LA DÉFIGURATION

La défiguration est l'altération visuelle de l'apparence d'un site Internet piraté. La nouvelle apparence du site peut être uniformément noire, blanche ou comporter des messages, des images, des logos et 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 web a été attaqué et que le ou les attaquants en ont obtenu les droits, leur permettant ainsi d'en modifier le contenu.

La défiguration est un acte qui peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site n'est souvent plus utilisable au moins partiellement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité. Par ailleurs, ce type d'attaque est visible publiquement voire médiatiquement et démontre que l'attaquant a pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données y compris les plus sensibles (données personnelles, bancaires, commerciales…), ce qui porte directement atteinte à la notoriété, au sérieux, donc à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…

BUT RECHERCHÉ

Le but premier de l'attaquant est de démontrer qu'il a pu prendre le contrôle du site et de le faire savoir.

Ses motivations peuvent être la recherche de notoriété dans les communautés de pirates informatiques, la revendication politique ou idéologique en ciblant des sites Internet de grande visibilité publique ou au contraire en jouant sur l'effet de masse en attaquant de nombreux sites de moindre visibilité. Dans certains cas, il peut s'agir pour l'attaquant de chercher de porter directement atteinte à l'image du propriétaire du site attaqué.

Enfin, l'attaquant pourra profiter de la défiguration pour voler des informations sensibles stockées sur le site Internet défiguré tels des données personnelles, bancaires, des listes de comptes et mots de passe, ou des documents confidentiels afin de les publier, les revendre voire les utiliser pour commettre d'autres actes frauduleux.

MESURES PRÉVENTIVES

- Appliquez de manière régulière et systématique les correctifs 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 de votre pare-feu afin de détecter toute tentative d'intrusion, ainsi que les fichiers de journalisation de vos serveurs exposés pour identifier les tests de mots de passe suspects en particulier.
- Vérifiez que les identifiants et mots de passe sont suffisamment complexes et changés régulièrement (voir www.ssi.gouv.fr/guide/mot-de-passe/) mais également que ceux créés par défaut sont effacés s'ils ne sont pas tout de suite changés.
- 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.

SI VOUS ÊTES VICTIME

- Coupez si possible la machine concernée d'Internet.
- Essayez de récupérer ou de faire récupérer les fichiers de journalisation (log) de votre pare-feu et des serveurs touchés qui seront des éléments d'investigation.

LA DÉFIGURATION

- Réalisez ou faites réaliser une copie complète de la machine attaquée et de sa mémoire.
- Tentez d'identifier ou de faire identifier les éléments sensibles qui ont pu être copiés ou détruits.
- Identifiez ou faites identifier le vecteur qui a permis de prendre le contrôle de la machine.
- Déposez plainte au commissariat de police ou à la gendarmerie la plus proche et tenez à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.
- Lorsque vous aurez repris le contrôle de la machine touchée, toutes les vulnérabilités identifiées doivent être corrigées et tous les mots de passe changés avant de la remettre en ligne.

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 :

- « 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 € à 300 000 € d'amende.