

BitDefender : Suppression de Stuxnet via un outil gratuit

S curit 

Post  par : JerryG

Publi e le : 11/10/2010 13:48:53

L'outil de suppression est disponible gratuitement en t changement sur le site Malwarecity . **BitDefender**,  diteur de solutions de s curit  pour Internet, publie un outil gratuit de suppression du ver **Win32.Worm.Stuxnet**.

Cet outil permet de supprimer toutes les variantes connues de ce malware, ainsi que les drivers rootkit qui sont utilis s pour dissimuler des composants critiques du vers.

Win32.Worm.Stuxnet est une nouvelle esp ce de e-menace qui a fait son apparition vers la mi-juillet. Bien qu'il infecte tous les syst mes Windows sans distinction, il cible en priorit  les syst mes de supervision de contr le et d'acquisition de donn es (SCADA) qui utilisent le logiciel Siemens WinCC.

Le ver se r pand en utilisant une multitude d'exploits de type Zero Day disponibles dans les diff rentes versions de Windows. De plus, il peut s'auto-ex cuter sur un media amovible d s que le fichier .lnk du disque a  t  lu par le syst me d'exploitation.



Lorsque la vulnérabilité est exploitée correctement il en résulte l'injection d'une backdoor, ainsi que l'installation cachée de deux rootkits dissimulant à la fois le fichier .lnk et le fichier.tmp qui l'accompagne.

« BitDefender a intégré une détection générique de toutes les variantes de Stuxnet le 19 juillet dernier, ce qui a permis de protéger nos clients depuis le 1er jour. Dans le cadre de notre volonté constante de participer à la lutte mondiale contre les e-menaces, BitDefender a aussi développé un outil de suppression indépendant contre Stuxnet. Les utilisateurs d'ordinateurs qui ne sont pas protégés par les solutions de sécurité BitDefender peuvent maintenant eux aussi nettoyer leur système infecté » déclare **Catalin Cosoi**, Directeur du Laboratoire BitDefender de lutte contre les e-menaces.

L'outil peut être lancé à la fois sur les systèmes 32 ou 64 bits et éliminera à la fois les drivers du rootkit et le ver lui-même.

L'outil de désinfection peut être téléchargé depuis la section Downloads du site [MalwareCity](#), le site communautaire de référence des logiciels de sécurité créés par l'initiative de BitDefender, qui propose des ressources gratuites pour les personnes intéressées par la sécurité en ligne.