



CASES articles

Certaines pages Internet sont abusivement utilisées par des criminels

Danger invisible sur la toile : Les attaques iFrame

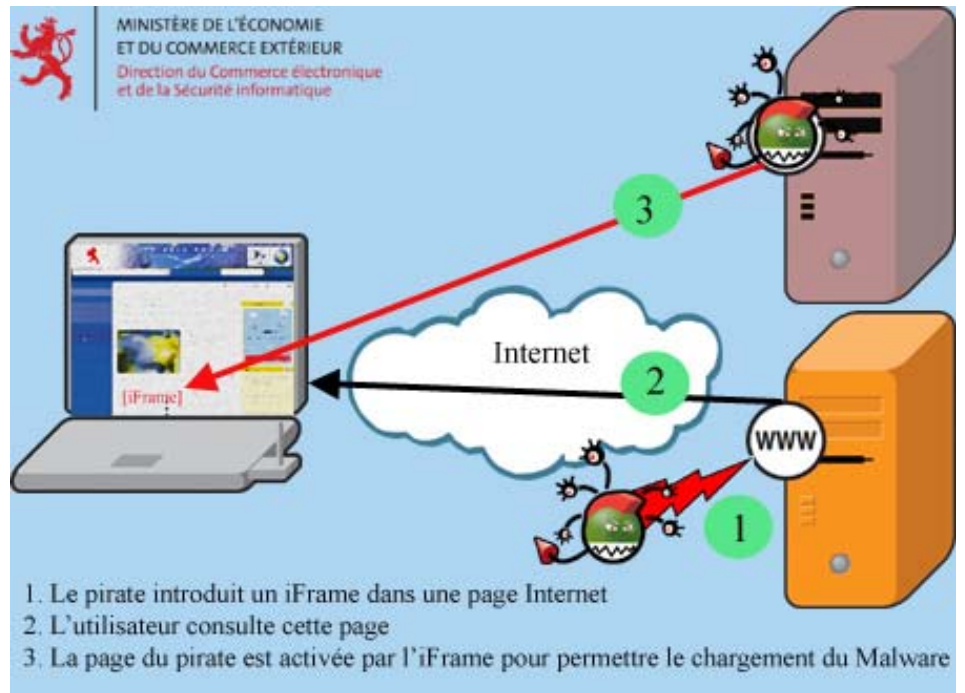
Pour plus de sécurité, adoptez les réflexes CASES !

Les pages Internet luxembourgeoises sont également concernées

Dans le passé, les cybercriminels ont largement exploité les failles de sécurité des applications d'e-commerce et d'e-banking. Ils ont également su profiter de la crédulité des utilisateurs. Loin d'être à court d'idées concernant de nouvelles formes d'attaque, ils ont désormais tendance à cibler directement les ordinateurs des utilisateurs d'Internet et leurs vulnérabilités. Pour ce faire, ils utilisent des tiers, à savoir des pages Internet communes présentant des failles de sécurité.

De nombreux utilisateurs d'Internet disposent de moyens techniques de protection insuffisants sur leur ordinateur. Les cybercriminels quant à eux se posent la question de savoir comment obtenir aisément accès à ces ordinateurs ? Les pages Internet d'utilisation courante leur ont permis de répondre à cette question. En effet, une nouvelle forme d'attaque utilise les pages Internet consultées quotidiennement par les usagers et présentant des failles de sécurité, afin de propager des malwares. Parmi ces attaques figurent par exemple les attaques iFrame, qui demeurent totalement invisibles pour l'utilisateur. Les pirates mettent ainsi à profit les habitudes de navigation des usagers ainsi que les vulnérabilités des pages Internet. Les pirates concentrent alors leurs efforts sur les pages web accueillant un grand nombre de visiteurs et qui sont consultées quotidiennement. Le but de ce nouveau type d'attaque est d'obtenir accès au plus grand nombre possible d'ordinateurs d'internautes.

