LA DÉFIGURATION

La défiguration est l'altération par un pirate de l'apparence d'un site Internet, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l'objet initial du site, voire une courte mention comme « owned » ou « hacked ». La défiguration est le signe visible qu'un site internet a été attaqué et que l'attaquant en a obtenu les droits lui permettant d'en modifier le contenu. Durant l'attaque, le site n'est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité. Par ailleurs, en étant visible publiquement, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales…) : ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…

BUT RECHERCHÉ

DÉMONTRER UNE PRISE DE CONTRÔLE DU SITE ET LE FAIRE SAVOIR
avec différents objectifs : la recherche de notoriété, la revendication politique ou idéologique, l'atteinte directe à l'image du site, et/ou le vol d'informations sensibles.

SI VOUS ÊTES VICTIME

Si possible, **DÉCONNECTEZ D'INTERNET** la machine concernée.

RÉCUPÉREZ LES FICHIERS DE JOURNALISATION (logs) de votre pare-feu, serveur mandataire (proxy) et des serveurs touchés qui seront des éléments d'investigation.

RÉALISEZ UNE COPIE COMPLÈTE DE LA MACHINE attaquée et de sa mémoire.

IDENTIFIEZ LES ÉLÉMENTS SENSIBLES qui ont pu être copiés ou détruits.

IDENTIFIEZ LE VECTEUR qui a permis de prendre le contrôle de la machine.

DÉPOSEZ PLAINTE au commissariat de police ou à la gendarmerie dont vous dépendez et tenez à disposition des enquêteurs tous les éléments de preuves en votre possession.

Lorsque vous aurez repris le contrôle de la machine touchée, **CORRIGEZ TOUTES LES VULNÉRABILITÉS ET CHANGEZ TOUS LES MOTS DE PASSE** avant de la remettre en ligne.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur www.cybermalveillance.gouv.fr des prestataires spécialisés susceptibles de pouvoir vous apporter leur expertise.

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système d'exploitation et des logiciels installés sur vos serveurs.

Ayez un pare-feu correctement paramétré : fermez tous les ports inutilisés et ne laissez que les adresses des machines indispensables accéder aux fonctionnalités d'administration du site.

Consultez régulièrement les fichiers de journalisations (logs) de votre pare-feu afin de détecter toute tentative d'intrusion, ainsi que les logs de vos serveurs exposés pour identifier les tests de mots de passe suspects en particulier.

Vérifiez que les mots de passe sont suffisamment complexes et changés régulièrement, mais également que ceux créés par défaut sont effacés s'ils ne sont pas tout de suite changés (fiche mots de passes sur www.cybermalveillance.gouv.fr).

Sensibilisez les utilisateurs à ne jamais communiquer d'éléments d'accès administrateurs et d'authentification à un tiers non identifié (ingénierie sociale, hameçonnage, etc.).

Ne conservez pas de manière accessible la liste nominative des personnes possédant les droits d'administrateur sur le serveur.

LES **INFRACTIONS**

L'incrimination principale qui peut être retenue ici est celle de l'**entrave à un système de traitement automatisé de données** (STAD ou système d'information).

Les **articles 323-1 à 323-7 du code pénal** disposent que :

- « le fait d'accéder ou de se maintenir, frauduleusement » dans un système de traitement automatisé de données (par exemple en utilisant le mot de passe d'un tiers ou en exploitant sciemment une faille de sécurité) ;
- « le fait d'introduire frauduleusement des données » dans un système de traitement automatisé de données. Ce texte peut s'appliquer dans le cadre de la défiguration de site. La défiguration désigne la modification non sollicitée de la présentation d'un site Web, à la suite d'un piratage du site ;
- le fait « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données » d'un système de traitement automatisé de données. La copie frauduleuse de données (souvent improprement qualifiée de « vol » de données) pourra être donc sanctionnée sur ce fondement ;
- « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données » ;
- les tentatives de ces infractions sont punies des mêmes peines.

En fonction du cas d'espèce, les peines encourues sont de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.