L'affaire Wikileaks sous l'oeil de Barracuda Networks, qui met en garde les usagers

Depuis la diffusion le 28 novembre de 250.000 notes confidentielles de la diplomatie américaine, Wikileaks n'a cessé de se battre pour rester en vie. Barracuda Networks, revient sur le jeu d'attaques- contre attaques auquel Wikileaks doit faire face.

Pour obtenir les dates clés de la saga Wikileaks, vous pouvez vous rendre sur le blog de Barracuda Labs : **www.barracudalabs.com/wordpress/index.php/2010/12/10/wikileaks-saga/**

L'analyse Technique

Après le retrait brutal du soutien de ses partenaires dont PayPal, Visa et Mastercard, Wikileaks.org s'est retrouvé en difficulté. Néanmoins, afin de fermer définitivement le site, les autorités ont dû aller au-delà du Déni de Service Distribué (DDoS) et ont dû se livrer à un jeu de pouvoir pour s'assurer qu'aucun serveur ne l'héberge. La raison pour laquelle les autorités ont dû se plier à ce jeu est la suivante : les services d'hébergement Cloud sont beaucoup plus résistants aux tentatives DDoS. Finalement, peu importe la manière dont Wikileaks.org a été affaibli, c'est la nature digitale de ses contenus qui le maintient en vie.

Le 3 décembre, Wikileaks a déménagé sur son domaine backup Wikileaks.ch, enregistré en Suisse mais hébergé en Suède dont une partie des câbles est hébergée par la société française OVH, un fournisseur français de solutions de téléphonie et d'hébergement internet. Par ailleurs, il existe quelques 1100 sites miroirs de Wikileaks.org déjà disponibles (et répertoriés).

Alerte aux usagers:

1. Alors que Paypal (4 Décembre), Mastercard (6 Décembre) et Visa (7 Décembre) ont bloqué tout paiement vers Wikileaks, de nouveaux acteurs, inconnus jusqu'alors, ont poussé comme des champignons et ont manifesté leur soutien au site. Il est plus que probable que certaines personnes essayerons de tirer profit de cette situation pour détourner les dons, donc soyez vigilant face à ces sites.

2. Il existe un bon nombre de groupes anonymes de riposte qui organisent des « botnets » (de très grands réseaux dont les ordinateurs sont infectés avec un cheval de Troie. L'auteur du cheval de Troie contrôle l'ordinateur infecté, qui alors réagit à ses ordres quasi automatiquement comme le feraient des robots) pour faciliter les attaques DDoS (denial of service) contre les organisations qui ont retiré leur soutien à Wikileaks. Le recrutement au sein de ces groupes se fait en envoyant une demande de téléchargement qui permettra à l'ordinateur de la nouvelle recrue de prendre part au « botnet ». Cependant, prendre part à de telles activités serait a) illégal et b) exposerai l'ordinateur à des virus/spyware ou d'autres programmes malveillants.

3. Beaucoup de sites miroirs déclarent héberger les contenus originaux de Wikileaks, cependant aucune preuve n'est apportée. Les sites miroirs n'étant pas vérifiés, il est plus que probable que des

groupes malintentionnés les utilisent par la suite à des fins malveillantes. Les sites qui fonctionnent avec du contenu disséminé tel que Torrents sont signés d'une clé publique ; cependant, les sites web ne le sont pas.