Barracuda : ma backdoor ne vient pas de la NSA

Suite à notre article « Espionnage de la NSA : les 8 leçons d'Edward Snowden », dans lequel **la présence de backdoor dans des VPN et Firewall Barracuda** est mentionnée, cette société nous écrit, estimant que cet article prête à « *confusion* ». Basé sur le rapport de la société Lexsi, notre article mentionnait la présence de backdoor ou vulnérabilités dans de nombreux produits de marques diverses (Juniper, Cisco, Dell, Huawei…). Dont Barracuda. Sans toutefois affirmer que la NSA aurait eu un rôle quelconque dans l'implantation de ces backdoor. « *Nous n'avançons pas le fait que la NSA ait demandé l'implantation de ces portes dérobées* », confirme Vincent Hinderer, un des deux auteurs de l'étude de Lexsi joint ce jour au téléphone.

Barracuda estime pourtant « *que le lien direct fait par M. Gadiolet (l'autre auteur de l'étude, NDLR) entre cette faille temporaire et une association quelconque avec la NSA et une* ***sur-interprétation de la réalité****, qui n'a aucun fondement* ». Et de préciser : « *La vulnérabilité des accès à nos produits, découverte il y a plus d'un an, avait pour cause un problème de maintenance, qui a été immédiatement réparé. De plus, nos clients ont été immédiatement et de manière transparente, informés du souci et de la façon d'y remédier. Nous souhaitons appuyer sur le fait que les gammes Barracuda NG Firewall et Barracuda Firewall et leurs accès VPN n'ont même pas été concernées par ce souci, puisqu'elles sont basées sur une technologie différente.* » Les solutions NG Firewall et VPN sont développées en Autriche, « *sous la direction du Dr Klaus Gheri, vice-président du département réseau sécurité chez Barracuda Networks* ». Certes. Mais le siège de Barracuda est lui situé en Californie. La société est donc directement soumise au droit américain.

Comptes utilisateurs oubliés

Suite à l'affaire RSA, la filiale sécurité de EMC soupçonnée d'avoir employé un algorithme de cryptage perméable à la demande de la NSA, **de nombreuses interrogations entourent les sociétés américaines**. Le Web fourmille de questions quant à l'origine de vulnérabilités découvertes dans certains produits. Selon Bloomberg, l'agence de Fort Meade était ainsi au courant de la faille Heartbleed environ deux ans avant sa divulgation, en avril dernier. Autrement dit, l'agence avait l'information en mains quasiment depuis l'introduction de la faille dans la bibliothèque OpenSSL, en janvier 2012.

Découverte en novembre 2012 par des chercheurs autrichiens, la vulnérabilité touchant Barracuda permettait des **accès non autorisés à un certain nombre d'appliances** de la marque (Barracuda Spam & Virus Firewall, Barracuda Web Filter, Barracuda Message Archiver, Barracuda SSL VPN, Barracuda Web Application Firewall version 7.6.4 et versions antérieures, ainsi que CudaTel). Liée à la présence de comptes utilisateurs inutiles et à leur accès distant, la vulnérabilité a été rapidement réparée, via deux correctifs proposés aux utilisateurs fin janvier et début février 2013. Barracuda avait alors parlé d'une lacune résultant d'un « *défaut dans la configuration des firewall* » concernés et de la « *présence de comptes utilisateurs par défaut sur les unités* ».

crédit photo © Pavel Ignatov – shutterstock

A lire aussi :

NSA : les matériels Cisco, Juniper et Huawei transformés en passoire