Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

**S.G.D.S.N**
*Agence nationale de la sécurité des systèmes d'information*
*CERTA*

Paris, le 2 mars 2012
N° CERTA-2012-INF-002

**Affaire suivie par :**
CERTA

# NOTE D'INFORMATION DU CERTA

## Objet : Les défigurations de sites Web



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2012-INF-002 |
| Titre | Les défigurations de sites Web |
| Date de la première version | 2 mars 2012 |
| Date de la dernière version | – |
| Source(s) | |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Introduction

À cause de leur grande visibilité, les sites Web sont des cibles de choix pour des attaques informatiques. Nous nous intéressons ici à une catégorie d'attaques visant des sites Web publics dans le but de modifier leur contenu. Nous les nommerons « défigurations » (en anglais, *defacement*). La motivation des attaquants est alors de vandaliser un site Web. Cette modification peut être visible, par exemple en modifiant la page d'accueil du site, ou bien plus discrète. Dans ce dernier cas, la défiguration restera le plus souvent invisible par un visiteur naïf du site. Toutefois, un visiteur « averti » aura accès au contenu modifié par l'attaquant, et ainsi avoir la preuve de la compromission réussie du site.

Une bonne partie de ces compromissions sont revendiquées (au travers de sites comme *Zone-H.org*), car les attaquants recherchent le plus souvent une certaine reconnaissance de leur communauté. L'objectif est de montrer leurs capacités techniques, ou encore de faire passer un message politique. Des moqueries envers les administrateurs du site sont également très courantes.

On peut ainsi séparer les défigurations d'autres types de compromissions plus silencieuses. Un attaquant souhaitant contrôler un système d'information sur le long terme, afin d'en faire fuire des données par exemple, essaiera au contraire d'être le plus discret possible.

# 2 Prévention

La défiguration d'un site Web est rendue possible par un défaut de sécurité. Plusieurs vecteurs sont exploités par des attaquants pour modifier de manière illégitime le contenu d'un site Web :

- défaut de sécurisation d'accès à une interface de gestion du site, ou *BackOffice* ;
- défaut de suivi de la procédure d'installation d'un site ;
- vulnérabilités de type « injection SQL » qui permettent à un attaquant de modifier les informations stockées en base de données ;
- vulnérabilités connues et non corrigées dans les différentes briques utilisées pour la construction du site (Framework, serveur Web, système d'exploitation, etc.) ;
- vulnérabilités non connues dans ces différentes briques (*zero-day*) ;
- compromission d'un site tiers hébergé sur la même plateforme ;
- politiques de gestion de mots de passe et de droits d'accès laxistes ;
- etc.

## 2.1 Suivre la procédure d'installation

De nombreux sites Web clés en main, ou des gestionnaires de contenu, sont fournis avec une procédure d'installation. Celle-ci détaille le plus souvent les permissions d'accès à appliquer à certains répertoires (stockage d'éléments envoyés par des visiteurs, cache, sessions, etc.), ou indique qu'il est nécessaire de supprimer manuellement des éléments temporaires générés lors de l'installation. Cette procédure doit être suivie scrupuleusement afin de ne pas laisser d'éléments qui pourraient aider un attaquant à modifier le site. Cette procédure indique parfois la nécessité de changer des mots de passe par défaut fournis avec l'installation. Aucune de ces étapes ne doit être ignorée ni ajournée.

## 2.2 Appliquer les correctifs de sécurité

Il convient, comme rappelé régulièrement dans les publications du CERTA, de maintenir à jour et de corriger les vulnérabilités de l'ensemble des éléments entrant en jeu dans la mise en ligne d'un site Web :

- gestionnaire de contenu (CMS) comme Joomla!, SPIP, Drupal, etc. ;
- extensions et modules de tierce partie éventuellement ajoutés à ces CMS ;
- langages utilisés et bibliothèques associées, comme PHP ;
- logiciels fournissant le service Web comme Apache ou IIS ;
- logiciels fournissant d'autres services nécessaires au fonctionnement du site, comme des serveurs SQL ;
- logiciels d'administration du site et de son environnement (AWStats, phpMyVisites, etc.) ;
- système d'exploitation sur lequel est installé un ou plusieurs de ces services.

