Microsoft sécurité : Les chevaux de Troie Conficker et Taterf ciblent la France

Issy-les-Moulineaux – C'est dans le rutilant nouveau quartier général de Microsoft que les responsables de la firme ont tenu à approfondir le 7e rapport semestriel sur la sécurité. Un secteur où les menaces restent en hausse même si **la France connaît un taux d'infection stable**.

La firme Microsoft a donc rendu son 7e rapport semestriel sur la sécurité pour la période entre janvier et juin 2009. Le principal intérêt de l'étude réside dans le fait que les résultats agrègent les observations provenant à la fois du système anti-phishing de **Bing**, de l'antivirus de Windows Live Hotmail mais aussi du MSRT (Malicious Software Removal Tool), **Windows Live OneCare** (appelé à être remplacé par Security Essentials) ou encore de l'outil anti-phishing d'Internet Explorer et du client Microsoft ForeFront utilisé par les entreprises. Un total de **plus de 500 millions de machines**.

Dans ce rapport de 232 pages en anglais (*Microsoft Security Intelligence Report*), Microsoft pointe du doigt la **dangerosité des chevaux de Troie** qui arrivent en première position des menaces. En second, les vers informatiques vont jusqu'à occuper en Espagne ou en Corée du sud notamment, la première place des menaces les plus fréquemment rencontrées sur des machines Windows.

Pour ces pays, le **ver Taterf** a connu une forte expansion, puisqu'il cible les joueurs en ligne. Le rampant utilise les ressources de l'ordinateur qu'il a infecté pour se multiplier et assurer sa propagation. Une fois niché dans les supports de stockage externe comme les disques durs ou les clés USB, il peut infecter d'autres machines. Un modus operandi qui sévit sur les sites de jeux en ligne.

Pour autant une des menaces les plus importantes est encore représentée par Conficker. A ce titre, Microsoft note que le ver est à lui seul **la plus grande menace détectée en environnement professionnel** au premier semestre 2009. **Vinny Gulotto**,responsable sécurité de l'éditeur commente la situation de ce ver qui procède à une **infection via clé USB** : « *Nous avons mis en place des groupes de travail à travers le monde afin de limiter le plus possible l'impact et la progression de Conficker, sous toutes ses versions. Ainsi des pays tels que l'Autriche, l'Allemagne ou le Japon ont pu dégager de bonnes méthodes pour son éradication* ». Bien que l'auteur du virus n'ait jamais été encore retrouvé, l'éditeur explique donc avoir amorti l'impact de l'infection en milieu professionnel.

A propos du cas particulier de la France, **Bernard Ourghanlian**, directeur technologie et sécurité de Mirosoft France fait le point sur la situation : « *Les faux antivirus ne sont plus la menace principale mais ce sont bien les chevaux de Troie qui regroupent avec 34,4 %, les principales voies d'action des pirates.* » Selon le rapport, au premier semestre 2009, le taux mondial d'infection par un malware pour 1.000 machines est de 8,7. Il est le plus élevé en Turquie (32,3 pour 1000 machines), au Brésil (25,4), en Espagne (21,6), en Corée du Sud (21,3). E **n France, il est de 7,9 pour 1.000.**

Enfin ces résultats sont à pondérer par le fait que de nombreux utilisateurs disposent de versions non authentiques des OS Microsoft. Les mises à jour sont alors plus rarement appliquées car bien des utilisateurs craignent de **bloquer leur logiciel en installant des correctifs,** qui permettent

aussi à Microsoft de vérifier la licence des produits. Autant de marchés sur lesquels la vision peut être rendue parfois grisée…