RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

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 Web 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 ou alertez votre hébergeur pour qu'il prenne les mesures nécessaires.

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 (COPIE PHYSIQUE) DE LA MACHINE attaquée et de sa mémoire.

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

Professionnels: **NOTIFIEZ CET INCIDENT À LA CNIL** s'il y a eu une violation de données à caractère personnel.

IDENTIFIEZ LA SOURCE DE L'INTRUSION et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

DÉPOSEZ PLAINTE au commissariat de police ou à la gendarmerie ou en écrivant au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

Lorsque vous aurez repris le contrôle de la machine touchée, **CORRIGEZ TOUTES LES FAILLES DE SÉCURITÉ 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 professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.

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 (tous nos conseils pour gérer vos mots de passe).

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.

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION