Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Unité de pilotage informatique de la Confédération UPIC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

GovCERT.ch

Instructions relatives à la suppression des maliciels sur les sites Internet

MELANI / GovCERT.ch

Version	v1.00
Auteur	MELANI / GovCERT.ch

[1] http://creativecommons.org/licenses/by-nd/3.0/ (en anglais)

Si vous lisez ces lignes, c'est probablement que votre fournisseur de services Internet ou votre hébergeur Internet vous a signalé que votre ordinateur était infecté ou que votre site Internet a été piraté. Les instructions suivantes vous indiquent, étape par étape, comment nettoyer puis sécuriser votre site Internet. Elles s'appliquent indépendamment du système d'exploitation de votre ordinateur.

Introduction

Pour accéder au contenu d'un site Internet, les pirates informatiques et les cybercriminels recourent à deux techniques largement répandues:

- **Le vol des données d'accès**: des cybercriminels ont dérobé les données d'accès à l'administration de votre site (par exemple données d'accès FTP). Pour accéder à ces données, les cybercriminels installent le plus souvent un logiciel malveillant (par exemple un cheval de Troie) sur l'ordinateur d'une victime qui gère un site Internet. Dès que cette personne, (ci-après: l'administrateur du site) accèdera à l'administration du site au moyen de FTP ou d'une interface web, les informations qu'elle aura utilisées pour se connecter (nom d'utilisateur et mot de passe) seront copiées puis transmises aux cybercriminels. Ces derniers ont ainsi un accès illimité au site Internet concerné et peuvent donc modifier n'importe quels contenus sur ce site, voire ajouter de nouveaux contenus dommageables.

- **L'exploitation des systèmes de gestion de contenu obsolètes**: logiciels très répandus, les systèmes de gestion de contenu («Content Management System», CMS), tels que WordPress, Joomla ou Typo3, de même que leurs modules d'extension («plug-ins») constituent des cibles idéales pour les pirates informatiques et les cybercriminels. Ceux-ci détectent souvent des lacunes de sécurité dans le code du programme et les utilisent afin d'installer des codes malveillants (maliciels) ou des pages d'hameçonnage («phishing») sur les sites Internet utilisant des CMS ou plug-ins obsolètes.

Suppression des maliciels

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération (MELANI) recommande d'appliquer la procédure suivante afin de vous débarrasser des maliciels:

1. *Localiser le logiciel malveillant sur le site Internet concerné*
   Les pages et les répertoires concernés doivent faire l'objet d'un examen approfondi. Il est bien possible que le même maliciel se soit introduit dans plusieurs sous-pages ou que d'autres maliciels aient infecté un même répertoire. Il faut faire particulièrement attention aux fichiers du répertoire dont l'extension est **.exe**. Si vous ne parvenez pas à localiser le maliciel, nous vous recommandons de contacter votre hébergeur Internet.

2. *Supprimer le logiciel malveillant*
   Après avoir localisé le maliciel, vous devez le supprimer. Dans certains cas, une ancienne sauvegarde peut vous être utile.

3. *Mettre à jour le système de gestion de contenu (CMS)*
   Si vous utilisez un CMS tel que WordPress, Joomla ou Typo3, assurez-vous d'avoir installé la version la plus récente. Vous empêcherez ainsi les cybercriminels d'introduire de nouveaux maliciels sur votre site Internet en exploitant la même faille de sécurité de votre CMS. Vous trouverez la dernière version des CMS sur le site de leur fournisseur respectif:

   - WordPress: http://wordpress.org/
   - Joomla: http://www.joomla.org/
   - Typo3: http://typo3.org/

   Attention: les modules d'extension («plug-ins») doivent également être mis à jour. Les cybercriminels utilisent régulièrement les failles de sécurité de ces modules pour accéder à des données.

4. *Rechercher les maliciels sur tous les ordinateurs ayant servi à la gestion du site*
   Avant que les données d'accès FTP et au CMS ne soient modifiées, il faut rechercher les maliciels existants sur tous les ordinateurs qui ont servi à gérer le site Internet, c'est-à-dire les ordinateurs sur lesquels ont été introduits un identifiant et un mot de passe permettant la gestion du site web. MELANI a publié des instructions à cet égard.

   ➔ Instructions relatives à la suppression des maliciels:
   http://www.melani.admin.ch/suppression-des-maliciels

5. *Modifier les mots de passe d'accès*
   Une fois que les maliciels ont été détectés et supprimés, il est nécessaire de modifier les données d'accès FTP et au CMS. Cette démarche permet d'empêcher les cybercriminels d'introduire de nouveaux maliciels sur le site Internet grâce aux données d'accès précédemment volées (nom d'utilisateur et mot de passe). Si les mots de passe utilisés sur l'ordinateur infecté ont également servi à accéder à d'autres services Internet (webmail, Paypal, etc.), ceux-ci doivent aussi être modifiés.

Si les points 3, 4 et 5 n'ont pas été respectés, il est fort probable que les cybercriminels puissent de nouveau accéder à votre site Internet et y installer des maliciels.

Contrôle de sécurité

Après que vous aurez nettoyé votre site Internet, nous vous recommandons de mettre en œuvre des mesures supplémentaires afin d'éviter que des cybercriminels accèdent à l'avenir à votre site web. Pour ce faire, MELANI a élaboré une liste de contrôle contenant les mesures à prendre.

➔ Mesures de prévention pour les systèmes de gestion de contenu (CMS):
http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=fr