MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
Liberté
Égalité
Fraternité

Direction des
Affaires juridiques

Lettre de la DAJ – Extension du domaine de la lutte… contre le cybersquattage

20/04/2023

La lutte contre le cybersquattage des identités de l'Etat est une politique de la DAJ (mission APIE) qui a été initiée en 2022 avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et dont le déploiement s'étend, en 2023, à l'ensemble des ministères.

©ArtemSam - stock.adobe.com

La dématérialisation croissante des services publics s'accompagne d'un accroissement du nombre d'arnaques sur Internet, se traduisant notamment par la création de noms de domaine reproduisant ou imitant des signes identitaires de l'Etat, qui pénalisent avant tout les citoyens et consommateurs.

La mission APIE intervenait jusqu'en 2021, de manière ponctuelle, pour protéger les identités de l'Etat visées par des acteurs malveillants sur internet[1]. La passation par l'ANSSI d'un marché global de lutte contre le cybersquattage des identités de l'Etat a permis de mettre en œuvre à partir de 2022 une politique systématique de protection contre les attaques de sites internet de l'Etat en recourant à un prestataire spécialisé et aux expertises juridiques et actions de défense de la mission APIE. Une phase expérimentale s'est déroulée en 2022 en ouvrant ce service de veille et défense à quelques ministères, et portant sur une centaine de termes sélectionnés pour leur degré de sensibilité (sites collectant des données bancaires ou personnelles, sites régaliens, sites de forte fréquentation publique).

Concrètement, l'APIE analyse la liste des noms de domaine litigieux issus de la surveillance quotidienne réalisée par le prestataire et décide différentes actions selon le degré de menace : mise sous surveillance par le prestataire, demande de suspension du site manifestement illicite auprès de l'hébergeur[2], lettre de mise en demeure au propriétaire du nom de domaine pour cesser les atteintes identifiées. Ces actions peuvent ensuite donner lieu à des procédures alternatives de règlement des litiges, en demandant la suppression du site litigieux ou son transfert à l'Etat, s'il apparait stratégique.

Les attaques identifiées en 2022 ont principalement porté sur des sites très largement consultés, comme celui des impôts ou FranceConnect, des sites relatifs au paiement des amendes, aux prestations d'assurance maladie ou de carte vitale ou à la délivrance de vignettes Crit'air. La technique la plus fréquente est celle du « site miroir » qui copie fidèlement un site public avec des signes officiels (Marianne, couleurs bleu blanc rouge) et un nom de domaine proche de l'adresse officielle (par exemple : « impots-gouv-fr.com » ou « vignette-critair-officiel.fr »). Même en l'absence de site actif, la configuration d'un serveur de messagerie sur un nom de domaine litigieux laisse craindre des opérations d'« hameçonnage » (ou « phishing ») avec pour objectifs d'obtenir des paiements indus ou des informations bancaires ou encore de tenter de récupérer des données personnelles pour les monnayer par la suite. Ce risque de phishing peut également faire l'objet d'actions juridiques.

Depuis le lancement du dispositif, plus de 4 300 noms de domaine ont été analysés et environ 4 000 ont été placés sous surveillance. Près de 1 300 sites manifestement illicites ont été bloqués et les actions juridiques ont permis la suppression ou le transfert à l'Etat d'une vingtaine de noms de domaine stratégiques.

Au regard des résultats très positifs obtenus en un an, il a été décidé d'étendre le dispositif, qui s'inscrit dans la priorité gouvernementale de lutte contre la fraude à

[1] Aux termes de l'article 1 du décret n° 2021-264 du 10 mars 2021, la DAJ «est chargée de la gestion des portefeuilles de marques » de l'Etat ; « elle engage, avec l'accord de ces administrations, toute action administrative ou précontentieuse utile à la protection de leurs marques. Elle peut également engager de telles actions en vue de la protection de leurs noms de domaine et plus généralement de leurs signes distinctifs. »
[2] Article 6.2 de la loi n° 2004-575 pour la confiance dans l'économie numérique (LCEN)

l'ensemble des ministères en 2023. Le dispositif trouvera ainsi à s'appliquer à tous les domaines d'action et d'intervention de l'Etat.