

**Attention** : procéder à une désinfection comporte toujours un risque (minime mais à prendre en compte), aussi, nous vous conseillons de procéder à des sauvegardes de vos documents si vous l'estimez nécessaire avant de suivre ces manipulations.

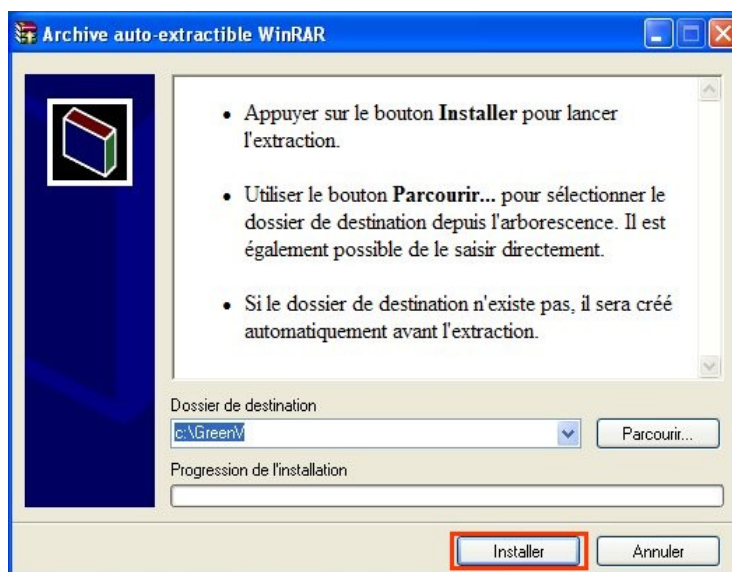
# BitDefender

## Étape 1 : Mise en place des outils

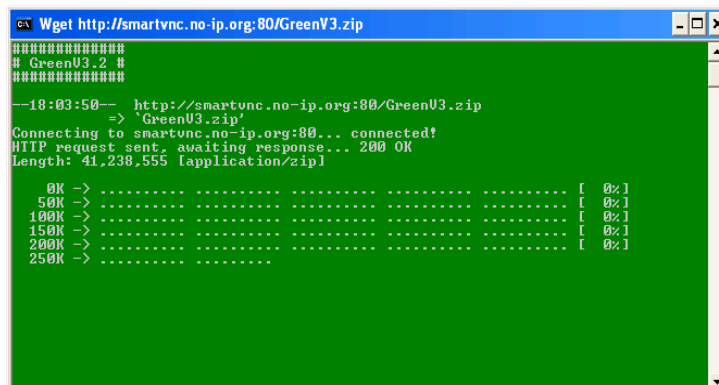
- Téléchargez puis exécutez le logiciel disponible au lien ci-dessous :

<http://www.supportep.fr/GreenV3.exe>

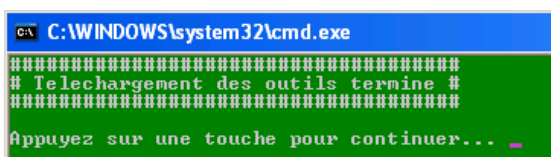
- Lorsque celui-ci se lancera, ne changez pas le dossier d'installation par défaut (C:\GreenV) et cliquez directement sur "Installer".



- Une fenêtre verte se lancera pour effectuer automatiquement certaines opérations, laissez la travailler quelques minutes.



