Hackers : penser petit, ça rapporte gros?

En se concentrant sur une ou deux compagnies à la fois, un cybercriminel peut gagner gros. Et même très gros, comme l'affaire des 40 millions de cartes de crédits MasterCard vient le confirmer (

lire nos articles). A terme, cette approche très ciblée pourrait constituer un retournement chez les 'hackers'. En effet, les pirates informatiques auteurs de virus recherchaient plutôt jusqu'ici les effets de masse. Une valeur sûre pour leur libido ou autre propension… L'affaire MasterCard a révélé que la menace est venue d'un simple script judicieusement placé sur des ordinateurs d'un prestataire, CardSystems Solutions. MessageLabs confirme d'ailleurs que les attaques, vers une ou deux sociétés exclusivement, ont augmentées de 150% depuis janvier. Astuce pour les hackers, réduire la cible permet de personnaliser l'attaque, comme de s'adresser en priorité aux employés ou aux proches de l'entreprise. Pour les inviter à télécharger un logiciel vérolé par exemple, ou à déposer leurs codes d'accès et mots de passe ! Autre astuce pour les cybercriminels, placer manuellement un Trojan, un *cheval de Troie*, sur un poste judicieusement choisi. Ce Trojan se chargerait ensuite, automatiquement et à l'insu de l'utilisateur, de transmettre aux mafieux des informations confidentielles. Ici aussi l'actualité récente vient confirmer la pertinence de la méthode, avec une affaire d'espionnage industriel révélée en Israël (*lire notre article*). Et puis, selon RSA Security, cibler une ou deux sociétés permet de réduire le spectre de la menace, et donc d'échapper plus facilement aux protections, majoritairement basées sur les l'identification des attaques de masse. Pas de repérage, c'est l'assurance de développer tranquillement son 'business'. Un rêve de hacker !