Le virus Conficker mute

Une nouvelle variante du **ver Downadup/Conficker** est sur la Toile. Il a été découvert voilà trois jours par les chercheurs du **SRI International**. Ils ont alors diffusé les **détails du code du virus** afin de mieux l'apprivoiser.

Pour des yeux profanes, le ver est le même et ne possède aucune différence avec le traditionnel Conficker B. Le **B++** utilise en fait une **nouvelle méthode de téléchargement du logiciel** conférant ainsi à ses créateurs plus de flexibilité pour infecter les machines.

Les postes infectés servent ensuite de terminaux pour l **'envoi de spams, le vol de codes et identifiants** ou encore peuvent servir de base de lancement pour des **attaques de type déni de service** (**DoS**). Cependant, un groupe s'étant appelé la **« cabale Conficker »** a pris soin de contrôler les effets du virus en craquant son algorithme.

Une manœuvre possible seulement lorsque le malware cherche un point de rendez-vous sur un nom de domaine afin qu'il obtienne un nouveau code (pour ainsi se diffuser). Ces « *points de rendez-vous sont en fait des noms de domaine tels que* ***pwulrrog.org,*** *désormais hors de mains criminelles* » expliquent les spécialistes.

En détail, les modifications du virus **Conficker** sont de nature presque chirurgicales. Seuls **39 nouveaux routages ont été ajoutés au B++ sur les 297 déjà existants.**

Aussi connu sous le nom de **Downadup**, le ver utilise une variété multiple de méthodes de diffusion. Il aurait atteint presque tous les continents et continuerait son infection. Une épine dans le pied de Microsoft puisque le malware **utilise une faille, pourtant corrigée, des OS signés Redmon** d.

Microsoft a même décidé de faire **justice elle-même** en proposant une **récompense de 250.000 dollars** pour celui qui fournira des informations permettant d'arrêter et de traduire en justice le responsable de la diffusion du ver. « *La prime est valable dans le monde entier* » précise Microsoft.

On estime à environ **10,5 millions le nombre de postes infectés** par toutes le variantes du malware. Presque une épidémie.