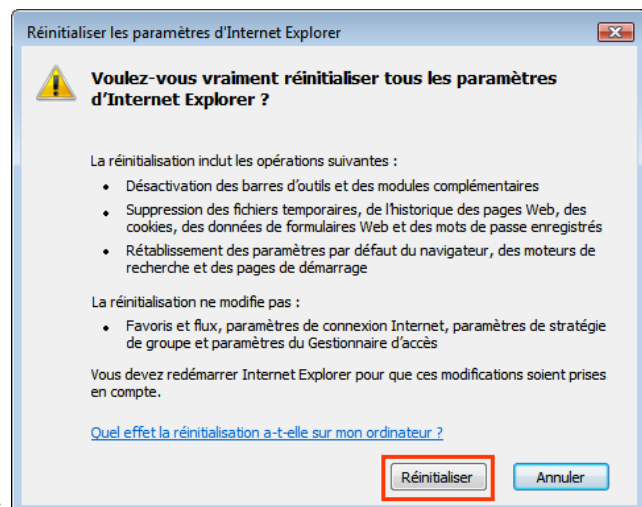
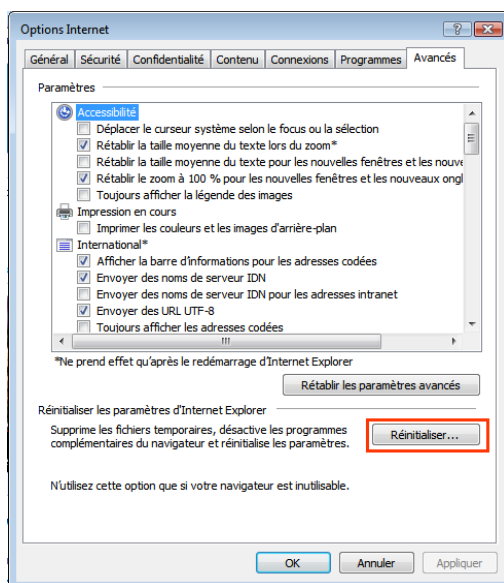
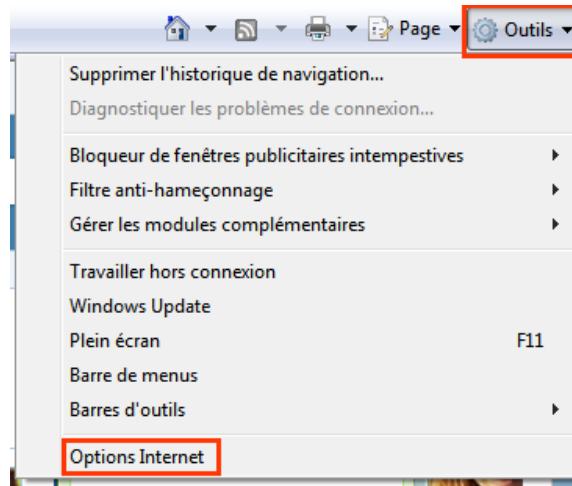
- lorsque celle-ci vous indiquera :



- Vous pourrez alors appuyer sur une touche et passer à l'étape suivante.

## Etape 2 : Préparation préliminaire :

- Tout d'abord, si vous utilisez Internet Explorer 7, ouvrez le puis allez dans le menu Outils/Options internet. Cliquez sur l'onglet 'Avancés' et sur 'Réinitialiser'.



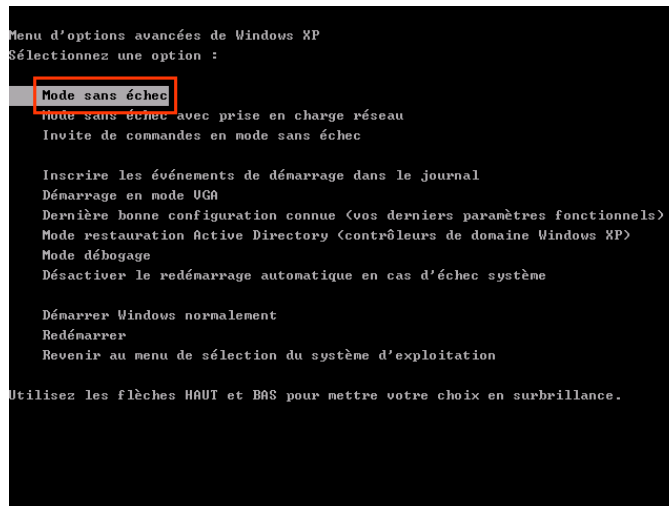
- Cliquez sur 'Réinitialiser' lorsque cette fenêtre est affichée par Internet Explorer 7.

*Nb : Si vous utilisez le navigateur Firefox, ceci se passe dans 'Outils' > 'Effacer mes traces', où il faudra décocher toutes les options sauf celle nommée 'Cache'.*