Bien qu'il soit tentant d'installer des modules supplémentaires ajoutant des fonctionnalités à un site Web, il est plus raisonnable de ne conserver que les éléments vitaux au fonctionnement du site. Une grande méfiance envers les modules de tierce partie, dont les développeurs négligent parfois la sécurité, est également de mise. Tout module supplémentaire augmente la surface d'attaque, et les vulnérabilités potentielles exploitables par un attaquant.

Pour une petite structure, il est souvent plus simple de faire héberger son site chez un prestataire. La mise a jour des éléments listés ci-dessus devient contraignante (donc nécessite des procédures bien détaillées) et parfois impossible. Dans ce cas, il est recommandé d'interroger le prestataire sur sa politique de sécurité. De plus, dans le cadre d'un hébergement de type mutualisé, la compromission d'un site hébergé sur une plateforme par un attaquant signifie souvent que celui-ci peut modifier d'autres sites hébergés sur cette même plateforme. Les bonnes pratiques concernant l'hébergement mutualisé sont rappelées dans la note d'information du CERTA CERTA-2005-INF-005.

Quand le site Web est développé par un prestataire, il convient de vérifier son engagement sur le suivi de son produit. Appliquera-t-il les corrections de vulnérabilités découvertes dans les briques logicielles utilisées ? Pourra-t-il apporter un soutien pour rechercher et corriger la vulnérabilité utilisée en cas de compromission ?

### 2.3 Politiques de gestion des mots de passe et de droits d'accès

Les mots de passe d'accès à des interfaces d'administration doivent suivre des règles élémentaires de complexité et de renouvellement. Celles-ci sont précisées dans la note d'information du CERTA CERTA-2005-INF-001.

Les droits d'accès à chaque répertoire du site doivent correspondre aux indications de la procédure d'installation. Lorsque celle-ci ne les précise pas, les permissions d'accès en lecture/écriture doivent toujours être les plus restrictives possibles.

### 2.4 Restriction d'accès à l'interface de gestion

Qu'il s'agisse d'une interface incluse dans le site Web permettant de modifier dynamiquement son contenu, ou d'un accès direct aux fichiers du site (par FTP, SSH, RDP, etc.), le CERTA recommande de mettre en place une politique de gestion des autorisations d'accès.

Cela peut passer par la mise en place d'une liste blanche réduite d'adresses IP depuis lesquelles des administrateurs ou des contributeurs peuvent légitimement effectuer des modifications. La validation des accès par rapport à cette liste blanche est appliquée par la configuration idoine du service d'administration (FTP, SSH, RDP, etc.), ou la mise en place de fichiers *.htaccess* pour limiter l'accès à des répertoires particuliers. Dans le cas où les adresses IP des administrateurs ne sont pas statiques, une authentification forte (validation de certificats clients par exemple) doit être envisagée.

## 3 Détection

### 3.1 Au niveau du serveur

Plusieurs mécanismes peuvent être envisagés pour surveiller l'intégrité d'un site Web. Un script peut vérifier périodiquement le condensé de chaque fichier, la présence de fichiers supplémentaires, les permissions des fichiers et répertoires, etc.

La lecture régulière des journaux d'accès permet souvent de détecter des tentatives de compromission. En effet, certains outils de recherche automatique de vulnérabilités laissent des traces reconnaissables. Un grand nombre d'accès à des pages intégrant des formulaires, concentrés dans le temps, depuis une même adresse IP, à des heures de faible fréquentation du site, peuvent indiquer une recherche de vulnérabilités.

### 3.2 Équipements extérieurs au site

Si des équipements réseau sont en coupure entre le site et le réseau Internet, l'analyse de leurs journaux ou de leurs rapports peut également donner des indices d'une tentative de compromission. Un pic de bande passante, des connexions anormales ou des flux réseaux rejetés par exemple, peuvent être de nouveaux indices d'une probable compromission.

