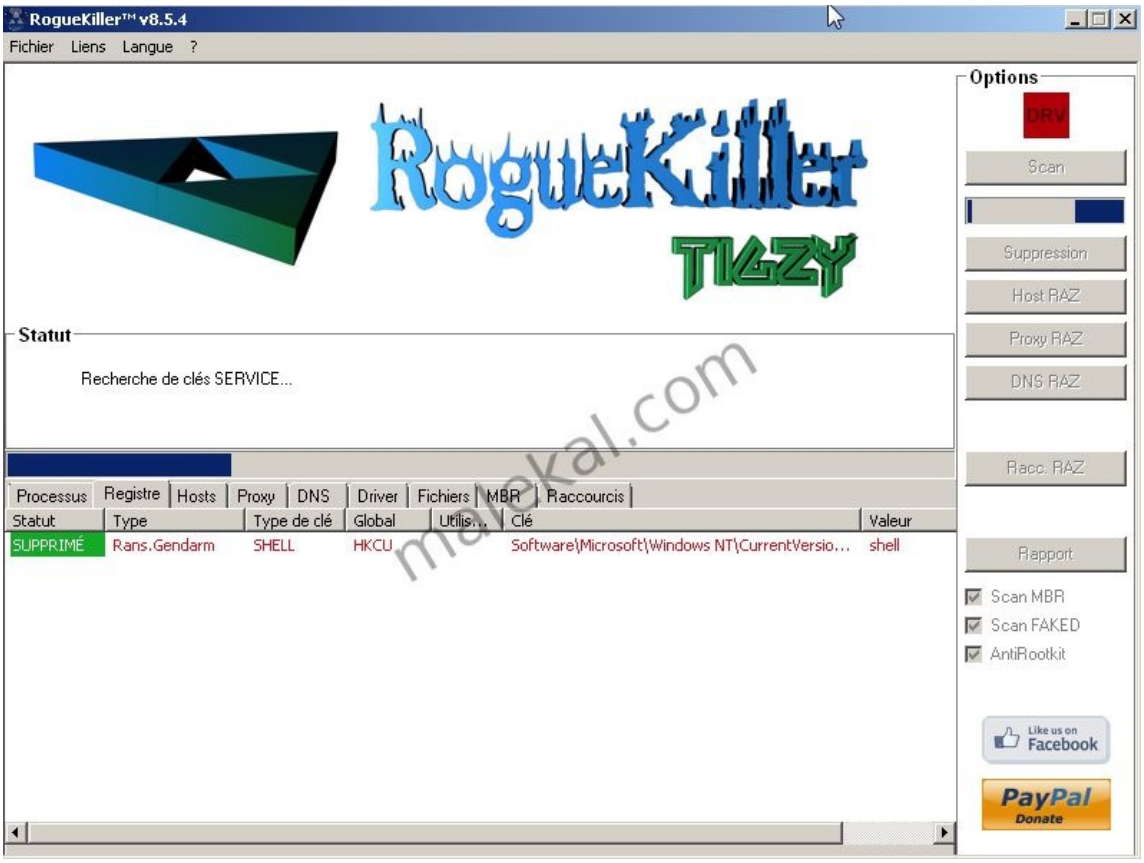


Lancer le Scan à partir du bouton en haut à droite Scan.
Rans.Gerdam doit être détecté.

