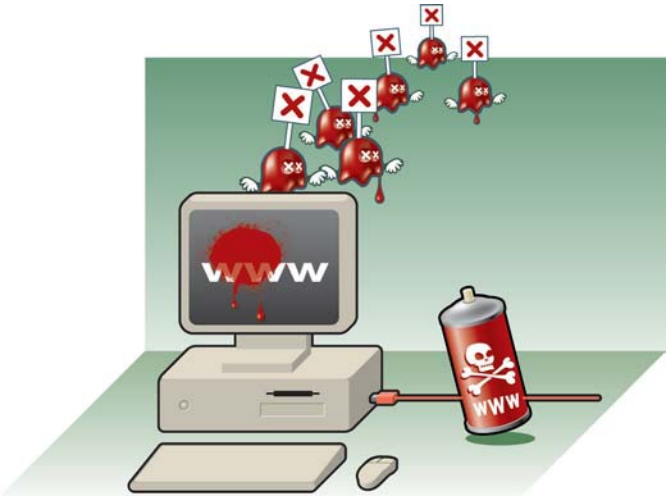
Defacement / Défiguration

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Ce document traite de menaces particulières sur Internet, à savoir les dégradations de sites Web. Ces attaques sont plus particulièrement connues sous le terme de défiguration (defacement). Sont décris dans ce document les caractéristiques principales de ce type d'attaque, les impacts possibles ainsi que les mesures préventives.

Table des matières



1 C'est quoi ?

Une défiguration (defacement) est une forme de cyber-délinquance de type cyber-vandalisme, voire cyber-terrorisme, dirigé contre un site Web.

Une défiguration correspond à une action délibérée de destruction, dégradation ou modification de données d'un site Web, dans un but de dommages et/ou de retentissement maximum, pour des raisons politiques, religieuses ou encore idéologiques.

De nos jours, la défiguration se manifeste d'avantage sur Internet, car de nombreux rootkits facilitent ce type d'attaques, mais aussi parce que le coût d'accès à Internet diminue, et que les attaques demeurent virtuelles (permettant à l'attaquant de rester masqué). De plus, une défiguration est beaucoup moins coûteuse que l'utilisation de matériel de type explosif ou autre arme de guerre.

2 Qui est concerné ?

Toute entreprise, organisation ou personne ayant un serveur Web connecté à Internet ou à un autre réseau de communication peut être la cible d'une défiguration. Il n'est pas nécessaire d'avoir un site particulièrement intéressant, le site personnelle d'un citoyen pourra très bien aussi être victime de ce type d'attaque.

3 Comment cela fonctionne-t-il ?

Plusieurs types de moyens peuvent être utilisés pour accomplir ce genre d'attaques. Ces moyens sont de complexité et de portée différentes, en fonction de leurs impacts voulues.

Parmi les moyens les plus courants, on trouve les défigurations de sites Web par l'exploitation de vulnérabilités et les «attaques sémantiques ».

La majorité des défigurations se fait par l'exploitation d'une vulnérabilité existante sur le serveur Web, permettant le changement du contenu du site Web ou de la page d'accueil de ce dernier. Dans certains cas, le pirate va carrément effacer tout le contenu du site.

Les attaques sémantiques consistent à changer légèrement le contenu des différentes pages Web afin d'en changer le sens, généralement pour faire passer une idée différente de celle d'origine. Cette modification est difficile à détecter par le responsable du site Web (webmaster), contrairement à la défiguration simple qui change l'apparence complète du site Web.

suite au verso

Defacement / Défiguration

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

4 Pourquoi se protéger ?

Les sociétés devenant de plus en plus dépendantes des réseaux de l'information, la simple modification de ceux-ci peut provoquer des dommages non négligeables de type économiques, sociaux, logistiques, émotionnels ou encore environnementaux.

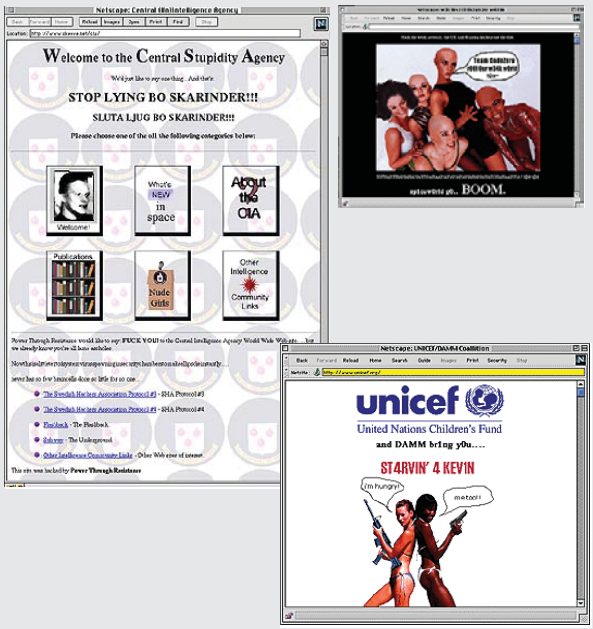
De plus, le public et les journalistes sont fascinés par tous les types d'attaques informatiques, ce qui conduit à une large couverture dans les médias. De fait, une défiguration conduite souvent à une baisse flagrante de l'image de marque de la victime.

Exemples :

En 1999, après le bombardement « non tactique » de l'ambassade chinoise à Belgrade, des attaquants chinois ont déposé des messages du type « nous ne cesserons d'attaquer jusqu'à ce que la guerre s'arrête » sur des sites Web gouvernementaux américains.

En avril 2001, après la collision au dessus de la Chine entre un avion espion américain et un chasseur chinois, et l'incarcération de l'équipage américain en Chine, des groupes de hackers des deux camps se sont menés une guerre violente. Plus de 1200 sites Web américains ont été défigurés et probablement autant de sites en Chine.

Si l'on considère que la défiguration de sites Web constitue le tout premier degré de cyber-attentat, on peut étudier les conflits Inde/Pakistan et Israël/Palestine. Depuis 1999 jusqu'à aujourd'hui on voit des défigurations de sites Web appartenant aux différentes parties. On observe un flagrant parallèle entre le nombre de défigurations et les événements politiques et militaires dans les régions citées.



5 Comment se protéger ?

Pour vous protéger contre une défiguration voire de certaines attaques sémantiques, il existe plusieurs mesures préventives principales qui sont :

- Utilisez un contrôleur d'intégrité ou de dispositifs anti-intrusion. Ces dispositifs contrôlent la non-modification du contenu des pages, incluant la page d'accueil, d'un site Web.
- Installez des patches sur le serveur Web. Ils permettent de réduire le nombre de vulnérabilités et donc de réduire la probabilité d'intrusion sur le serveur.
- Confiez à des personnes de confiance, externes ou internes à l'organisation, la vérification et le contrôle régulier du site Web à protéger, par exemple consultation de l'intégrité du contenu une fois par jour.

Grâce à ces trois mesures préventives, il est possible pour vous de réduire la probabilité de défiguration d'un site Web.