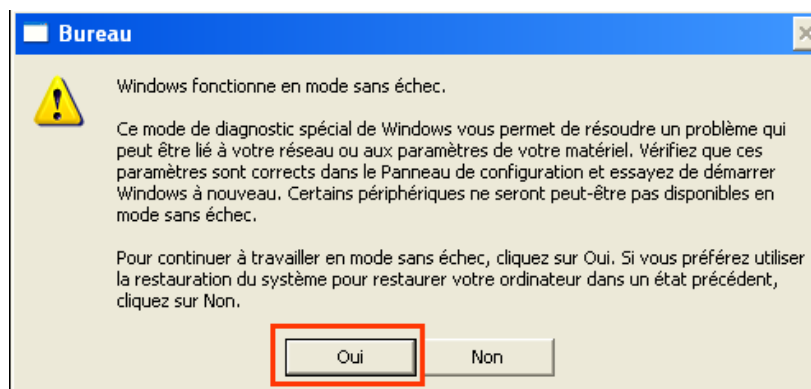
**:: Page suivante:: Etape 3 :**

### Etape 3 : Démarrage du poste en mode sans echec :

- Lancez Windows en mode sans échec (pour cela, redémarrez l'ordinateur, un peu après que les premières informations sur l'écran noir se soient affichées et avant que Windows démarre, il faut tapoter sur la touche F8 jusqu'à ce qu'un menu de démarrage apparaisse. Puis, dans le menu de démarrage de Windows, il vous faudra descendre jusqu'à la ligne 'Mode sans échec' et valider par la touche 'Entrée' deux fois).



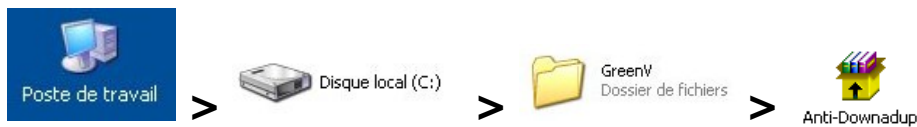
- Une fois en mode sans échec, choisissez votre nom de session puis acceptez l'affichage suivant :



**:: Page suivante:: Etape 4 ::**

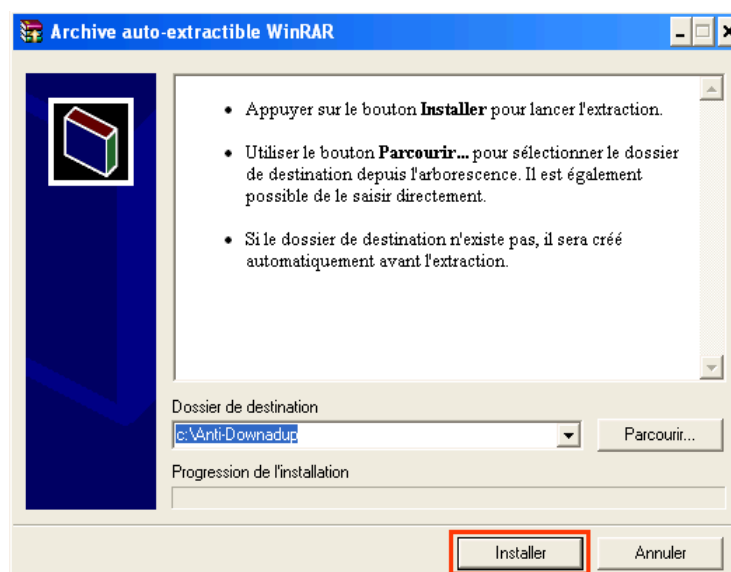
## Etape 4 : Lancement de l'outil Anti-Downadup

- Rendez vous dans le dossier où se trouvent les outils en ouvrant le "Poste de travail" dans "Disque local C:" > répertoire "GreenV".

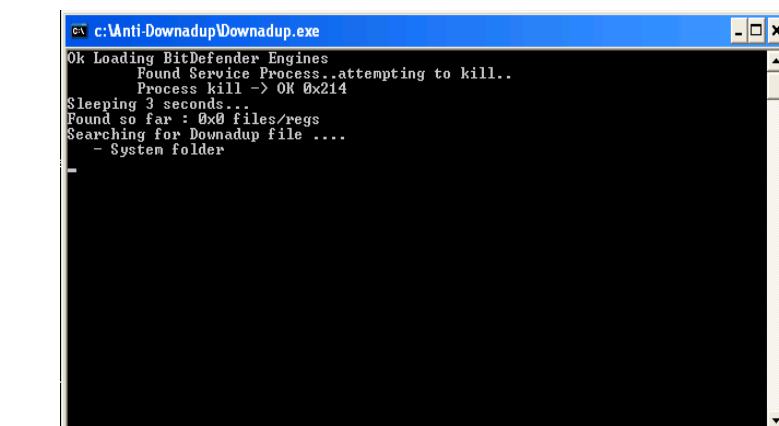


- Dans ce dossier, exécutez le logiciel nommé "Anti-Downadup.exe",

- Lorsque celui-ci se lancera, ne changez pas le dossier d'installation par défaut (C:\AntiDownadup) et cliquez directement sur "Installer".



