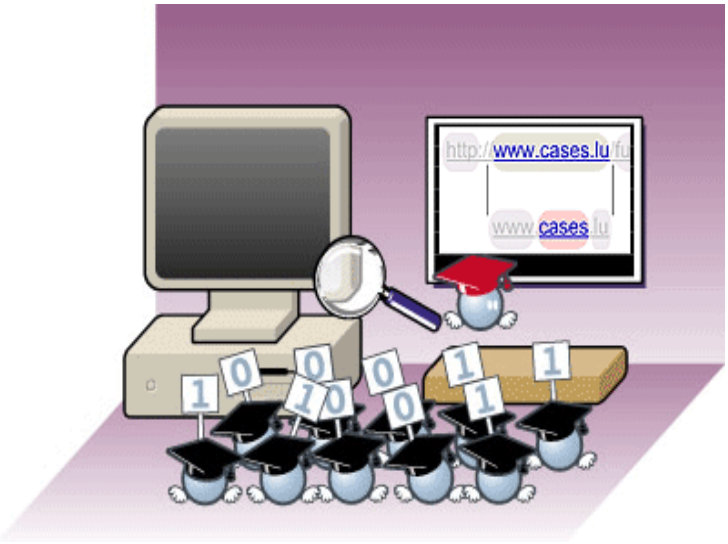
Attaques sur noms de domaine

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Ce document traite du thème des attaques sur les noms de domaine, perpétrées par les pirates informatiques. La connaissance d'un nom de domaine est une des clés pour accéder à l'information sur le Web mais depuis qu'Internet est utilisé en masse par le grand public, les pirates ont multiplié leurs attaques et dirigent parfois leurs victimes vers un autre site Internet que celui initialement désiré. Deux principaux types d'attaques sont à connaître
- Le cybersquatting
- Le typosquatting
Elles concernent autant les personnes privées que les organisations et grandes entreprises, victimes, soit de se voir déposséder d'un nom de domaine, qui, en toute logique, devait leur revenir ; soit redirigés vers d'autres sites que ceux souhaités, par le simple fait d'une erreur de frappe.

Table des matières



1 C'est quoi ?

Il existe deux principaux types d'attaques sur les noms de domaines :

1.1. Le Cybersquatting

L'attaque dite de cybersquatting consiste à déposer, en premier, un nom de domaine choisi en fonction de l'actualité, des entreprises reconnues, des modes, etc. En spéculant sur la prochaine notoriété du nom de domaine déposé, l'objectif est de bénéficier de sa notoriété, tandis qu'en anticipant la volonté de l'entreprise de l'obtenir, le cybersquatter espère le revendre au prix fort et réaliser ainsi une plus-value conséquente.
Aujourd'hui, le cybersquatting est puni par la justice qui ordonne le plus souvent la cession de nom de domaine déposé dans un objectif de cybersquatting, à l'organisation légitime, donnant ainsi tort au cybersquatter.

1.2. Le Typosquatting

Le typosquatting est une forme de cybersquatting reposant sur la probabilité que les internautes feront des erreurs de frappe ou se tromperont de TLD lors de la saisie d'une adresse Internet. Misant sur ces erreurs, le typosquatter dépose un nom de domaine pour diriger l'internaute vers un autre site que celui initialement désiré.

La plupart du temps, les sites pornographiques ou de casinos en ligne abusent du typosquatting pour attirer des visiteurs. De même, le typosquatting revêt parfois la forme d'attaques visant à détourner la clientèle d'un concurrent vers un autre site Internet.

Une variante du typosquatting consiste pour les pirates à déposer des noms de domaine dont l'apparence visuelle est très proche de celui d'une organisation de confiance. Cette technique est parfois employée dans le cadre d'attaques de phishing.

2 Comment cela fonctionne-t-il ?

Pour perpétrer ces attaques, les pirates peuvent :
- Déposer un nom de domaine comportant une ou des fautes de frappe conduisant vers un service similaire d'une autre société,
- Déposer un nom de domaine comportant une ou des fautes de frappe conduisant vers un service totalement différent,
- Déposer des noms de domaine et service identique mais TLDs et éditeurs différents,
- Déposer des noms de domaine identiques mais TLDs différents,
- Réaliser des attaques sur l'apparence visuelle du nom de domaine (mimétisme de nom de domaine),
- Réaliser des attaques sur des déclinaisons de noms de domaine.

Exemples:
- www.googl.de (faute de frappe de www.google.de sans le E) conduit vers un autre moteur de recherche que Google.
- www.wetter.fr et www.wetter.de, tous deux proposent des prévisions météorologiques pour l'Allemagne, sont rédigés en langue allemande. Contenu et langue similaires, mais éditeur différent (Lycos ou RTL)

Attaques sur noms de domaine

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

3 Qui est concerné ?

Tous les citoyens, entreprises et administrations déposant des noms de domaines et/ou souhaitant consulter un site précis mais se trompant, même de peu, dans l'écriture de l'adresse.

4 Pourquoi se protéger ?

4.1. Concernant le cybersqautting

Puisque le dépôt de nom de domaine sur Internet repose bien souvent sur la règle du premier arrivé / premier servi, le cybersquatter essaie d'être le plus rapide pour parvenir à « squatter » un nom de domaine qui aurait pu revenir de droit à une société renommée. La société n'est alors plus en mesure d'obtenir son nom de domaine à moins de lui verser une forte somme d'argent pour libérer le nom de domaine.
Il faut également rester en alerte lors de l'ouverture de nouveaux gTLDs. Les cybersquatters se tenant prêts à déposer en masse de nombreux noms de domaine utilisant ce nouveau champ d'action qui leur est offert. Ainsi, des sociétés reconnues se sont vues privées de leur nom de domaine en .mobi, des cybersquatters ayant été les plus rapides lors de l'ouverture de celui-ci.

4.2. Concernant le typosqautting

En anticipant les erreurs de frappe des internautes, le typosquatter dépose un nom de domaine, très proche de celui dont il souhaite s'octroyer la notoriété…et voit le nombre de ses visiteurs augmenter ; alors que le site piraté voit sa fréquentation baisser.

5 Comment se protéger ?

Les contre-mesures à appliquer sont quasi identiques à celles destinées au phishing.

5.1. Pour les particuliers

Saisir soi-même l'adresse habituelle du site et non pas celle donnée dans le corps du message,
Prendre le plus grand soin dans la saisie d'adresse Internet, et ainsi, éviter les fautes de frappe,
Ne jamais cliquer sur un lien contenu dans un e-mail.

5.2. Pour les organisations et entreprises

Réserver toutes les déclinaisons possibles de leur nom de domaine en fonction de chaque gTLD,
Réserver toutes les déclinaisons possibles du nom pour chaque pays dans le monde,
Eventuellement, réserver des noms de domaine en jouant sur les fautes de frappe potentielles (sachant que cette contre-mesure est aléatoire et onéreuse).

CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur