Sécurité : La FiFa 2010 et MS Office 2010 : des plateformes pour les pirates
Sécurité
Posté par : JulieM
Publiée le : 17/6/2010 15:00:00

Les experts en messagerie de **Retarus** constatent une forte augmentation des attaques virales depuis le début du mois : **la proportion d'emails infectés a quintuplé** durant les deux premières semaines de juin

Sur la seule journée du 11 Juin, toutes les entreprises dont les infrastructures de messagerie sont protégées par Retarus ont été menacées par 1.000 emails vérolés en moyenne.

Le responsable de cette augmentation est un cheval de Troie connu qui se manifeste depuis ces derniers jours sous les noms Troj/JSRedir- AR, Mal/TDSSPack-Q et TrojanDownloader:Win32/Rugzip.A.

Retarus recommande une stratégie multi-scan, c'est-à-dire de recourir à une solution qui détecte les virus à l'aide de plusieurs scanners fonctionnant simultanément pour obtenir une protection maximale.

Retarus est un des plus importants prestataires en matière de communication et de sécurité du trafic d'emails en Europe.

Les experts de Retarus observent depuis le début du mois une forte augmentation d'emails

infectés par rapport au flux total. D'ordinaire, le pourcentage d'emails vérolés est inférieur à **1%** du volume total d'emails, alors qu'il a parfois atteint **5%** au début du mois de Juin. Retarus a même enregistré un taux de **66%** sur deux jours consécutifs pour l'un de ses clients représentant 30 000 utilisateurs de messagerie.

Ces emails vérolés sont en phase avec l'actualité puisque la plus grande partie d'entre eux comportent des objets tels que « FIFA World Cup South Africa ... bad news » ou « Outlook Setup Notification ». Ils coïncident ainsi avec le lancement de la Coupe du Monde de Football en Afrique du Sud, ainsi qu'avec le récent lancement d'Office 2010. Le risque qu'un utilisateur ouvre accidentellement un email vérolé est ainsi accentué.

La grande majorité de ces virus sont des programmes malveillants qui s'installent sur un ordinateur à l'insu de son propriétaire et le transforme en plateforme d'envoi de spams, souvent via l'adresse email du propriétaire. Le cheval de Troie détourne ainsi la puissance de l'ordinateur pour construire ou alimenter des réseaux zombies.

« *Les flux de chevaux de Troie sont constitués de trois malware qui, bien que connus, restent toujours dangereux* », explique **Frédéric Brault**, Directeur Commercial de Retarus France.

« Il s'agit concrètement des chevaux de Troie : Mal/TDSSPack-Q, Troj/JSRedir-AR et TrojanDownloader:Win32/Rugzip.A. Pour se défendre efficacement face à de telles attaques, il faut absolument disposer de mécanismes de protection sophistiqués. Chaque email qui transite par nos centres de calculs, est vérifié en parallèle par quatre antivirus différents, à jour en permanence. C'est la seule façon de s'assurer que de nouvelles mutations de virus connus ou des virus moins connus ne puissent arriver jusqu'au destinataire. Grâce à la fiabilité de notre stratégie multi-scan, aucun de ces codes nuisibles n'a pu atteindre nos clients » résume **Frédéric Brault**.