BENIN DNS FORUM

Menaces et contres mesures sur les noms de domaine

Ramanou BIAOU
Engineer in cybersecurity and scalability of Internet system
CyberSpector/World Internet Labs

b.ramanou@cyberspector.com
@RamanouB

PLAN DE LA PRÉSENTATION

- Nom de Domaine
- Les principales menaces
- Les contres mesures

3 Nom de Domaine

- C'est une adresse sur internet permettant d'accéder à des services et des contenus.

- Composition d'un NOM, un POINT et une EXTENSION

3 Nom de Domaine

- Votre Adresse postale sur Internet
- Nécessaire pour la création de votre site Internet public
- Votre nom de domaine vous permet d'exprimer toute votre créativité, par le choix des mots et des extensions qui font sens pour votre public
- Le but est de communiquer un nom sympathique au lieu d'un chiffre (IP addresse)

Les Problèmes ?

5 CyberSquatting

- Achat ou usage des noms de domaine proches ou identiques au nom d'un tiers
- Intention de revendre à un tiers le nom de sa marque ou se rapprochant de la marque
- L'achat et la vente de noms de domaine est une activité légale (on parle en franglais de « domaining »)

5 CyberSquatting

- Le cybersquatting ne vise pas à tromper l'internaute (contrairement au hameçon- nage), uniquement à priver la victime d'un nom de domaine qu'elle aurait pu prendre

- On parle de Cybersquatting si quelqu'un enregistre un nom identique à sa marque ou s'y rapprochant

- **Banquepostale.bj** et **bankpostale.bj** ou **banquepostalee.bj**

6 Les Spams

- Lorsqu'un domaine identique ou proche au nom d'un tiers est utilisé dans du spam (envoi en masse de courrier non sollicité

- Vous recevez un courriel de **bankpostale.bj** au lieu de **banquepostale.bj**

- Si je reçois un message prétendant venir de contact@banquepostale.bj cela ne prouve pas que c'est la banque postale qui vous envoie le courriel ni que le courriel est piraté

7 Malware

- Logiciel malveillant que l'utilisateur n'a pas demandé à Installer
- Installation en consultant certains sites web (Cheval de troie, streaming, Site pour adultes)
- Pas d'analyse de nom de domaine avant de l'Installer
- Pirate des sites légitimes pour y déposer un script de Malware
- Eviter d'accuser à tort le TLD

8 Mensonges

- Si on veut répandre des fausses informations, il peut être utile de disposer d'un nom de domaine « crédible »
- Peu d'utilisateurs vérifient le nom de domaine
- Cas de vinci suite à une fausse nouvelle sur le domaine **vinci.group**

9 Hameçonnage

- L'hameçonnage consiste à attirer les victimes vers un site Web qui ressemble à un site Web qu'elles connaissent
- Le méthodes techniques permettent de détourner via DNS ou BGP le Traffic d'un site
- Le nom de domaine est légitime mais le site est faut
- Et Formatage des messages électronique en HTML est une bonne source de dissimulation de fausses adresses

Quelles actions face à ces différentes menaces ?

Actions face aux menaces

- Le registre n'est pas forcément responsable des abus commis par les titulaires de noms de domaine. Au contraire, les règles d'enregistrement précisent souvent que le titulaire est seul responsable

- Il n'y a pas de solution technique magique, qui résoudrait tous ces problèmes à la fois, et sans inconvénients

Actions face aux menaces

- Surveiller les listes noires
- Surveiller sa marque ou ses domaines prioritaires de services
- Activer le DNSSEC sur les domaines
- Activer l'authentification de l'envoi des mails via votre domaine
- Vérifier les données sociales fournir lors de l'enregistrement (par exemple vérifier que la ville indiquée dans l'adresse existe bien dans le pays en question)

Merci pour votre attention

Questions - Contributions - Commentaires