Désinfection de Downadup

Historique des versions de documentations			
N° de version	**Eléments modifiés**	**Date**	**Rédacteur**
1.0	Version Initial	15/03/2010	BOURGINE Christopher

BitDefender propose un outil de désinfection contre Downadup

Win32.Worm.Downadup, un ver informatique qui se répand en utilisant une vulnérabilité du service serveur Windows RPC a été détecté par BitDefender®. Ce ver (aussi appelé Conficker ou Kido) n'est pas nouveau en soi. Il est apparu pour la première fois fin Novembre 2008, exploitant la vulnérabilité MS08-067 pour se répandre facilement à travers les réseaux locaux et installer des programmes malveillants (programmes rogues) sur les ordinateurs infectés.

Fin décembre, les Laboratoires BitDefender avaient découvert une nouvelle version de ce ver appelée Win32.Worm.Downadup.B. Le malware présente de nouvelles caractéristiques, outre son mode de propagation et des signes d'amélioration.

Le ver utilise des clés USB pour se diffuser. Il se copie dans un dossier aléatoire à l'intérieur du répertoire RECYCLER (utilisé par la corbeille pour stocker les fichiers supprimés) et crée un fichier autorun.inf dans le dossier racine du lecteur infecté. Le ver s'exécute alors automatiquement si le lancement automatique est autorisé.

Le ver a également corrigé certaines fonctions TCP afin de bloquer l'accès aux sites Internet liés à la sécurité informatique en filtrant certaines chaînes de caractères contenues dans chaque adresse. Cela le rend encore plus difficile à éliminer puisqu'il est presque impossible de recueillir des informations à son sujet à partir d'un ordinateur infecté. De plus, il supprime certains droits d'accès de l'utilisateur afin de protéger ses fichiers.

Le ver est également conçu de façon à ne pas être détecté par les antivirus : il travaille avec des interfaces API rarement utilisées afin d'éviter les technologies de virtualisation. Il empêche les mises à jour Windows et certains trafics réseau, en optimisant les caractéristiques de Vista pour faciliter sa propagation.

Win32.Worm.Downadup.B a un algorithme de génération de noms de domaine similaire à celui trouvé dans des botnets comme Rustock. Il compose 250 domaines par jour et vérifie certains d'entre eux pour effectuer des mises à jour ou télécharger et installer d'autres fichiers.

En raison de ses caractéristiques (un système extrêmement récent, une bonne protection) et car beaucoup de gens ne font pas de mises à jours régulières de leur antivirus, ce ver pourrait devenir un rival aux botnets existants comme Storm ou Srizbi.

Pour plus d'informations techniques, vous pouvez consulter le blog Malwarecity (Malwarecity Blog) et la description de ce ver informatique (description du ver). Un outil de suppression est également disponible sur ces pages.

Source : http://www.bitdefender.fr/NW923-fr--BitDefender-propose-un-outil-de-desinfection-contre-Downadup.html

Procédure

Pour supprimer Win32.Worm.Downadup, veuillez suivre les étapes suivantes :

1. **Désactiver le Système de Restauration.**
   a) Dans la barre des tâches Windows, cliquez sur **Démarrer**.
   b) Cliquez avec le bouton droit de la souris sur **Poste de Travail** puis cliquez sur **Propriétés**.
   c) Dans l'onglet Restauration du système, sélectionnez **Désactiver la Restauration du système** ou **Désactiver la Restauration du système sur tous les lecteurs**.

   Note : Si vous ne voyez pas l'onglet Restauration du système, vous n'êtes pas connecté sous Windows comme Administrateur.

   d) Cliquez sur **Appliquer**.
   e) Lorsque le message de confirmation apparaît, cliquez sur **Oui**.
   f) Cliquez sur **OK**.

Recommendation

Afin de facilité la Désactivation de la Restauration Système, vous pouvez avoir recourt à un script.

Télécharger la clé registre **ici** et **copier** la dans \\Ip_du_Scribe\commun\scripts\

Note : Si le dossier intitulé scripts n'existe pas, créer-le.

