La future version de Conficker angoisse les spécialistes

Conficker poursuit ses ravages et confirme, semaine après semaine, sa position de ver le plus dangereux depuis pas mal d'années. Selon *Computerworld*, une nouvelle variante du malware (la troisième) pourrait apparaître la semaine prochaine, seul problème, les spécialistes et les éditeurs de sécurité ne savent absolument pas à quoi s'attendre.

Cette nouvelle version prévue pour le 1er avril (une date qui n'a pas été choisie au hasard), utilisera d'autres techniques de diffusion et de propagation, estiment les spécialistes. Pour autant, excepté cette date, que les ingénieurs ont retrouvé dans le code du ver, personne ne sait vraiment ce qui va se passer.

*« Nous n'avons aucun élément, excepté la date »,*concède Joe Stewart, directeur de la recherche pour SecureWorks, cité par nos confrères. *« Personne ne sait rien »,* ajoute Vincent Waefer, vice-président de Symantec. Pas très rassurant.

Une chose est sûre, ce Conficker.C devrait être encore plus armé contre les outils de détection et de nettoyage.

En attendant cette nouvelle attaque, des chercheurs de l'Université du Michigan sont actuellement à la recherche de la première victime du ver afin de mieux comprendre l'épidémie.

En utilisant un réseau international de senseurs électroniques, l'équipe de l'Université du Michigan a obtenu des milliers de données sur Conficker et la façon dont le ver s'est répandu.

Rappelons que Conficker 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.

Selon les éditeurs de sécurité, plus de 10 millions de machines sur la planète sont contaminées par une variante de Conficker.

Aussi connu sous le nom de **Downadup**, le ver utilise une variété multiple de méthodes de diffusion (clés USB, AutoRun…). 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.**

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.