En juin 2007, les premières grandes attaques iFrame ont été menées en Europe. En quelques jours, plusieurs milliers de pages web, en Italie par exemple, ont alors été crackées. Depuis, le Luxembourg n'a pas été épar-



gné par cette forme d'attaque, elles sont même de plus en plus touchées.

À quoi ressemble une attaque iFrame?

Les pirates recherchent généralement d'éventuelles failles de sécurité dans les pages Internet d'utilisation courante. Une fois découvertes, les criminels passent à l'étape suivante : ils insèrent un iFrame presque invisible dans le code HTML de la page concernée. Le propriétaire de cette page devient ainsi la première victime de l'attaque. Lors de sa navigation, l'internaute n'est pas en mesure de détecter la manipulation de la page web concernée, les pirates choisissant en effet une taille de caractère minuscule ou empêchant complètement l'affichage de l'iFrame.

Lors de la consultation d'une page manipulée par les pirates, l'iFrame dissimulé établit une connexion avec une deuxième page web malveillante. La connexion à cette page conçue spécialement à cet effet par les pirates se fait totalement à l'insu de

Définition : iFrame

iFrame signifie *inline frame*. Il s'agit d'un élément du langage informatique HTML écrit sous la forme `<iFrame>`. Cet élément est utilisé lors de la réalisation de pages Internet et permet d'inclure des informations contenues dans différentes pages Internet sur une seule page web. Un iFrame est par exemple utilisé sur une page web propre pour insérer la page d'accueil d'un ami.

l'utilisateur. Les cybercriminels tentent par ce biais de charger un code malveillant, dénommé malware, sur l'ordinateur de l'usager. Les experts en sécurité parlent alors d'un « drive-by-download ». Le malware est bien sûr contrôlé par le pirate et il est exécuté dès lors qu'une faille de sécurité exploitable a été détectée sur l'ordinateur de la victime. Les criminels obtiennent ainsi un accès direct à de nombreux ordinateurs privés et des droits d'accès à tous les ordinateurs présentant des points faibles.

Les cybercriminels ont atteint leur but dès lors que le malware est installé sur l'ordinateur de la victime.

Une fois l'accès obtenu, ils sont en effet en mesure de recueillir des données telles que mots de passe, identifiants de connexion pour applications de banque en ligne, numéros de cartes de crédit ainsi que d'autres données personnelles, comme le numéro de sécurité sociale, le nom, l'adresse et la date de naissance. Ce sont en particulier ces dernières informations qui permettront aux pirates d'usurper l'identité des utilisateurs d'Internet. Les criminels peuvent également obtenir le contrôle complet de l'ordinateur de la victime. Celui-ci se transforme alors en robot commandé à distance, également qualifié de « bot ». Le bot peut ensuite par exemple être exploité pour la propagation de spams ou de contenus pornographiques à caractère pédophile ou encore pour mener des attaques sur d'autres ordinateurs. Tout comme le propriétaire de la page web manipulée, l'utilisateur devient ainsi victime – mais aussi complice – de ces agissements.

Se protéger des attaques iFrame

« Étant donné que de nombreuses pages Internet dignes de confiance ont recours aux iFrames, il n'est pas possible de les interdire sans restreindre la libre navigation sur l'Internet », explique Pascal Steichen, expert en sécurité de la plateforme luxembourgeoise CASES du Ministère de l'Économie et du Commerce extérieur, « il est donc indispensable que les usagers d'internet adoptent des réflexes de sécurité et mettent en œuvre des mesures de protection techniques ».

La mesure de protection la plus importante consiste à s'informer des règles à respecter lorsque l'on surfe sur la toile. Tout comme l'utilisation des ceintures de sécurité en voiture, ces règles devraient devenir des réflexes.

