



Attaque <iFrame>

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

1. Qu'est-ce que la balise <iFrame> ?
2. Comment se déroule une attaque <iFrame>?
3. Qui est concerné ?
4. Pourquoi se protéger ?
5. Comment se protéger



L'objectif principal de beaucoup de pirates informatiques est de corrompre les ordinateurs d'internautes pour pouvoir voler des informations personnelles. Des numéros de cartes de crédit ou des données d'authentification pour les accéder à des sites commerciaux ou bancaires sont très recherchés. Pour réussir leur attaque, les pirates ont beaucoup de possibilités.

Un des moyens utilisés en force depuis 2007 consiste à déployer des codes malicieux tels que des chevaux de Troie en usurpant de sites Internet à haute fréquentation, mais mal protégés.

Une telle attaque est minutieusement préparée et déployée en plusieurs étapes. Lors de la première étape de l'attaque, les pirates informatiques préparent un site hébergeant des codes malicieux capables d'infecter les ordinateurs des internautes qui passent. Cette technique d'attaque s'appelle "drive-by download". Elle n'est pas souvent couronnée de succès, car il faut qu'une victime vienne se perdre sur le site. Cependant pour augmenter les chances d'une telle visite, les pirates peuvent employer plusieurs techniques. Ils incitent les potentielles victimes à venir sur le site en leur envoyant des liens contenus dans des courriers électroniques, ou ils introduisent des commandes dans des sites mal protégés, mais bien fréquentés. Cette dernière technique s'appelle attaque par <iFrame>. En effet <iFrame> est une balise HTML qui va récupérer du contenu sur un autre site pour l'afficher.



1 Qu'est-ce que la balise <iFrame> ?

La balise IFRAME est une composante du langage HTML. Le langage HTML est utilisé pour créer des pages Web sur Internet. Il se sert de balises permettant de présenter et de formater les informations, textes, images, sons, vidéos, etc. que l'on souhaite afficher sur une page Web. Comme balises très connues, on peut notamment nommer ... pour formater en gras le texte entre les deux balises, ou encore <script>....</script> une balise qui permet d'inclure un script, donc une suite d'instructions comme notamment du JavaScript, dans une page web.

La balise <iFrame> signifie « inline frame ». Elle est utilisée pour insérer, au sein d'une même page Web, des informations stockées sur différents sites Internet. Les concepteurs de sites ont le plus souvent recours à la balise <iframe> pour permettre l'affichage de publicités, ces dernières étant hébergées sur des serveurs leur étant spécifiquement dédiés.

EXEMPLE DE CODE HTML UTILISANT LA BALISE IFRAME

L'utilisation de la balise IFRAME permet d'intégrer et de réunir au sein d'une même page HTML le contenu et les informations de différents sites Internet. Prenons un exemple : un internaute qui possède le site www.site-perso.lu a créé une IFRAME reprenant la page d'accueil de CASES Luxembourg pour l'insérer sur la page d'accueil de son propre site. Le texte « Le site ci-dessous est en fait une IFRAME vers <http://www.cases.lu> » est la seule information propre à son site personnel.

La balise IFRAME est totalement personnalisable. On peut, par exemple, choisir la source d'information pour le contenu de l'IFRAME (src), la taille de l'IFRAME (height et width), la navigation en scrolling, respectivement l'affichage des scrollbars (scrolling), l'affichage ou non d'un bord autour de l'IFRAME (frameborder). Vous pouvez consulter sur le site du W3C (<http://www.w3.org/>), l'organisme définissant les standards sur Internet, les spécifications de la balise IFRAME. Le code HTML ci-dessus permet d'afficher la page suivante dans un navigateur. (Les informations encadrées en bleu et rouge permettent de faire la distinction entre les informations provenant de www.site-perso.lu et de www.cases.lu.)

Lorsqu'un internaute se connecte à www.site-perso.lu, la page d'accueil demandée est transférée vers son ordinateur. Le navigateur va analyser les balises et afficher la page d'accueil. Mais puisqu'une

```
<html>
<head>
<title>Inline Frames - demonstration</title>
</head>

<body>
<h1>Le site ci-dessous est en fait une IFRAME vers
http://www.cases.lu</h1>
<iframe src="http://www.cases.lu"
height="500" width="800" frameborder="0" scrolling="no">
Texte alternatif pour les navigateurs Internet qui ne savent pas gérer
les IFrames.
</iframe>
</body>
</html>
```



balise <iFrame> est contenue dans code, le navigateur va se connecter au site www.cases.lu pour récupérer le contenu demandé. Le navigateur affiche les deux contenus provenant de deux sites différents.



Comment se déroule une attaque <iFrame> ?

Les attaques exploitant de manière malveillante la balise IFRAME ont bien souvent pour objectif la diffusion et l'installation de malwares sur les ordinateurs d'internautes victimes.

Les malwares diffusés sont très souvent des keyloggers ou chevaux de Troie utilisés pour espionner les informations personnelles et sensibles de leurs victimes telles que leur numéro de carte bancaire ou leur mot de passe à des services e-banking. En général, les pirates à l'origine de ces attaques recherchent un intérêt financier.

Malheureusement, ce type d'attaque reste le plus souvent silencieux et invisible aux yeux des internautes, la rendant ainsi encore plus dangereuse.

L'idée de l'attaque réside dans l'utilisation de la balise IFRAME pour inclure un contenu malveillant au cœur d'une page de confiance. Ce contenu malveillant est hébergé sur un serveur sous le contrôle des pirates.

Les pirates insèrent sur le site légitime le code HTML d'une balise IFRAME invisible aux internautes, en lui donnant, par exemple, une taille réduite ou en bloquant son affichage (ce qui n'empêchera toutefois pas la connexion vers le site malveillant). Ainsi, la balise IFRAME force la connexion vers un site malveillant. La future victime qui se connectera sur ce site Internet sera

alors, à son insu, forcée de télécharger du code malveillant depuis le serveur sous le contrôle des pirates au travers de la balise IFRAME. Une fois téléchargé, le code malveillant s'exécute, essayant d'exploiter des vulnérabilités du navigateur respectivement de la machine de l'internaute pour s'installer.



Qui est concerné ?

On a vu que de nombreux sites Internet, même les plus honorables, peuvent être corrompus. Ainsi, au cours des attaques de juin 2004, en Italie, ce ne sont pas des sites pour adultes qui ont été compromis pour diffuser des malwares, mais des sites reconnus et respectables, permettant ainsi aux pirates de toucher un très grand nombre de victimes. Des sites sur l'industrie de l'automobile

et des films, mais aussi des portails sur le tourisme et l'hôtellerie, tout comme des sites gouvernementaux auraient été touchés.

Ces éléments montrent que l'on peut être impacté par ce type d'attaque en surfant sur des sites institutionnels et, plus seulement, sur des sites underground ou pour adultes.

LES INTERNAUTES

Sachant que l'on peut être victime de ce type d'attaque simplement en surfant sur un site Internet corrompu, les internautes sont les premiers concernés par l'exploitation malveillante de la balise IFRAME.

Si l'on peut rencontrer une exploitation malveillante de la balise IFRAME en surfant sur

Internet avec son navigateur Web, on peut aussi en souffrir **en ouvrant un e-mail enregistré en format HTML** contenant une IFRAME. Celle-ci peut établir automatiquement et à votre insu une connexion vers un site Internet qui pourrait être malveillant. Il faut donc autant se méfier lorsque l'on surfe que lorsque l'on lit ses e-mails.

LES CRÉATEURS DE SITES INTERNET

Les créateurs de sites Internet peuvent être confrontés à l'exploitation de la balise IFRAME, si leur site a été corrompu par un pirate qui y a ajouté du code HTML créant, via la balise IFRAME, une connexion vers un site Internet

malveillant diffusant, par exemple, des spywares. C'est dans ce sens que les créateurs de sites Internet peuvent être confrontés à l'exploitation malveillante de la balise IFRAME.

