Un ‘rootkit trojan’ pourrait obliger à ré-installer Windows

Les ‘patch Tuesdays’ se succèdent (cf. article: ‘Microsoft patch tuesday: 34-vulnérabilités à corriger en juin’), mais parfois, Microsoft est prêt à le reconnaître, cela ne suffit pas.
La dernière alerte lancée aux Etats-Unis ce lundi 27 juin s’appelle ‘***Popureb***‘: ce ‘malware’ est une infection ‘*rootkit’* qui se propage comme un redoutable ‘trojan’ (cheval de Troie); il s’enferre si profondément dans Windows qu’il pourrait bien conduire les utilisateurs à une ré-installation complète de l’OS. Sa référence exacte : ***Trojan:Win32/Popureb.E*** .
Dixit Microsoft! Car la source est un certain Chun Feng, ingénieur du **MMPC**, qui n’est autre que le très officiel *Microsoft Malware Protection Center*, lequel vient de lâcher l’information sur un blog.
Ce ‘malware’ écrase, ni plus ni moins, l’enregistrement du ‘boot’ (ou ***MBR***, *master boot record*), le fameux secteur 0 du disque dur, où est stocké le code de lancement du système d’exploitation, une fois que le ‘BIOS a été lancé et fait son ‘check-in’.
De ce fait, confirme Computerworld, ce ver cheval de Troie ne peut pas être détecté, ni par les anti-virus ni les autres systèmes de sécurité -semble-t-il, puisque non visible par l’OS.

Recommandations
« *Si votre système est infecté avec ce Trojan:Win32/Popureb.E, nous vous recommandons de rétablir le MBR et d’utiliser ensuite le CD de restauration pour restaurer votre système à un état antérieur à l’infection*« , déclare cet ingénieur de Microsoft.
Selon ses explications, Popureb détecte les opérations d’écriture visant le MBR – opération conçues justement pour en assurer le nettoyage ainsi que d’autres secteurs du disque pouvant contenir du code susceptible d’attaquer le système – et ensuite le ‘malware’ échange l’opération d’écriture par une opération de lecture. Alors même que l’opération semble avoir été effective, la nouvelle donnée n’est, en fait, pas enregistrée sur le disque. Donc, le nettoyage n’aura pas fonctionné.
La recommandation, avec des liens vers des instructions pour rétablissement du MBR, vaut pour ***Windows XP, Vista*** et ***Windows 7***.
Encore faut-il disposer de son ‘*Recovery CD*‘, car la procédure de restauration à partir de son disque dur paraît donc compromise.

(A suivre)