Un 'trojan' s'invite dans les disques Seagate

À la suite d'un problème encore non déterminé sur la chaîne de production, un cheval de Troie s'est retrouvé embarqué dans 1.800 disques dur du fabricant américain Seagate.

Heureusement, seul le marché taiwanais est frappé, mais la bourde est énorme.

1.800 disques durs portables de « large capacité de stockage », qui se destinent donc surtout aux entreprises, mais aussi aux ministères taiwanais et aux locaux des agences gouvernementales ont été livrés avec un trojan.

Cette terrible erreur a été dévoilée par le *Taipei Time*, et une enquête est en cours pour déterminer comment ce maudit code malveillant est arrivé dans les équipements de stockage.

Seagate a bien confirmé cette information, le groupe n'a cependant pas joué la carte de la transparence jusqu'au bout, puisqu'il n'a pas publié d'alerte en rapport avec cet événement sur son site officiel. Par contre, la branche Asie Pacifique de Seagate annonce avoir ouvert une enquête interne.

Selon nos informations, le « canasson » embarqué sur les disques avait pour fonction d'envoyer toutes les données stockées sur le HD vers des pages Web hébergées à Pékin.

Apparemment les disques incriminés, de la famille des Maxtor Basics 500GO, ont été fabriqués en Thaïlande. Selon le bureau de la Justice de Taiwan deux trojans ont été identifiés. Ils sont nommés autorun.inf et ghost.pif.

Les sites de Pékin utilisés sont les suivants : www.nice8.org et www.we168.org. Pour des raisons évidentes de sécurité, nous déconseillons l'accès à ces URL. Des données sensibles ont probablement déjà été dérobées.

Cette affaire « hors du commun » montre qu'il n'est pas nécessaire d'utiliser le Web pour être victime de piratage informatique. Dans ce cas, la Toile n'est pas le vecteur de contamination mais elle est uniquement utilisée pour le rapatriement des données volées sur la machine de l'attaquant .

On se souvient notamment de la méthode utilisée par le couple israélien Haephrati. Ces derniers avaient utilisé une approche totalement nouvelle pour pirater leur cible. Lui envoyer un faux CD de marketing vantant une offre alléchante, mais en guise de « promotion » l'utilisateur était infecté par un Trojan.