‘Drive-by pharming’ : les routeurs du Net seraient en danger

Symantec et l’*Indiana University Scholl of Informatics* ont découvert une nouvelle menace qui pourrait toucher un accès internet au domicile sur deux, le ‘***drive-by pharming***‘.

Cette technique est dérivée du ‘***pharming***‘, qui consiste à dérouter l’internaute ? en modifiant la page d’accueil du navigateur ou en manipulant le serveur de DNS (*Domain Name Server*) ? vers un autre site qui renferme une menace, généralement sous la forme d’un code vérolé.

Avec le ‘*drive-bu pharming*‘, la visite du site web vérolé permet à l’attaquant de modifier à distance les réglages du routeur ou de l’accès sans fil afin de détourner l’internaute vers un site pirate, qui imite généralement un service financier, afin de dérober l’information qui sera saisie par l’internaute.

Les routeurs d’accès internet sont protégés par un mot de passe, mais la majorité des internautes ne prennent pas le temps de modifier celui qui est d’origine livré avec la machine, avec toutes les machines ! Les pirates l’ont compris et exploitent cette faiblesse, qui aujourd’hui menace des millions d’internautes.

Le danger est d’autant plus important que de nombreux internautes ne mettent pas à jour leurs environnements de protection – pare-feu, antivirus, détection des intrusions, etc. – ou continuent de penser qu’ils sont protégés alors que le logiciel de sécurité est arrivé à expiration depuis longtemps. Le pirate peut donc par ce biais prendre le contrôle du PC à l’insu de son utilisateur.

Cette faille dans la sécurité des accès internet, qui menace selon Symantec un accès au domicile sur deux, est d’abord le fruit d’un défaut d’éducation. Avant d’envisager de s’équiper d’outils de protection, un simple geste suffirait en effet pour se protéger de la menace du ‘*drive-by pharming*‘, changer le mot de passe par défaut du routeur?

Quant à Graham Cluley, le directeur technique de Sophos, il donne un conseil simple : établir une nouvelle ligne de défense en désactivant le JavaScript en provenance de sites web non sécurisés. La première solution est sans aucun doute la plus simple, demander à un internaute qui n’a pas su modifier son mot de passe d’accès au routeur d’aller modifier le paramétrage de son navigateur relève de l’exploit?