Un service de veille peut être mis en place pour surveiller l'état du site. La veille peut être manuelle ou automatique, grâce à des scripts ou des produits vérifiant par exemple l'absence de certains motifs prédéfinis sur chacune des pages Web.

## 4 Réactions

Dès lors que la défiguration d'un site Web est découverte en interne ou signalée par une entité extérieure comme le CERTA, plusieurs actions sont à entreprendre.

### 4.1 Conservation des traces

Une copie de l'état compromis du site Web (ou du serveur, si l'environnement n'est pas mutualisé) doit être réalisée. Cette copie sera utile pour l'analyse technique de la compromission, ou pour alimenter un dossier dans le cas où une plainte est déposée. Il convient également de sauvegarder les journaux d'accès au site Web, et ceux de

tous les services permettant de modifier le site à distance (FTP, SSH, etc.). Ces éléments doivent parfois être demandés à l'hébergeur du site Web. Lorsqu'ils existent, les traces des équipements environnants (pare-feux, serveurs mandataires, etc.) doivent également être consignés.

L'analyse de la compromission est nécessaire pour trouver quelle vulnérabilité a été utilisée par l'attaquant pour compromettre le site. Il sera alors possible de combler cette vulnérabilité. La simple restauration du site dans un état « sain » ne bloquera pas la faille utilisée par l'attaquant, qui pourra rapidement compromettre le site à nouveau. Il faut également garder à l'esprit qu'une vulnérabilité trouvée par une personne dont le but est de défigurer un site, a déjà pu être découverte et exploitée par un attaquant souhaitant réaliser d'autres opérations illégitimes de manière plus discrète.

### 4.2 Recherche d'autres intrusions

Comme rappelé ci-dessus, un site défiguré est un site vulnérable. Il faut donc rechercher d'autres traces de compromission et modifications du site. Il se peut que du contenu malveillant ait été déposé comme par exemple :

- pages d'hameçonnage (phishing) ;
- insertion de malware ;
- insertion de publicités non légitimes ;
- modification de la configuration du site, ou des fichiers *.htaccess* ;
- installation d'un porte dérobée (*PHP shell*, etc.) permettant d'utiliser le site pour effectuer d'autres actions malveillantes (nouvelles compromissions, déni de service, etc.) ;
- stockage de fichiers soumis au droit d'auteur ;
- etc.

Il ne suffit pas de vérifier la présence de nouveaux fichiers dans l'arborescence du site. Si le site s'appuie sur une base de données, celle-ci a également pu être modifiée, et devra être restaurée à partir d'une sauvegarde dont le contenu aura été vérifié.

### 4.3 Reconstruction du site

Il est possible, une fois la copie du site compromis (ou de l'intégralité du serveur, si possible) réalisée et sauvegardée, de restaurer le site dans son état normal. Toutefois, avant de le remettre en ligne, il est nécessaire de corriger d'abord les vulnérabilités précédemment identifiées. Si une sauvegarde est utilisée, il est impératif de s'assurer que celle-ci est bien saine et ne date pas d'un moment ultérieur à la défiguration. Si aucune sauvegarde n'est disponible, seuls les éléments de la défiguration pourront être modifiés ou supprimés. La vulnérabilité utilisée doit toujours être corrigée.

## Documentation

- Zone-h
  http://www.zone-h.org
- Les bons réflexes en cas d'intrusion sur un système d'information CERTA-2002-INF-002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/
- Du bon usage de PHP CERTA-2007-INF-002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/
- Les mots de passe CERTA-2005-INF-001 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Sécurité des applications Web et vulnérabilités de type « injection de donnée » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/
- Bonnes pratiques concernant l'hébergement mutualisé CERTA-2005-INF-005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Sécurité des applications Web et vulnérabilité de type "injection de données" CERTA-2002-INF-002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/
- Définition du filoutage/hameçonnage (phishing) CERTA-2006-INF-002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/CERTA-2006-INF-002.html#hame

**2 mars 2012** version initiale.