

SECURINETS



**CLUB DE LA SECURITE INFORMATIQUE
INSAT**

SECURILIGHT 2011

**Sécurisation des services internet et des
réseaux sociaux**

Chef Atelier : Maroua GASMI (RT5)

Naoures KHAIRALLAH (RT5)

Eya HJIRI (RT3)

Imen SOUILHI (RT3)

Elyssa BERRICH (MPI)

30/11/2011

L'internet ne cesse plus d'offrir des services qui sont de plus en plus importants dans notre vie quotidienne, ce qui nous rend de plus en plus dépendants.

Mais comme tout autre système, ces services présentent des risques à coté de leurs maints avantages. Citons par exemple la confidentialité, qui est le principal but des attaques effectuées par les hackers.

C'est au cours de cet atelier donc, nous avons introduits quelques attaques subites sur divers services et les moyens favorables pour s'en protéger.

1) E-commerce:

On appelle e-commerce, l'utilisation d'un média électronique pour la réalisation de transactions commerciales.

Les commerçants généralement demandent des informations personnelles et le numéro de carte de crédit du client à l'aide d'un formulaire à partir du site même. Cette organisation traite ensuite elle-même la demande comme s'il s'agissait d'une commande téléphonique où le client fournit le numéro de sa carte de crédit.

Cette forme de e-commerce n'est nullement sécurisée. En fait, plein types d'attaques peuvent avoir lieu, dans cet exemple nous citons le Phishing et le Pharming.

I. Pharming :

Cette technique est une amélioration du phishing. Elle consiste à s'attaquer directement à la résolution DNS. L'internaute tape correctement l'adresse du site d'origine dans son navigateur (<http://www.mabanque.fr>) mais l'adresse IP associée est piratée et il accède finalement au site contrefait. Pour réaliser ce tour de force, les pirates disposent de plusieurs modes d'attaque :

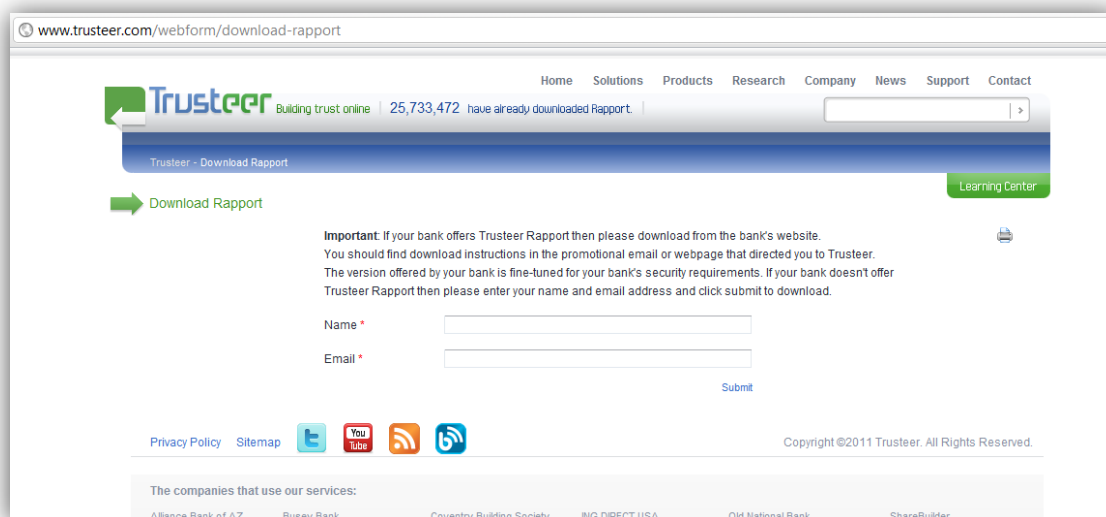
La manipulation du cache DNS de l'internaute. Chaque ordinateur gère un cache des résolutions DNS qu'il a déjà effectuées afin d'accélérer les résolutions suivantes similaires. Un virus ou un cheval de Troyes peut pirater ce cache et ainsi modifier artificiellement l'adresse IP associée à un site pour l'utilisateur infecté. De par la vulnérabilité de nombreux postes informatiques, ce type d'attaque est le plus simple à mettre en œuvre ;

