Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Affaire suivie par :
Florian MAURY

Paris, le 31 AOUT 2016
N° 3514 /ANSSI/SDE/ST/LRP

Note
à
destinataires *in fine*

Objet : Sécurisation des noms de domaine contre les attaques par détournement DNS.

Référence : Guide ANSSI « Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine », disponible en ligne sur http://www.ssi.gouv.fr/guide-dns.

L'exploitation de vulnérabilités d'applications web est la méthode la plus employée pour porter atteinte à des sites Internet, aussi bien à des fins de défiguration ou de déni de service que de captation de données. Cependant, même les sites correctement sécurisés restent potentiellement vulnérables à des attaques affectant la résolution des noms de domaine, dites « attaques DNS ».

De telles attaques peuvent notamment prendre la forme de détournements DNS[1], qui consistent à modifier les informations relatives aux noms de domaine renseignées auprès des bureaux d'enregistrement. Un attaquant peut par exemple tenter de modifier la liste des serveurs DNS responsables d'un domaine, pour la remplacer par des serveurs sous son contrôle. En cas de succès, l'attaquant pourra ensuite rediriger les utilisateurs de n'importe quel service du domaine détourné vers un autre serveur sous son contrôle. Outre les serveurs web, une telle attaque est susceptible d'affecter également des services de messagerie électronique, ou tout autre service en ligne.

Des cas avérés de détournements DNS ont régulièrement été rapportés par la presse ces dernières années. La *Syrian Electronic Army* a par exemple mené ce type d'attaque en 2014 contre plusieurs sites à forte visibilité, comme le *New York Times*, *Ebay* ou *Paypal*. Les rapports publiés à la suite de ces événements mentionnent généralement soit une compromission du bureau d'enregistrement ou de l'un de ses revendeurs, soit un vol des mots de passe permettant d'accéder aux interfaces d'administration du nom de domaine.

Les contremesures à ces attaques se classent en deux catégories : le renforcement du contrôle d'accès d'une part, et la validation manuelle des opérations critiques d'autre part. Ces approches et les recommandations associées sont détaillées dans le guide de l'ANSSI cité en référence.

[1] En anglais, *DNS hijack*.

Depuis 2015, l'*AFNIC*, responsable notamment de la gestion des noms de domaine en .fr, propose un mécanisme de validation manuelle des opérations critiques, connu sous le nom de « verrou de registre » ou *« .fr lock »*. Ce mécanisme, une fois activé, prévient toute modification administrative ou technique du domaine verrouillé. Son déverrouillage suit une procédure impliquant l'*AFNIC* et le bureau d'enregistrement en charge du domaine, qui comprend notamment une intervention humaine et des vérifications d'autorisation.

L'activation du *« .fr lock »* nécessite que l'option soit prise en charge par le bureau d'enregistrement[2]. Cette option est généralement payante, de l'ordre de quelques dizaines d'euros par mois. Elle est parfois également disponible pour des noms de domaine relevant d'autres gestionnaires de noms de premier niveau, comme .com, .net ou encore .co.uk.

Compte tenu de son apport en sécurité, l'ANSSI recommande l'activation des verrous de registre pour les noms de domaine sensibles, lorsque l'option est disponible et que la procédure de déverrouillage proposée est compatible avec les contraintes opérationnelles.

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

[2] À ce jour, une vingtaine de bureaux d'enregistrement ont signé un contrat avec l'*AFNIC* pour la prise en charge du verrou de registre.