Un cheval de Troie exploite les événements de Birmanie pour se propager

L'actualité est un des moyens préférés des malfaiteurs de la Toile pour propager les menaces. Déjà lors du terrible tsunami dans l'océan indien en 2005, mais aussi suite à la mort du pape Jean-Paul II, ou bien encore après le crash du Concorde et les attentas de Londres, les cybercriminels avaient multiplié les hoax, spams, virus et Trojan sur ces thèmes. Le message de spam utilisé, se fait passer pour un mail de soutien aux moines et aux manifestants birmans. Il est soi-disant signé par le leader du mouvement bouddhiste, le Dalaï-Lama. Il contient un fichier en pièce jointe qui essaye de contaminer le PC de la cible. La pièce jointe contient un document nommé (hhdl burma_001.doc) qui essaye d'exploiter une vulnérabilité dans Word en téléchargeant un cheval de Troie, nommé Agent-CGU, sur la machine de la victime. Pour renforcer la crédibilité de l'email, un lien renvoyant vers le site officiel du Dalaï-Lama est visible à la fin du message. Une version française du spam est également en circulation, et ce n'est pas le fruit du hasard puisque la communauté bouddhiste française est l'une des plus importantes d'Europe. L'utilisation de l'actualité est une des méthodes favorites des hackers. Presque toutes les tragédies sont exploitées par les cybercriminels.

« Le régime au pouvoir en Birmanie tente de bloquer les nouvelles en provenance du pays en fermant les cafés Internet et en contrôlant les accès au Web. C'est sans doute ce qui a donné aux pirates l'idée d'exploiter la situation pour mieux répandre leur programme malveillant » , commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud.

« Cette manière d'exploiter l'actualité pour inciter les utilisateurs à cliquer sur le virus est loin d'être neuve, mais il faut croire qu'elle fonctionne toujours, ou les pirates l'auraient abandonnée depuis longtemps. S'en protéger est avant tout affaire de bon sens et de prudence vis-à-vis de messages d'origine inconnue. »

Extrait du message (en anglais dans l'original) :*« Chers Amis et collègues Veuillez trouver en lien un message de Sa Sainteté le Dalaï-Lama qui exprime son soutien aux manifestations démocratiques qui se déroulent dans le pays. Vous pouvez librement redistribuer cet email à vos contacts. Salutations. Tenzin Taklha, le conseiller du Dalaï-Lama «*