La manipulation d'un serveur DNS d'un FAI. Ce type d'attaque est plus efficace mais plus difficile à mettre en œuvre. Il consiste à insérer un enregistrement DNS frauduleux directement sur le serveur DNS d'un fournisseur d'accès à Internet. Tous les clients de ce FAI utilisant ce serveur seront alors affectés par l'attaque ;

La manipulation d'un serveur DNS autoritaire. Cette attaque est identique à la précédente mais concerne directement un serveur DNS autoritaire pour le nom de domaine visé. Elle est ainsi la plus dévastatrice car chaque internaute souhaitant accéder au site contrefait sera affecté.

II. L'outil de protection: Trusteer Rapport:

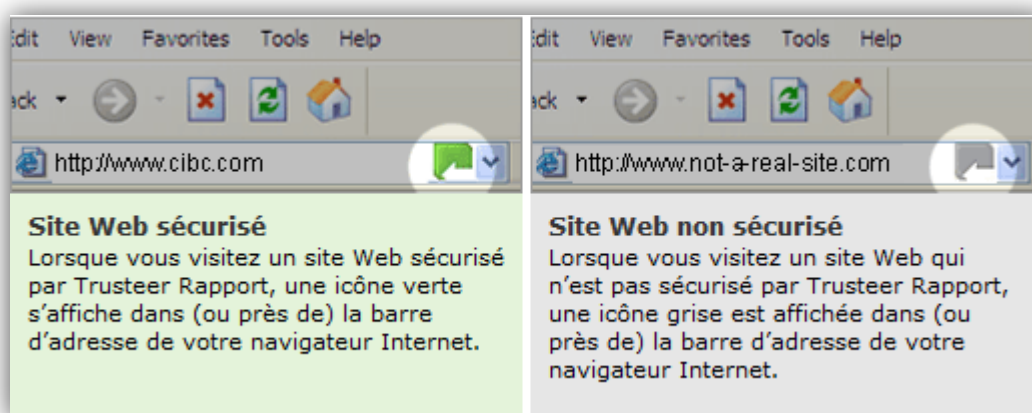
Pour protéger efficacement votre ordinateur, nous vous offrons Trusteer Rapport, un logiciel de protection en direct contre la fraude et le vol d'identité. En installant le logiciel Trusteer Rapport, vous améliorez la sécurité de votre ordinateur.



Trusteer est un outil, une fois installé dans votre ordinateur, sera automatiquement intégré dans les différents navigateurs existants.

Lorsque vous tapez l'URL d'un site e-commerce (banque ou site de vente), Trusteer parcourt une base de données distantes pour vérifier si c'est bien cette adresse IP qui correspond à l'URL entré.

Si tout va bien, l'indicateur aura la couleur verte sinon il reste en gris. Dans le cas de Pharming, Trusteer permet de rediriger l'utilisateur vers la vraie adresse IP.



Cet outil offre la possibilité d'ajouter un site non e-commerce pour qu'il soit vérifié dans un futur accès.



Exemple de site non protégé



Le site est maintenant protégé et toute tentative de phishing ou pharming sera automatiquement signalée.

Pour télécharger le plugin voilà le site :

<http://www.trusteer.com/webform/download-rapport>

2) Boite mail:

C'est un service de transmission de messages envoyés électroniquement via internet dans la boîte aux lettres électronique d'un destinataire choisi par l'émetteur.

