Black-listes : scandale en Grande-Bretagne

Sous le prétexte que de nombreux internautes abonnés au service du câble de Telewest possèdent des ordinateurs transformés en machines zombies, la firme

Spam Prevention Early Warning System (Spews) spécialisée dans les 'black-listes' a mis à l'index plus d'un million d'adresses! Les machines « zombies » sont les victimes d'infections virales qui les transforment en serveurs d'e-mails contrôlables à distance par des pirates, afin d'expédier en masse des e-mails spammés qui renferment généralement des vers ou des virus. Ayant fait ce constat, Spews a donc fait le choix de très largement mettre au rebut (ou 'black-lister') des adresses en provenance de l'opérateur du câble. Ce dernier reconnaît d'ailleurs l'objection! Et affirme travailler à la résolution de ce problème très en amont afin de protéger ses clients. Les 'black-listes' sont une solution à laquelle de nombreux acteurs de la sécurité Internet et des réseaux font appel. Ce système est très simple, puisqu'il consiste à comparer l'adresse d'origine d'un e-mail, voire d'un site Web, avec une liste d'adresses déclarées dangereuses, donc à éviter. Dans cette affaire, c'est l'importance du volume des adresses black listées qui surprend. Y aurait-il donc autant d'ordinateurs victimes des pirates informatiques et transformés en PC zombie ? La question est posée, mais il semble que Spews soit allé un peu vite en besogne ! Ainsi, Matt Peachey, directeur européen de Ironport – un service de surveillance des adresses Internet qui évalue l'ampleur de la menace des spammers – évalue le nombre d'ordinateurs abonnés aux réseaux Telewest sur lesquels un moteur d'e-mails aurait été installé à l'insu de leurs utilisateurs à seulement 16.000 postes ! Certes, cette étude révèle qu'un PC zombie adhérant aux réseaux Telewest peut envoyer plus de 100.000 e-mails par jour. Mais malgré les dégâts que cela représente, et le risque omniprésent de voir se multiplier les postes vérolés au travers du réseau, fallait-il bloquer l'accès d'un million d'utilisateurs sachant que 1,6% seulement d'entre eux sont probablement vérolés ? Cette affaire relance le débat autour des black listes. Et des faux positifs qui les accompagnent. C'est-à-dire des parfois nombreuses adresses Internet bloquées par ces systèmes pour des problématiques de redondance, de proximité sémantique, voire d'adhésion à des communautés jugées peu fiables. Alors qu'elles ne représentent aucun danger et qu'elles sont généralement utilisées par des internautes innocents, mais victimes d'un système qui va parfois trop loin !