LES HÉBERGEURS DE SITES INTERNET

De part leur position d'intermédiaire entre les internautes et les créateurs de sites, les hébergeurs de sites Internet sont également concernés par l'exploitation malveillante de la balise IFRAME.

A ce titre, ils font également partie des personnes à sensibiliser et peuvent contribuer à lutter contre ce type de problème.



Pourquoi se protéger ?

Il est important de se protéger contre l'exploitation malveillante de la balise IFRAME. Bien que la balise IFRAME ne soit pas malveillante en elle-même, un

détournement de ses fonctionnalités peut permettre à des pirates de l'utiliser pour déployer et contaminer les internautes par des malwares.

LES INTERNAUTES

Le premier moyen de protection réside dans la connaissance et l'application des bonnes pratiques de navigation sur Internet. Il faut notamment éviter de surfer sur des sites suspects qui pourraient exploiter les IFRAMES pour corrompre votre ordinateur et dérober des données personnelles dans un but lucratif ou de vol d'identité.

LES CREATEURS DE SITES INTERNET

Tout comme dans la vie réelle, une bonne réputation dans le monde numérique est parfois difficile à conserver et tout le travail sur la confiance peut être détruit si le nom d'un site Internet, auparavant reconnu comme fiable, est lié à des affaires de propagation de malwares. La renommée d'un site Internet garantit souvent sa pérennité.

LES HEBERGEURS DE SITES INTERNET

Tout comme les créateurs de sites Internet, les hébergeurs ont une réputation à défendre et doivent lutter pour empêcher que leur nom ne soit

Les informations les plus prisées sont les informations personnelles (nom, adresse, date de naissance, numéro de sécurité sociale, etc.) permettant de lancer des attaques d'usurpation d'identité, les mots de passe, les identifiants de sites e-banking ou encore les numéros de carte bancaire.

Les créateurs de sites Internet engagent leur réputation et ont une obligation, tout du moins morale, de protéger les internautes visitant leur site contre la désinformation, de protéger les données personnelles qui pourraient leur être confiées et de sécuriser les informations qu'ils diffusent.

lié à des cas avérés de propagation de malwares ou de diffusion de contenus contraires à la législation et aux bonnes mœurs.



Comment se protéger

Puisque des sites Internet innocents ont été corrompus pour être utilisés comme relais, via IFRAME, dans des attaques de grande ampleur, il

est clair que les techniques de filtrage d'URL ou d'adresses Web se révèlent inefficaces. Il ne suffit plus de ne pas surfer sur des sites "louches"

POUR LES INTERNAUTES

Puisque les balises IFRAME sont définies par le W3C, l'organisme définissant les standards sur Internet et que leur utilisation est très courante sur de nombreux sites Internet de confiance, il est impossible de bloquer leur utilisation sans restreindre les possibilités de navigation sur Internet.

Il est donc important d'appliquer des contre-mesures techniques et organisationnelles simples mais efficaces pour se protéger.

Pour les internautes, les bonnes pratiques à respecter sont les suivantes :

- Utiliser et mettre à jour votre **logiciel antivirus** ;
- **Installer les patchs de sécurité** pour maintenir à jour votre système d'exploitation et ses applications, en particulier les navigateurs Web et les outils de messagerie e-mail ;
- **Éviter de surfer sur des sites qui ne sont pas dignes de confiance** et qui pourraient exploiter les IFRAMES en conjonction d'autres outils de piratage pour corrompre votre ordinateur ;
- **Désactiver l'Active Scripting** afin de limiter l'impact d'une attaque exploitant une IFRAME pour forcer le téléchargement de malwares à votre insu ;
- **Forcer son outil de messagerie** à n'ouvrir les messages qu'en format texte et non en format HTML.