Copier la ligne suivante dans un fichier texte **DomainUsers.txt** sous \\IP_du_Scribe\netlogon\scripts\groups

```
cmd, regedit.exe /s, \\ip_du_scribe\commun\scripts\disable_SR.reg, HIDDEN, NOWAIT
```

Note : Si le fichier DomainUsers.txt existe déjà, rajouter simplement la ligne à la suite des commandes existantes.

2. **Télécharger et installer le patch de vulnérabilité de Microsoft MS08-067 ici**

   Cette mise à jour de sécurité corrige une vulnérabilité signalée dans un service Windows. En effet, cette vulnérabilité pourrait permettre l'exécution de code à distance, si un système infecté recevait une requête RPC spécialement conçu.

3. **Télécharger et exécuter l'outil de suppression développé par les laboratoires BitDefender.**

   A/ Pour l'application sur un seul poste :

   a) Télécharger l'outil de suppression **ici**.

   b) **Extraire** les fichiers de l'archive.

   c) Exécuter le fichier **cleaner_cmd**.

   d) Redémarrer la machine et rebrancher le câble ou réactiver la carte réseau.

   B/ Pour l'application sur un réseau :

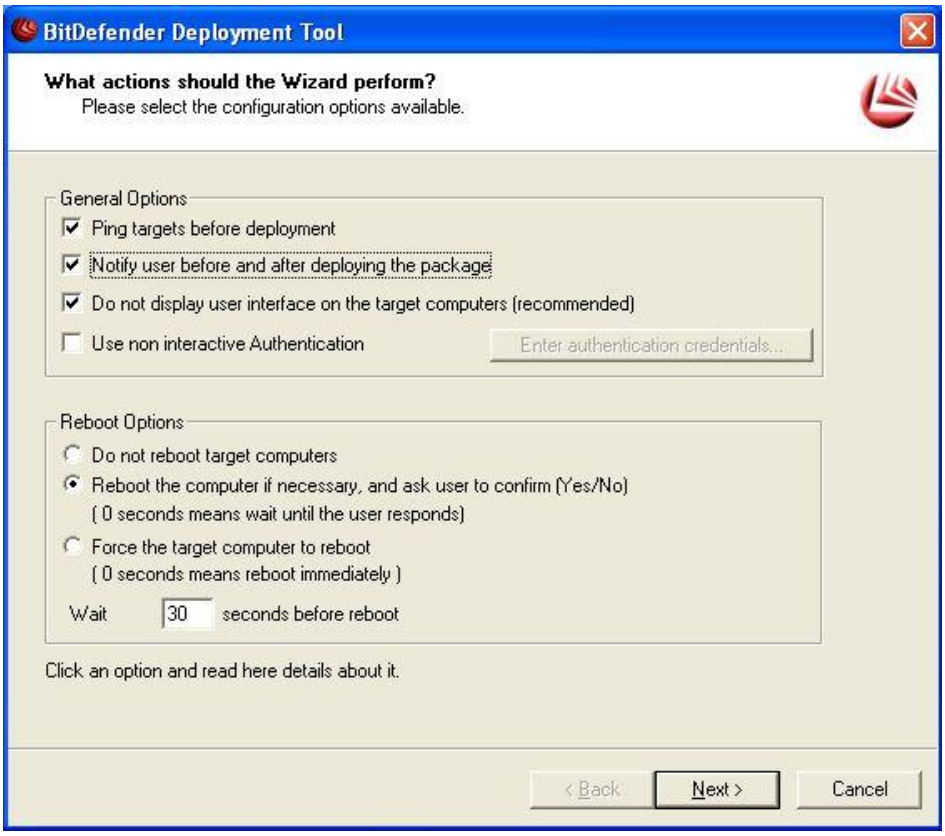
   a) Télécharger l'outil de suppression **ici** puis l'installer sur un ordinateur du réseau (ex : BDA pour le réseau Administratif et BDP pour le réseau Pédagogique).

   Note : Il est préférable, mais pas nécessaire, de l'installer sur une machine propre.

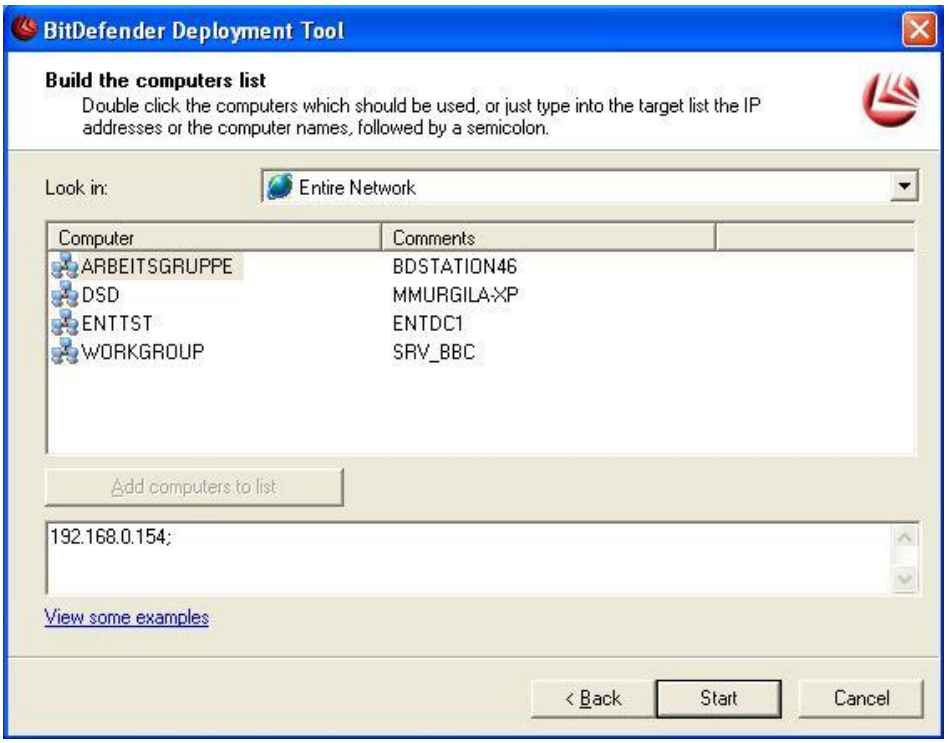
   b) Exécuter l'**Outil de déploiement** à partir du raccourci sur le Bureau ou du menu démarrer.

c) Sur l'écran des paramètres, cochez l'option « **Redémarrer si nécessaire** ».

Paramétrer les autres options si nécessaires.

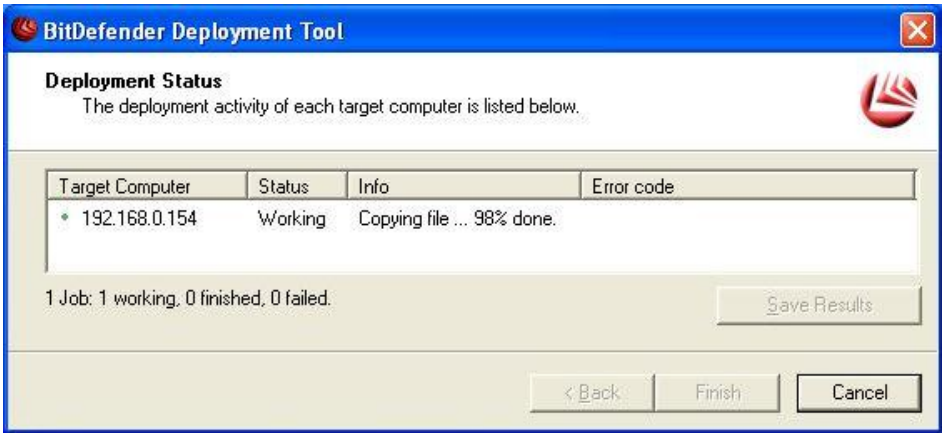


d) **Sélectionner** les ordinateurs devant être scanné à partir de la liste et démarrer le déploiement.



Note : Le processus sera très long si certaines machines ne sont pas en ligne. Cliquer sur Démarrer pour continuer.

e) L'outil de déploiement installera et exécutera l'outil de suppression Downadup sur les ordinateurs sélectionnés.



f) Si aucune infection n'est trouvée l'outil renverra la mention « Travail fini ». Au contraire, si une infection est trouvée, elle sera supprimée et la machine infecté sera programmée afin de redémarrer après 30 secondes.

Note : Le message « Travail fini » apparaître également pour tout autres situations (machine cible hors ligne, outil de suppression ne pouvant être exécuté, etc…)