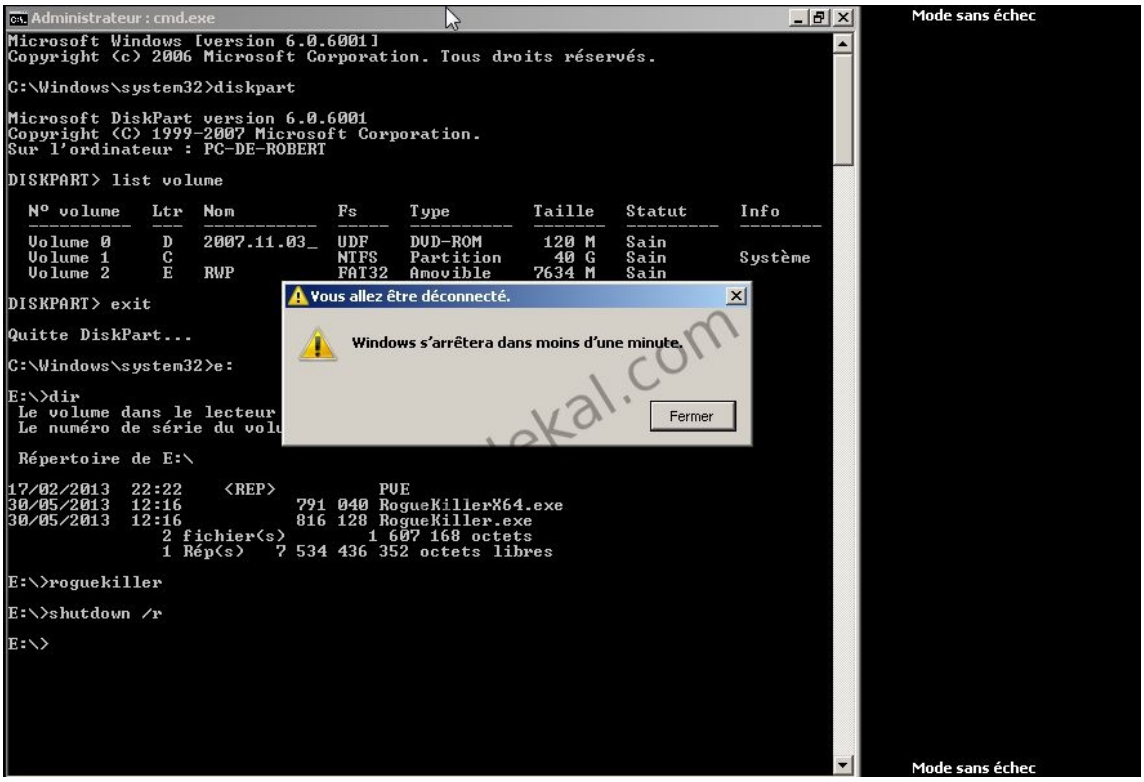


Une fois le scan terminé, faites Suppression à droite.

On doit avoir Supprimé sur RogueKiller si des éléments malicieux sont détectés.



Une fois la suppression effectuée, fermez RogueKiller.
Il convient de redémarrer l'ordinateur, pour cela, tapez la commande **shutdown /r** et validez par entrée.
Faites OK sur la popup d'information, l'ordinateur doit redémarrer et vous devez être débarrassé du virus gendarmerie.



Après la désinfection – Très important

Changer vos mots de passe WEB (Facebook, Mails, SN, jeux en ligne etc), ces derniers peuvent avoir été récupérés.

Il est ensuite conseillé d'effectuer un scan Malwarebyte
=> http://www.malekal.com/2010/11/12/tutorial-malwarebyte-anti-malware/

Des PUPs/LPIs sont certainement installés sur votre ordinateur, ces derniers étant très répandus.
Il est conseillé de faire un scan de suppression (bouton suppression) avec AdwCleaner.

Votre ordinateur est vulnérable car vos logiciels ne sont pas à jour – Un site hacké ou une publicité malicieuse qui conduit à un exploit sur site WEB peut infecter votre ordinateur (si votre antivirus est dans le vent, ce qui est souvent le cas).
La source de l'infection est d'avoir sur son ordinateur des logiciels non à jour.
Des logiciels permettent de vous y aider

=> **http://forum.malekal.com/logiciels-pour-maintenir-ses-programmes-jour-t15960.html**

Pensez à maintenir à jour vos logiciels (notamment Java, Adobe Reader et Flash), ces programmes non à jour permettent l'infection de votre système.
Plus globalement pour sécuriser son ordinateur : Sécuriser son ordinateur (version courte)

Vous pouvez aussi installer HOSTS Anti-PUPs/Adwares qui devrait filtrer les publicités clicksor.

Aucune aide ne sera donnée en commentaire, si vous avez besoin d'aide, créer votre propre sujet sur le forum partie VIRUS : http://forum.malekal.com/virus-aide-malwares-vers-trojans-spywares-hijack.html

---

[Traduction]