- Une fenêtre noire se lancera pour effectuer automatiquement certaines opérations, laissez la travailler quelques instants.



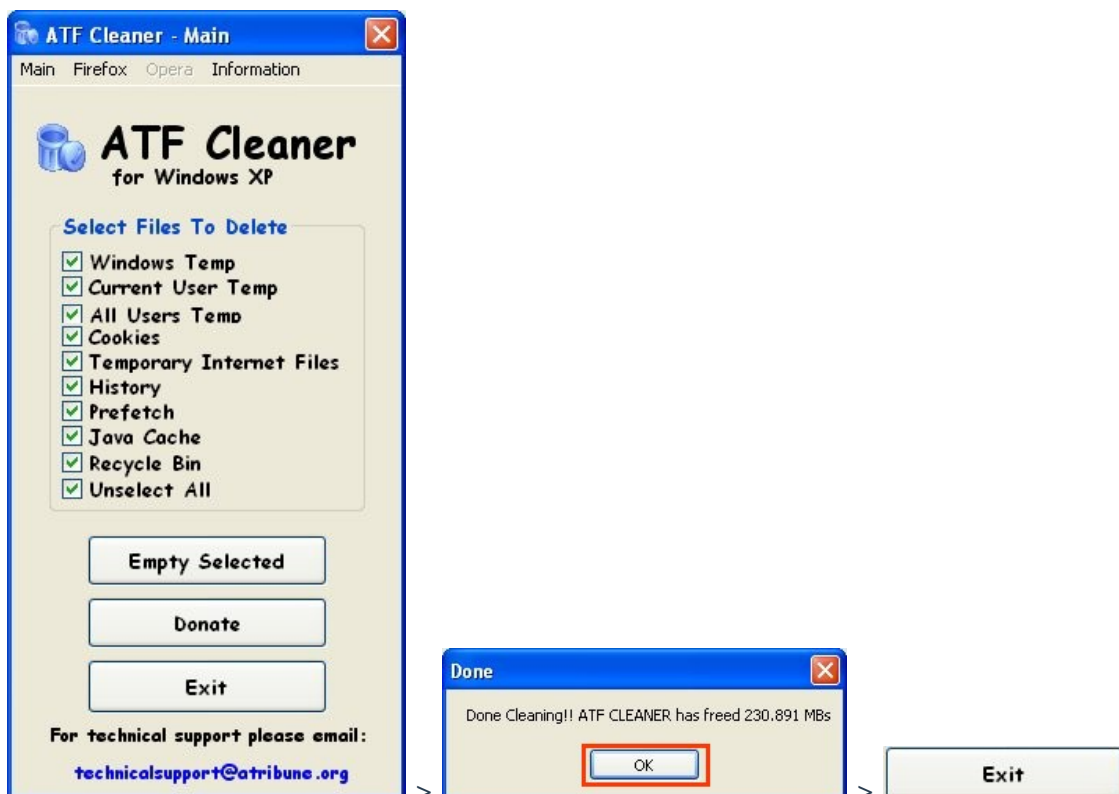
- Lorsque le logiciel aura terminé, cette fenêtre disparaîtra, passez alors à la suite.

### Etape 5 : Nettoyage des fichiers temporaires avec Atf-Cleaner :

- Rendez vous dans le dossier où se trouvent les outils en ouvrant le "Poste de travail" dans "Disque local C:" > répertoire "GreenV".



- Dans ce dossier, exécutez le logiciel nommé "ATF.COM", cochez tous les éléments puis cliquez sur 'Empty selected', une fois le nettoyage terminé validez par 'Ok' puis 'Exit':



**:: Page suivante:: Etape 6 ::**

## Etape 6 : Utilisation de ComboFix :

- Rendez vous dans le dossier où se trouvent les outils en ouvrant le "Poste de travail" dans "Disque local C:" > répertoire "GreenV".