POUR LES CRÉATEURS DE SITES INTERNET

Puisque les créateurs de sites Internet peuvent être la cible d'attaquants, il est important qu'ils participent à la lutte contre les attaques, par exemple :

- en sécurisant le code des pages. Si vous avez un site Internet dynamique, un forum, un blog, un site e-commerce ou un site e-banking, utilisant un langage de programmation tel que le PHP pour interagir avec les internautes sur votre site, vous devez prendre en compte les aspects de qualité et de sécurité de votre code afin d'empêcher toute compromission de votre site par un pirate.
- en effectuant des scans d'intégrité sur certaines pages de votre site Internet, en particulier sur les pages ou les sections statiques de pages Web ou les pages de commentaires des blogs (Web

2.0). Il peut s'avérer nécessaire de mettre en place une solution de scans d'intégrité des pages afin de détecter toute modification et ainsi détecter le plus rapidement possible une corruption éventuelle de votre site par un pirate. On parle de FIDS – Filesystem based Intrusion Detection System ou FIA – File Integrity Assessment. L'un des plus connus est TripWire.

- Les pages Web 2.0 commentées par les visiteurs peuvent être quotidiennement modifiées de manière autorisée et donc lever de fausses alertes si on les inclut dans les scans d'intégrité. Comme propriétaire du site, vous êtes responsable pour son contenu, qu'il s'agisse d'un site normal ou d'un site contributif du type web 2.0.

POUR LES HÉBERGEURS DE SITES INTERNET

Puisque ces attaques, pour pouvoir réussir, doivent souvent exploiter des vulnérabilités sur les serveurs, les hébergeurs de sites se doivent de garantir la sécurité :

- en mettant à jour leurs serveurs Web pour empêcher l'exploitation de vulnérabilités connues et corrigées qui pourrait conduire à la corruption de la sécurité des serveurs et de tous les sites Internet hébergés ;
- dans le cas de l'hébergement mutualisé de sites Internet sur une même machine, en cloisonnant

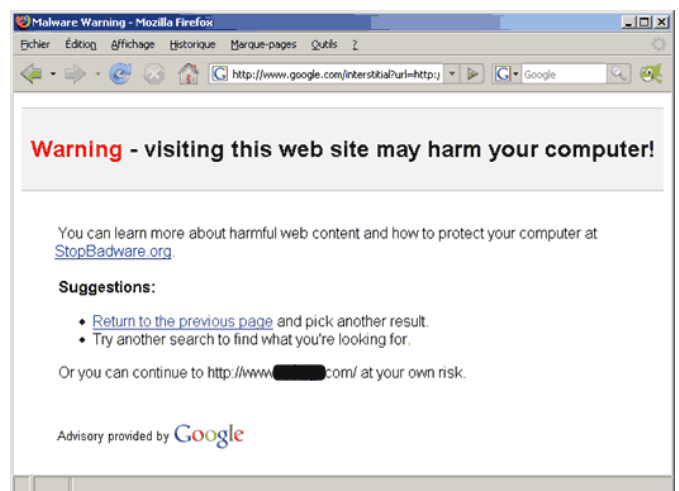
de manière sûre les différents sites afin d'empêcher qu'une compromission de l'un d'entre eux n'entraîne une réaction en chaîne en compromettant tous les sites hébergés sur la même machine ;

- en s'assurant de la sûreté des informations et des programmes qui sont diffusés sur les sites Internet qu'ils hébergent (par exemple, en contrôlant, tout en respectant les lois relatives aux données personnelles, le contenu des pages et en proposant des services de détection de code malveillant).

LES AVERTISSEMENTS SUR CERTAINS MOTEURS DE RECHERCHE

Les moteurs de recherche sont également sensibilisés aux risques sur Internet. A titre d'exemple, on peut citer Google qui, lors du lancement d'une recherche susceptible de mener sur un site « dangereux ».

Sachez toutefois que ce type d'avertissement ne pourra jamais remplacer les précautions d'usage et que cette technique n'est pas sans erreur. Google se base sur des blacklists, c'est-à-dire des listes de sites reconnus pour être potentiellement dangereux. Toutefois, cette technique ne peut assurer des résultats fiables à 100%



Retrouvez les dossiers, fiches thématiques, alertes et actualités sur :

www.cases.lu

CASES 2008