Une nouvelle attaque pourrait écraser le pare-feu de XP

Le code en question a été publié sur le Net dimanche matin. Ce dernier pourrait être utilisé pour mettre hors de fonctionnement *« le firewall »* de Xp, le tout sur un ordinateur avec l'ensemble des *« services pack »* de l'OS.

Il faut cependant que l'ordinateur utilise le service ICS (Internet Connection Service). ICS permet aux utilisateurs de se mettre en réseau sur un LAN (Local Area Network). C'est typiquement un programme très utilisé par les particuliers et les PME.

En utilisant ICS, une personne malintentionnée pourrait par exemple envoyer un paquet contenant du code sur un ordinateur distant qui provoquerait la fin du service. Mais le pire reste à venir puisque ce service est connecté au pare-feu Windows, et le fichier envoyé par le pirate est conçu pour l'éteindre.

Tyler Reguly, un ingénieur de nCircle Network Security Inc a publié une note à ce sujet sur son weblog, précisant : *« Une fois que le pare-feu est désactivé, l'utilisateur lambda n'a plus de défense. Le cyber-criminel peut alors lancer de nouvelles attaques. »*

Reste que cela n'est pas si évident, Reguly souligne *« Le pirate doit être dans le LAN pour faire fonctionner son attaque, et il ne peut cibler que les systèmes utilisant ICS, qui rappelons le est désactivé par défaut. Qui plus est, cette attaque n'aurait aucun effet sur les autres firewalls! »*

Pour se protéger, les utilisateurs doivent vérifier l'état d'ICS et si besoin est, le désactiver. En sachant que cela va détruire le partage des connexions internet. Ou bien passer sur un routeur ou sur un équipement NAT (Netword Address Translation).

Pour l'instant, XP est la seule plate-forme vulnérable. Windows Server 2003 n'est pas touché mais la prudence est de mise.