# Reportage: comment Microsoft évalue les menaces sur Internet ?

**Redmond**. – Ils sont fort nombreux, très divers et font le malheur de bien des internautes. « Ils », ce sont les **malwares** qui viennent empoisonner la vie des utilisateurs.

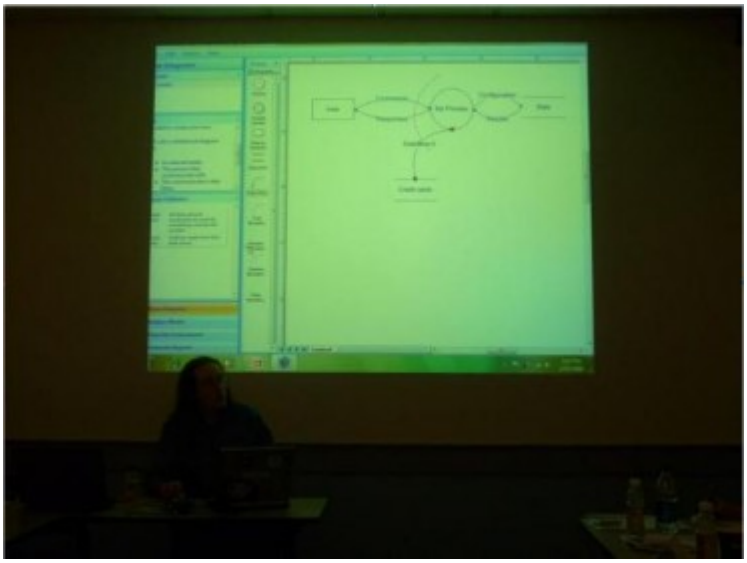
« *Quand nous réalisons nos patchs, l* ***es pirates cherchent immédiatement la parade*** *et comment les contourner. C'est un challenge permanent. Le* ***MMPC*** (Microsoft malware protection Center) *est donc au centre des attentions*« , nous explique Jimmy Kuo, du centre de protection. La guerre est permanente.

Chaque mois, sont produits via des blogs et sites spécialisés les détails des attaques et les systèmes de protection visés par les attaques. De même, une **encyclopédie du malware est sur pied** pour pouvoir identifier plus rapidement les failles et autres virus arrivant sur la Toile. Le dernier état des lieux de Microsoft date de janvier à juin 2008. Le **Microsoft Security Intelligence Report** établit une sorte d'état de l'Art des failles déjà existantes. Il relève alors que « *s'il y a moins de vulnérabilités, les attaques sont de plus en en plus importantes*« . Face à ces nouvelles menaces, de nouvelles technologies sont nécessaires.

Jimmy Kuo témoigne : « ***Les trojans évoluent peu en somme.*** *Lorsque l'attaque Conficker est arrivée, nous avons réalisé que son impact dépendait beaucoup de comment étaient configurés les ordinateurs des victimes. Cependant il a fallu* ***mettre à jour les bases de la cellule de réponse Microsoft*** (MSRT, ndr). *Maintenant nous sommes capables de détecter les nouvelles versions de Conficker*« . L'expert fait ici référence aux nouvelles versions du malware qui ont déjà sévi, capables d'infecter de nouveaux postes.

Il faut dire que le géant de **Redmond s'est fait taper sur les doigts par l'US-Cert** sur ces manques de sécurité à propos du ver Conficker/Downadup. L'éditeur s'est vu contraint de trouver une solution en développant une « rustine » spécifique qui corrige le bogue dans la **fonction AutoRun.** Une modidification qui sera diffusée en mode push à travers Windows Update.

Par la voix de Jimmy Kuo, Microsoft explique qu'il met en place un **système de détection automatique des exploits contre des vulnérabilités** (Conficker par exemple). Les différents modes opératoires de Conficker/Downadup sont par exemple la possibilité de tenter nombre de connexions via le réseau vers des postes non sécurisés, (**mots de passe trop faibles, postes peu voire peu mis à jours…**). Une technique qui lui permet de se diffuser plus rapidement.



Tout est question d'argent.**Les spams, le vol de données financières, les faux logiciels, les marchandises de type Viagra et autres sont faits pour générer de l'argent.** Depuis trois ans l'utilisation de rootkits (accès frauduleux à un système) s'est faite beaucoup plus importante. On voit grandir cette tendance dans la mesure où cette méthode peut contribuer à générer beaucoup d'argent ».

Là aussi, la **notion de confiance** prend de l'importance. Une définition contrebalancée par le fait que certaines méthodes (notamment le *phishing*) passent au delà de cette notion. L'utilisateur est alors berné par sa propre confiance qu'il porte envers un site. En ce sens, les réseaux sociaux sont des proies faciles. De nombreux liens fleurissent ('quelqu'un vous a pris en photo sur une webcam cachée') sur les sites communautaires afin d'induire en erreur l'internaute.

« ***Les logiciels de voix sur IP ne sont pas en reste.*** *Prenez Skype où de fausses alertes diffusent de faux bulletins de sécurité et vous proposent de nettoyer votre système. Un faux antivirus se cache alors derrière et ne fera qu'ouvrir une porte pour quelques* ***chevaux de Troie prêts à l'attaque«*** . Un combat compliqué puisque parfois de mauvais sites Web apparaissent plus haut dans la liste de recherche que les sites jugés sains.

Autre tendance, la propension qu'a eu le jeu en réseau ***World of Warcraft*** à être visé par les malwares. En 2005, le nombre d'infections a fait un bon gigantesque à cause des voleurs de mots de passe. Les virus **Win 32/Taterf** et **Win32/Frethog** ont infecté respectivement 127.833 joueurs et 44.859 rien que sur le territoire américain.

A en croire les responsables de Microsoft, le danger est partout et il convient de se protéger de tout. Alors que la sécurité est simple comme un clic… de vigilance. » />