Les pirates attaquent et manipulent de plus en plus souvent des pages utilisées quotidiennement et ces attaques demeurent totalement indétectables pour l'utilisateur. Il est donc devenu indispensable pour celui-ci de mettre en œuvre des moyens spécifiques

Conseil de sécurité :

La désactivation ou restriction de la fonction Active Scripting dans le navigateur Internet permet de limiter les conséquences d'une attaque iFrame. L'exécution de scripts Java et Flash est ainsi également interrompue ou restreinte.

Comment procéder :

Le navigateur Mozilla Firefox 2.0 propose une solution simple

Étape 1 : Vérifiez que le navigateur Mozilla Firefox 2.0 est installé. Si oui, passez à l'étape 3, si non, voir étape 2.


Étape 2 : Installez le navigateur Mozilla Firefox 2.0, par exemple en langue française, sur le site www.mozilla.com. Ce navigateur est gratuit.

Étape 3 : Dans la barre des menus du navigateur, cliquez sur [Outils] / [Modules complémentaires] puis sur [Extensions].

Ou : rendez-vous sur <https://addons.mozilla.org/de/firefox/> en utilisant le navigateur Mozilla Firefox 2.0.

Étape 4 : Réglez le second champ de recherche sur [Toutes les extensions], introduisez le nom de module *noscript* dans le premier champ de recherche, puis appuyez sur la touche Entrée.



Étape 5 : Le module *noscript* s'affiche . Cliquez ensuite sur [Ajouter à Firefox], puis sur [Installer] et [Redémarrer Firefox]. Le navigateur Mozilla Firefox se ferme.

Étape 6 : Après réouverture du navigateur, apparaît en bas à droite de la fenêtre un [S]. Cliquez sur ce symbole à l'aide du bouton gauche de la souris, puis sur [Options] et [Greffons].

Étape 7 : Cochez l'option {Interdire IFRAME} ainsi que celles concernant les scripts et Flash situées au-dessus. Cliquez sur [OK].

Étape 8 : Vérifiez le fonctionnement du module *noscript* de Mozilla Firefox. À cet effet, utilisez le navigateur Mozilla Firefox et rendez-vous sur www.cases.lu. Sur la droite de la page d'accueil, la rubrique CASESmag (la Newsletter de CASES) ne devrait pas être accessible. CASESmag n'est rendu accessible qu'après un clic gauche dans la fenêtre correspondante suivi de votre confirmation (car il s'agit d'un iFrame).

Effectuez ensuite un clic gauche sur le [S] en bas à droite de la fenêtre pour autoriser de façon permanente ou temporaire l'exécution de tous les scripts, iFrames et Flash sur la page www.cases.lu.

Pour toutes les pages Internet, vous pourrez désormais autoriser ou interdire l'Active Scripting.

afin de protéger son ordinateur privé. Les pages Internet qui ne sont pas dignes de confiance ne devraient jamais être consultées. Celles-ci présentent en effet toujours un risque plus important de dissimuler des iFrames à caractère criminel.

Pour des raisons de sécurité, toutes les applications de l'ordinateur devraient être mises à jour régulièrement. Cela permet de remédier aux vulnérabilités avérées. Les utilisateurs devraient également veiller à corriger le plus rapidement possible, les failles de sécurité communiquées par les fabricants de logiciels à l'aide de programmes correctifs, également appelés patches. Un programme anti-virus régulièrement mis à jour ainsi qu'un pare-feu correctement paramétré

devraient être à la base des moyens de protection techniques de chaque ordinateur. De plus, il est recommandé de procéder régulièrement à l'analyse de l'ordinateur à l'aide d'un logiciel anti-spyware afin de détecter les éventuels programmes d'espionnage. « Outre le grand nombre de produits commerciaux, il existe également des produits gratuits pour les utilisateurs privés », précise Pascal Steichen. Il conseille de plus aux utilisateurs d'Internet de se tenir informés des nouvelles menaces sur la toile ainsi que de leur mode de fonctionnement. Une description détaillée du mode de fonctionnement des attaques iFrame et des mécanismes de protection à adopter peut être consultée sur www.cases.lu.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu