Un site du ministère de la Défense détourné vers l'Allemagne

Les infrastructures des institutions françaises sont de nouveau victimes de piratage. Après les attaques informatiques qui ont secoué Bercy en mars dernier, c'est **au tour du ministère de la Défense de subir les affronts des pirates**.

L'éditeur Vade Retro Technology annonce avoir découvert, le 10 juin dernier, **une attaque de type « DNS Poisoning »** (ou empoisonnement du cache DNS) de haut niveau sur l'un des sites Internet du ministère de la Défense. Autrement dit, le serveur de noms de domaine (qui traduit les adresses alphabétiques comme Silicon.fr en adresses numériques IPv4 ou IPv6, seules à même d'être interprétées par les serveurs web) avait été modifié pour diriger des requêtes à destination d'un des sites du ministère des Armées vers un site web marocain hébergé en Allemagne, précise l'éditeur français.

« En conséquence l'ensemble des requêtes qui étaient faites auprès de ce serveur DNS et de ses fils répercutait une fausse information en prétendant que le nom de domaine du ministère de la Défense Française correspondait à ***une adresse IP localisée en Allemagne****. Situation pas impossible mais plutôt cocasse… »*, note Vade Retro. Il serait effectivement intéressant de savoir quel était l'objet des pirates derrière ce détournement de domaine. A noter que le site web en question du ministère est bien hébergé en France, chez Oleane précisément. Mais la nature de ce site n'est pas dévoilée.

C'est en constatant la présence d'**une activité de *phishing*** sur ce serveur que Vade Retro a pu enquêter et constater la corruption du serveur DNS. Le site web en lui-même n'a pas été affecté par l'attaque. Rappelons que Vade Retro fournit une solution anti-spam utilisée par plus de 100 millions de boîtes dans le monde.

Plus de peur que de mal, apparemment. *« Cette technique n'a été utilisée fort heureusement que pour une simple opération de phishing commercial »*, souligne Vade Retro. Mais l'aventure aurait pu mal tourner : *« Un hacker plus entreprenant aurait pu créer une copie à l'identique du site visé et ainsi récupérer par exemple des noms d'utilisateurs et mots de passe d'agents gouvernementaux. »* Ce qui n'aurait pas manqué de faire son petit effet, médiatique notamment, très dommageable en terme d'image de marque et de sécurité pour la Défense française. La situation est revenue à la normale dès le 11 juin au matin. Jusqu'à la prochaine attaque?