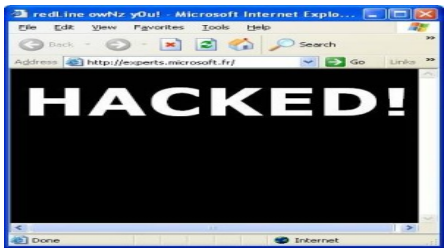
Sécurité économique territoriale
Rhône-Alpes

MESSAGE D'ATTENTION
DEFACEMENT DE SITES INTERNET

Suite aux récents événements tragiques, de nombreuses cyber-attaques touchent actuellement les sites internet français ayant un nom de domaine en « *.fr* ».

Commises de manière aléatoire, ces attaques appelées «*défacement ou défaçage*» ont déjà touché plusieurs centaines de sites en six jours et devraient s'amplifier dès le 15 janvier 2015.



DE QUOI PARLE-T-ON ?

Le « *défacement ou défaçage* » consiste à défigurer un site internet classique en remplaçant la page d'accueil originale par une autre. Il est provoqué par l'exploitation d'une faille présente sur la page web ou tout simplement une faille du système d'exploitation du serveur web.

Une page défacée peut contenir un ou plusieurs éléments :

- **un fond uni (souvent noir), qui peut être le seul indice de défacement d'un site ;**
- **un simple mot, comme *owned*, *hacked* ou le pseudonyme du défaceur ;**
- **une image, les revendications du défaceur et quelques fois un fichier audio.**

Le risque premier de ce type d'attaque est l'atteinte à l'image de marque de la société, ceci mettant en exergue l'existence de sérieux problèmes de sécurité. En effet, il s'agit d'une intrusion dans le système d'information ayant permis de modifier des données visibles par tous. Même si le serveur web est isolé, même si aucune donnée sensible n'est dérobée, la réputation du propriétaire du site elle, en sort grandement affectée.

QUE FAIRE ?

Les conséquences de telles attaques pouvant avoir un impact catastrophique sur l'image et le fonctionnement de l'entreprise, il convient d'y apporter une attention particulière. Il est donc conseillé de :

Mettre rapidement à jour **votre site internet ou** ***demander à votre prestataire*** **de services d'effectuer ces opérations dans les plus brefs délais. Appliquer les correctifs de sécurité et configurer correctement les applications ;**

Contrôler l'intégrité **et** ***mettre en place des journaux d'événements*** **(*serveurs, pare-feu, …*) ;**

Effectuer des sauvegardes complètes régulièrement **et** ***des bases de données quotidiennement. D*****ans la mesure du possible,** ***installer un plugin*** **automatisant cette opération ;**

Si vous avez un utilisateur nommé « *admin* » (*souvent l'administrateur par défaut du site*), les pirates tenteront d'entrer dans l'interface par ce biais. ***Créer un nouveau compte utilisateur*** **en choisissant un nom différent auquel vous adjoindrez un** ***mot de passe fort*** **(*minimum 14 caractères, mélange de caractère alphanumériques, lettre majuscules et minuscules et symboles*).**

Si le site s'est déjà fait pirater, ***effectuer un scan*** **afin d'obtenir la liste des fichiers corrompus.**

En cas d'atteinte, ***prendre toutes mesures de préservation des preuves numériques*** **(*blocage du site ou copie des journaux de logs, copies d'écrans, information des éventuelles victimes en cas de vol de bases de données (clients, membres, …)*).**

Les pirates sont en perpétuelle quête de potentielles failles en vue de les exploiter. Il convient donc de prendre quelques instants afin de sécuriser son site.

Attention : « *Le risque zéro n'existe pas !!!* »

En cas de problème avéré :

Déposer rapidement plainte **auprès du service de police ou de gendarmerie territorialement compétent.**

Lettre électronique N° 4 éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp - ☎: 04.37.85.21.00
Rédaction : Cellule Intelligence Économique régionale