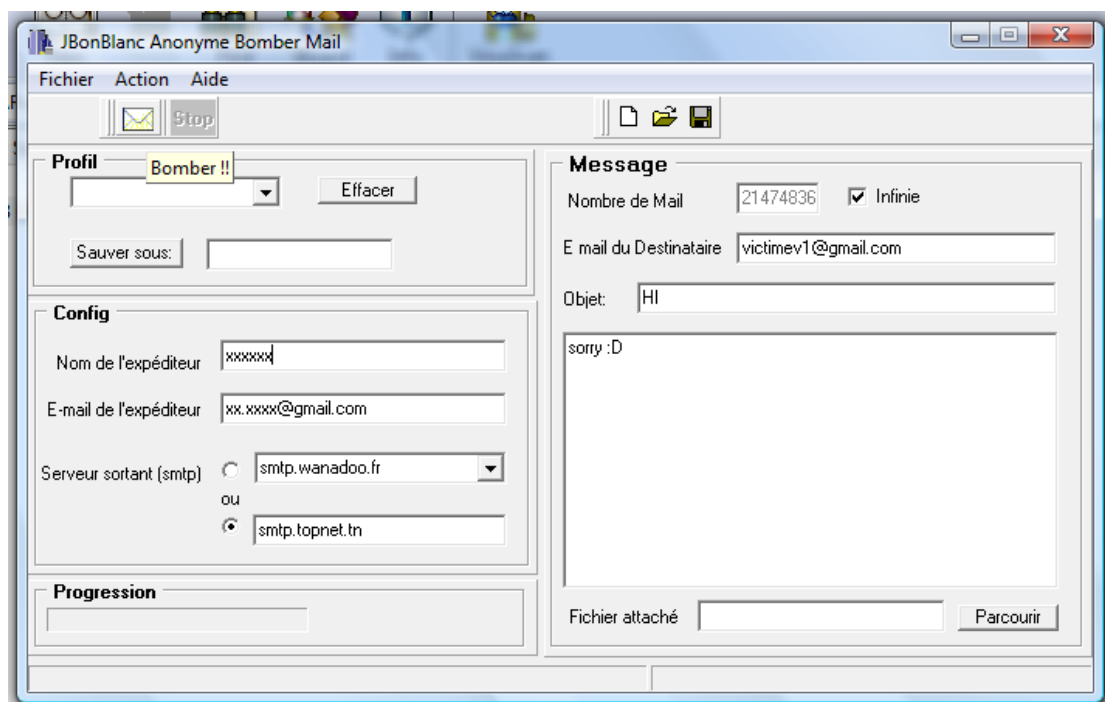
Ce type de service, peut être également vulnérable à plusieurs types d'attaques. Citons par exemple le mailbombing.

I. Mailbombing:

Le Mail Bombing consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. L'objectif étant de :

saturer le serveur de mails saturer la bande passante du serveur et du ou des destinataires, rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

Il existe plusieurs outils pour effectuer cette attaque, tels que Jbonblanc.



II. Outils et conseils pour se protéger du mailbombing:

- Tout d'abord, si vous avez une adresse personnelle à laquelle vous tenez, ne la communiquez qu'aux personnes dignes de confiance. Il faut aussi penser à créer un second compte de messagerie, pour tout ce qui est mailing List par

exemple et groupe des discussions. Si ce compte est attaqué vous pourrez sans difficulté reprendre une autre adresse et vous réabonner.

- Sachez que vous pouvez aussi utiliser le logiciel eremover pour éviter les mails bombers, et installer un logiciel anti spam qui interdira la réception de plusieurs messages identiques à un intervalle de temps trop court.
- filtrez les messages reçus à leur arrivée dans votre logiciel de messagerie.
- Dans Outlook choisissez "Outils" puis "Assistant Gestion des messages...",
- Dans Outlook Express choisissez "Outils" puis "Règles de messages" puis "Courrier...",
- Dans Mozilla sélectionnez le compte puis cliquez sur "Create message filters" et laissez-vous guider.
- Définissez une règle de filtrage pour que les messages comportant l'expression "ADV:", "[ADV]" ou "ADV " dans leur objet soient redirigés vers un répertoire poubelle. Ces expressions sont parfois utilisées par les spammers pour signaler que le message est une publicité (advertisement, en anglais) ;
- Définissez une règle de filtrage pour que les messages comportant l'expression "ks_c_5601-1987", "KS_C_5601-1987" ou "euc-kr" dans leur entête soient redirigés vers un répertoire poubelle, si vous n'avez pas de correspondant coréen. Ces expressions correspondent précisément aux jeux de caractères du Coréen, une langue très fréquente dans les spams internationaux ;
- Définissez une règle de filtrage pour que les messages contenant l'expression ".com.br", ".com.tw", ".net.tw", ".co.kr", ".co.jp" ou ".com.cn" dans l'adresse d'expéditeur ou dans leur entête soient redirigés vers un répertoire poubelle, si vous n'avez pas de correspondant brésilien, taïwanais, coréen, japonais ou chinois. Ces domaines exotiques sont également assez largement utilisés dans les spam internationaux.
- Si vous avez été victime d'un mail bombing, il est parfois possible de remonter jusqu'à l'émetteur. En effet, il existe des informations dans chaque message qui donnent des informations sur leur auteur.