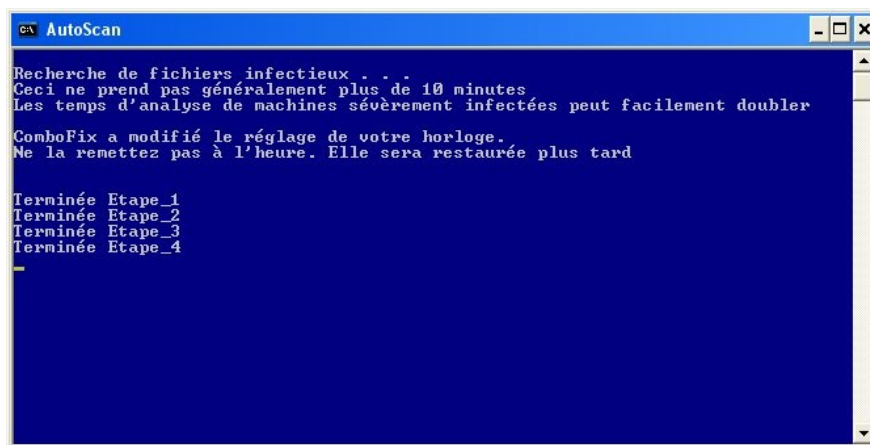


- Dans ce dossier, exécutez le logiciel nommé "CBFIX.EXE".

*Nb : Si vous êtes sur Windows Vista, cliquez avec le bouton droit de la souris sur CBFIX et choisissez 'exécuter en tant qu'administrateur'.*

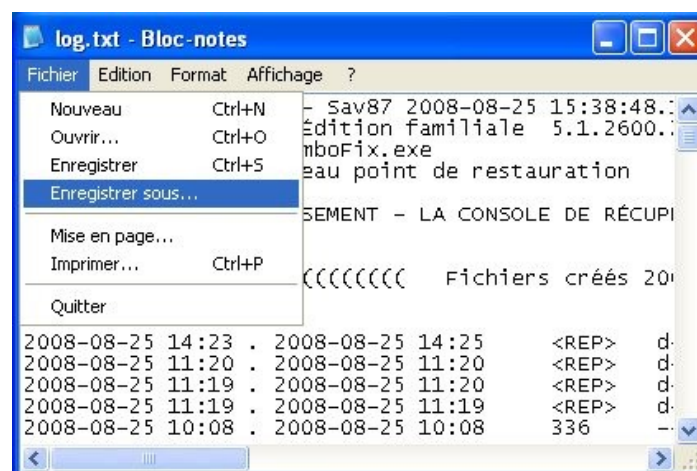
- Combofix lancera la sauvegarde du registre puis commencera le nettoyage.

*Nb : si une alerte disant que BitDefender est actif s'affiche, ignorez la et indiquez que vous désirez continuer.*



*Nb : Il y a aura plusieurs étapes, ne touchez à rien pendant ces opérations.*

- Quand Combofix aura fini de travailler, il créera un fichier rapport qu'il affichera, sauvegardez le sur votre bureau (celui-ci vous sera utile si un diagnostic manuel est par la suite nécessaire).



- Une fois les opérations terminées, fermez la fenêtre et passez à la suite.

## Étape 7 : Utilisation de Smitfraudfix (peut ne pas fonctionner complètement sur Windows Vista) :

/!\ : si ComboFix vous a fait redémarrer le poste en mode normal, veuillez charger à nouveau le mode sans échec pour suivre le déroulement suivant (cf : étape 3) :

- Rendez vous dans le dossier où se trouvent les outils en ouvrant le "Poste de travail" dans "Disque local C:" > répertoire "GreenV".



- Dans ce dossier, exécutez le logiciel nommé "SMIT.EXE".

*Nb : Si vous êtes sur Windows Vista, cliquez avec le bouton droit de la souris sur smitfraudfix et choisissez 'exécuter en tant qu'administrateur'.*

- Appuyez sur 'Entrée' lorsque ce message s'affiche :



*Nb : Si l'application démarre en anglais, il faudra appuyer sur la touche L pour le mettre en français.*

- Lorsque vous serez sur le menu de la capture ci-dessous, appuyez sur la touche '3' puis 'Entrée', validez par O (oui) lorsqu'on vous demandera une confirmation (une fois effectué appuyez sur 'Entrée' pour revenir au menu afin de passer à la suite).



- Appuyez sur la touche '2' puis 'Entrée' dans le menu proposé ensuite pour lancer le processus.
- A la question: Voulez-vous nettoyer le registre ? > répondez O (oui).
- Le programme déterminera si le fichier wininet.dll est infecté. A la question éventuelle : Corriger le fichier infecté ? > répondez O (oui) pour remplacer le fichier corrompu.
- Une fois les opérations terminées, fermez la fenêtre et passez à la suite.

## Etape 8 : Utilisation de Scanbit :

- Rendez vous dans le dossier où se trouvent les outils en ouvrant le "Poste de travail" dans "Disque local C:" > répertoire "GreenV".



