Phishing: la fausse mise à jour Microsoft cache un 'Troyen'

Des pirates profitent de la publication mensuelle du bulletin de sécurité Microsoft pour entamer une campagne de phishing. Comme nous vous le révélions ce lundi, plusieurs éditeurs de solutions de sécurité ont détecté récemment une vague d'e-mails usurpés, prétendument envoyés par Microsoft, qui invitaient les internautes à télécharger une nouvelle mise à jour (« Wupdate-20050401.exe ») disponible à travers le site Windows Update.

Or, il s'agit là d'un site pirate, un piège, qui distribue à qui veut bien cliquer un cheval de Troie nommé « Troj/dsnx-05 ». Une fois installé, ce « malware » ouvre une porte dérobée (backdoor) qui permet au pirate de se connecter sur la machine infectée à l'insu de son utilisateur. La ressemblance du site pirate avec le véritable site Windows Update est frappante (voir photo). A cette heure, le piège semble être « hors ligne », cependant, d'après les spécialistes, ces attaques devraient être de plus en plus fréquentes. Microsoft, le vrai, en profite pour rappeler sa politique de diffusion d'alertes et de mises à jour. L'éditeur de Redmond ne joint jamais aucun fichier à ses emails qui sont toujours rédigés au format texte (pour les alertes et bulletins de sécurité). Quant au site Windows Update, il est préférable de saisir manuellement l'adresse plutôt que de cliquer sur un lien présent dans un e-mail. Méfiance donc. (*) **pour Vulnerabilite.com**