Le virus Conficker s'exporte d'abord en Asie et en Amérique du Sud

Bien que la faille que le ver **Downadup** exploite ait été corrigée depuis trois mois, le malware continue de faire des siennes. A en croire les experts, il serait même en passe de devenir **la plus grosse attaque contre les PC Windows** depuis des années.

Selon **Panda Labs**, au moins **1 PC sur 16 dans le monde est infecté** par ce ver et 6% des systèmes scannés par l'éditeur sont touchés (soit 111.000 postes sur un parc de 2 millions de machines). De son côté, Symantec avertit que le malware a débarqué sur les côtés asiatiques et sud-américaines. L'éditeur poursuit en précisant que la **Chine et l'Argentine** ont été les deux pays les plus durement touchés par la propagation. L'éditeur estime même à **29% le nombre de postes infectés par le virus en Chine** (11% en Argentine).

Downadup exploite une **vulnérabilité dans le service Serveur de Windows** qui permet l'exécution de code à distance si un système affecté recevait une requête RPC (Remote Procedure Call) spécialement conçue. Du coup, les **critiques contre Microsoft** se sont faites plus acerbes. L **'US-CERT** (Computer Emergency Readiness Team) y est même allée de sa pique en jugeant les **contre-mesures de la firme insuffisantes.**

La firme de Redmond avait seulement conseillé comme mesure préventive **de désactiver les fonctions Autorun ou Autoplay des clés USB**, histoire de ne pas encourager la propagation du virus. Les experts du CERT ont répliqué que **la mesure n'empêchait en rien la propagation du ver** (un simple double-clic sur le Poste de travail peut suffire à déclencher un fichier Autorun). Rappelons néanmoins que Redmond a publié un patch corrigeant la faille exploitée en octobre dernier.

Des débats qui n'empêchent pas Conficker de continuer son tour du monde, en infectant un poste après l'autre. Il se pourrait que des **codes spéciaux aient été élaborés pour atteindre les réseaux des pays touchés**, ce qui expliquerait le nombre important de postes infectés.

Pour rappel, **Conficker dérobe les mots de passe** et se permet de bloquer nombre de comptes nécessitant des identifiants. Mais le ver évolue à son propre rythme dans la mesure où sa version la plus récente installe un **programme appelé Antivirus XP**, **un faux antivirus** bien connu dont la tâche est de vous submerger de pop-ups.

Reste maintenant à attendre les c hiffres de sa propagation de tous les éditeurs et de Microsoft afin de connaître la portée réelle du ver **Downadup/Conficker** et les dégâts qu'il aura causés.