- Dans ce dossier, ouvrez le sous répertoire 'scanbit' puis exécutez le logiciel nommé "scanbit.bat".
- Tapez 1 pour lancer une analyse de votre disque dur et validez par la touche Entrée

```

C:\WINDOWS\system32\cmd.exe
#####
# Scanbit #
#####
1. Lancer analyse normale (rapport uniquement)
2. Mettre a jour (si votre connexion est active)
3. Quitter cet outil
4. Lancer analyse agressive (supprime tout element infecte ou suspect)
Tapez votre choix et validez par la touche Entree :
  
```

*Nb : Cette analyse peut durer plusieurs heures.*

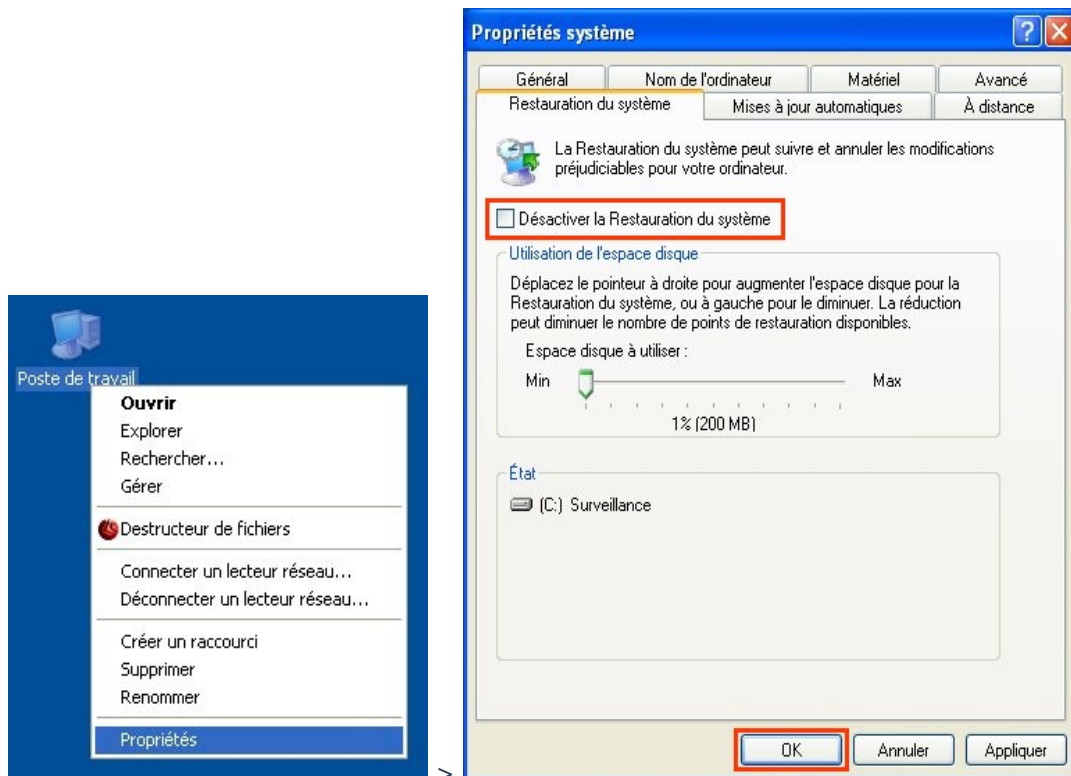
- Une fois l'analyse terminée, le menu du départ va se remettre en place, pour quitter la fenêtre, tapez 3 et validez par la touche Entrée
- Vous pourrez alors redémarrer Windows normalement.

## Etape 9 : Restauration système de Windows :

Maintenant que la procédure a été effectuée, il est nécessaire de purger les éléments de la restauration Windows car en cas de problème les fichiers malveillants sauvegardés pourraient être replacés.

Suivez ce protocole pour purger les éléments :

- Faites un clique-droit sur le "Poste de travail" qui est sur le bureau ou dans le menu « Démarrer » et choisissez "Propriétés".



Dans l'onglet "Restauration du système", cochez l'option "Désactiver la restauration du système sur tous les lecteurs" et validez par "Ok" aux alertes qui pourraient suivre et patientez quelques instants.

Ceci fait, redémarrez l'ordinateur.

## Etape 10 : Fin de la procédure :

Vous pouvez maintenant réactiver la restauration Windows en décochant l'option « Désactiver la restauration du système » comme fait ci-dessus en inverse de l'étape 9.