

Paris, 17/04/2009

Les utilisateurs de Twitter victimes d'un ver

Qu'est-ce que Twitter ?

Twitter est un site communautaire dans lequel les membres postent des informations courtes les concernant ou concernant leur communauté. On peut le qualifier de « micro-blogue ». Il est possible de suivre l'actualité de personnes. On devient dans ce cas le « follower » de la personne et l'on a accès aux éléments postés par cette personne.

Peut-on parler d'un ver ?

Un ver est un programme externe qui sera téléchargé puis exécuté sur l'ordinateur. Dans ce cas, le ver profite simplement de certaines faiblesses du navigateur et du serveur WEB pour se "reproduire". Aucune présence de programme externe n'est donc nécessaire. Il convient donc mieux de parler d'un "ver WEB" ou "ver XSS/CSRF" car ce ver exploite des vulnérabilités de "Cross-site scripting (XSS)" et de "Cross-site request forgery (CSRF)".

Concrètement que fait-il ?

Les motivations du jeune hacker (17 ans) ne sont pas claires. C'est sans doute pour gagner en notoriété qu'il a mis au point ce ver. Ce dernier poste de façon automatique à la place d'un utilisateur légitime, un message incitant ses « followers » à aller visiter un site Web. Si une personne clique sur ce lien, le même sort lui est réservé. (Ses « followers » verront que cette personne a posté un message incitant à aller visiter ce site WEB)

Quel est son mode opératoire ?

Tout d'abord, le ver utilise une faille XSS. Le XSS ou (cross site scripting) permet à un attaquant de faire exécuter du code javascript ou html au navigateur de l'utilisateur.

Ce type d'attaque est le plus souvent utilisé pour récupérer les cookies de sessions de l'utilisateur ou pour modifier l'apparence du site WEB.

En l'occurrence, dans ce cas il s'agit de récupérer le cookie de session de l'utilisateur.

Une fois le cookie récupéré une requête Ajax est forgée de façon automatique avec votre cookie session (ce cookie sert de gage au serveur WEB pour déterminer si la requête vient de vous). Cette requête simule totalement ce que vous auriez fait en temps qu'utilisateur pour poster un message incitant vos « followers » à se rendre sur un site WEB.

Dans la deuxième version du ver, le simple fait de visiter la page twitter d'une personne "infectée" permet de déclencher l'attaque.

Quels sont les impacts de ce type d'attaque ?

Dans ce contexte précis, l'impacte pour les utilisateurs était très faible (poste d'un message à la place de l'utilisateur légitime). Toutefois, l'attaquant prend le contrôle du navigateur pour le forcer à réaliser des actions; on peut donc imaginer les dégâts que peuvent réaliser ce type d'attaques sur des sites sensibles, car ce scénario peut également être perpétré sur des sites traditionnels.

Le mécanisme est maintenant bien rodé sur des sites communautaires. Sans être devin, il est fort à parié que ce genre d'attaque sera perpétué sur d'autres type de sites. On imagine bien le potentiel de ces attaques : forcer un utilisateur à acheter ou vendre un bien ou un service ... Les hackers ne sont limités que par leur imagination et la robustesse des systèmes de sécurité qu'ils trouveront face

à eux.

Le trafic généré par ce type de ver doit aussi être pris en considération, car il peut mettre à mal la disponibilité du site WEB.

Comment se prémunir de ce type de ver ?

Si vous avez un serveur WEB et que vous souhaitez prémunir vos clients de ce type de vers, on peut:

- Prendre en compte les aspects de sécurité lors du développement d'applications WEB (validation des données envoyées par l'utilisateur);
- Renforcer le control des en utilisant des bibliothèques qui épurent les éléments transmis par les l'utilisateur (Par exemple [AntiSamy](#));
- Taguer les cookies de sessions avec le flag [HTTPOnly](#) . Ce flag permet d'interdire l'accès au cookie de session via java script rendant les attaques XSS qui ciblent les cookies de session inefficaces.
- Utiliser un [Firewall Applicatif WEB](#) (WAF) .Cet équipement situé devant le serveur WEB permet de bloquer les tentatives d'injections de code.(Il peut aussi flaguer à la volée les cookies de session en HTTPOnly si l'on n'a pas de contrôle sur l'applicatif)

Si vous êtes utilisateur:

- Utiliser [noscript](#) sur Firefox (ce module permet de n'activer java script qu'au cas par cas).

Johanne Ulloa

julloa@denyall.com