Si vous retrouvez des informations comme l'adresse email ou le serveur qui ont permis l'arrivée des messages, il est important de se plaindre auprès du fournisseur d'accès. En effet, dans la plupart des cas, les fournisseurs d'accès n'apprécient pas ce type de procédés via leurs serveurs et prennent toutes les mesures nécessaires pour empêcher les auteurs de recommencer.

3) CMS (WordPress):

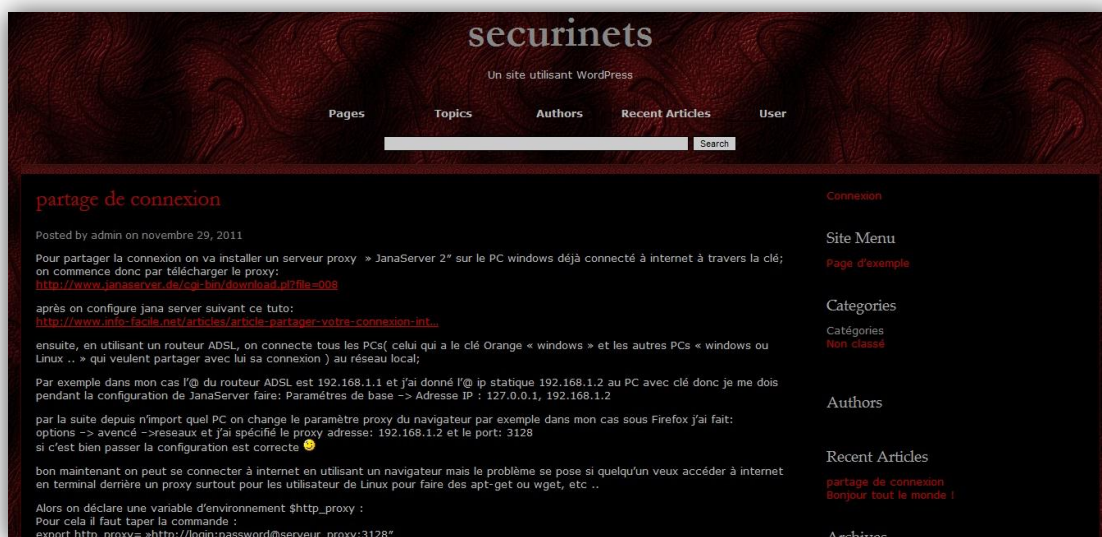
les CMS est une famille de logiciels destinés à la conception et à la mise à jour dynamique de site Web ou d'application multimédia.

I. Présentation de WordPress:

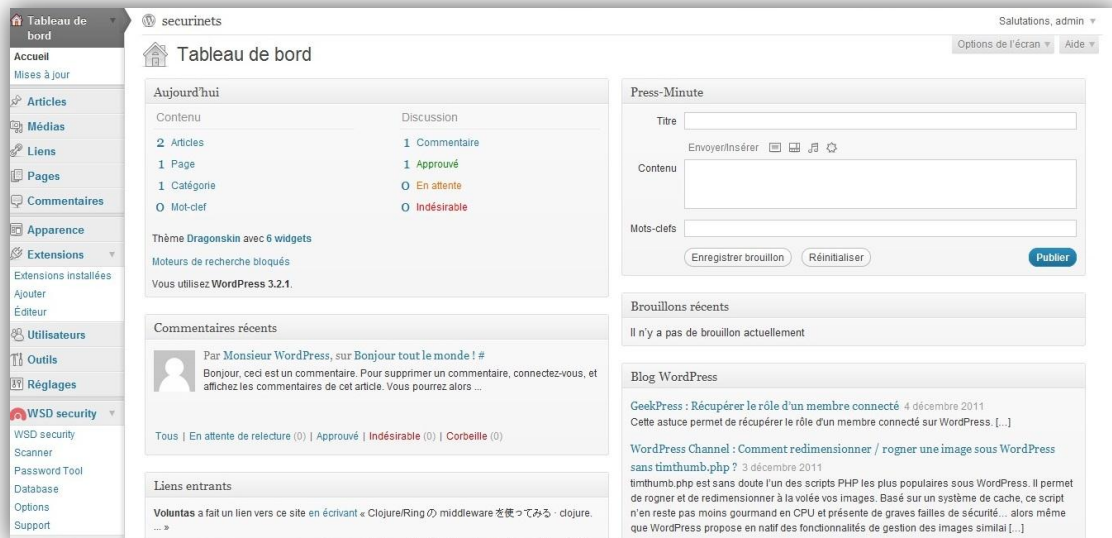
WordPress : c'est un CMS (Content Management System) permettant de créer aisément un site web ou blog.

La gratuité, la facilité d'utilisation et l'étendu des fonctionnalités présentent dans ce système de gestion de contenu ont permis sa renommée, en particulier sur la blogosphère.

Il est désormais entouré par une grande communauté qui permet au CMS de disposer à aujourd'hui de nombreux plugins (extensions) et thèmes augmentant ses possibilités de personnalisation et ceci de manière simple.



Interface des visiteurs du blog



Interface administrateur

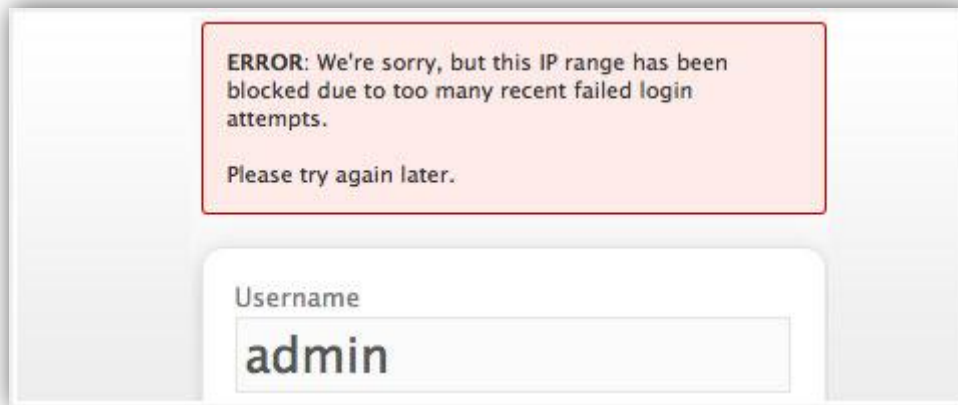
II. Outils de sécurisation:

Afin d'éviter les attaques, certains plugins sont appelé à être présents.

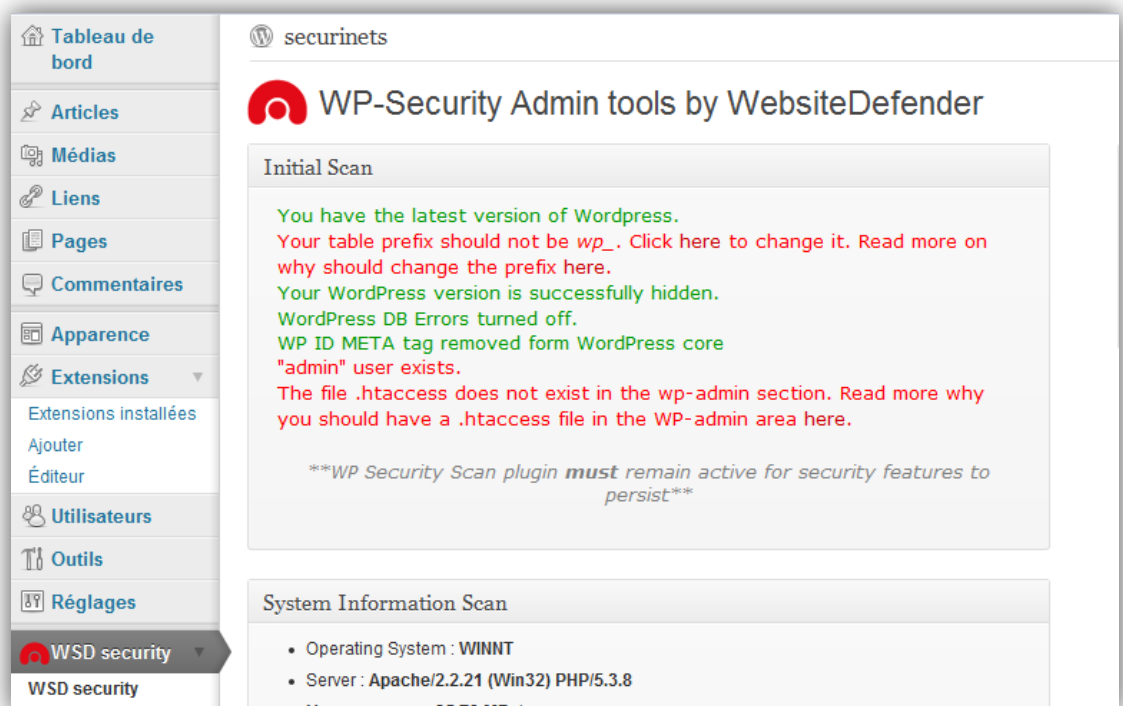
- ❖ Login Lockdown : ce plugin enregistre les tentatives infructueuses d'accès au compte administrateur de votre blogue. Après quelques tentatives l'adresse IP est automatiquement bloquée. L'administrateur gère lui-même les réglages de ce plugin :



Après avoir dépassé le nombre de tentatives permises le message suivant s'affichera :



- ❖ Wp Security Scan, cet outil est multifonctionnel, il permet entre autre de:
 - scanner votre blog afin de relever d'éventuelles failles. C'est aussi grâce à ce plugin que vous devrez modifier l'extension de vos tables WordPress afin de limiter les risques d'injections SQL pour votre site internet.



- Vérifier le niveau de sécurité de votre mot de passe d'administration :

WP - Password Tools

Password Strength Tool

Type password: Password Strength: **Strong**
Minimum 6 Characters

Strong Password Generator
Strong Password: **8vasvXIDCzi47@**

For comments, suggestions, queries and bug reports please visit the [WebsiteDefender Forums](#). Plugin by [WebsiteDefender](#)

➤ vérifier le niveau de permissions sur les fichiers et répertoires :

WP - Security Scan

Directory Info

Warning: fileperms() [function.fileperms]: stat failed for: //htaccess in C:\Program Files\EasyPHP_5.3.8.1\www\wp-content\plugins\wp-security-scan\libs\functions.php on line 39

Name	File/Dir	Needed Chmod	Current Chmod
root directory	..	0755	0777
wp-includes/	../wp-includes	0755	0777
.htaccess	../htaccess	0644	0
wp-admin/index.php	index.php	0644	0666
wp-admin/js/	js/	0755	0777
wp-content/themes/	../wp-content/themes	0755	0777
wp-content/plugins/	../wp-content/plugins	0755	0777
wp-admin/	../wp-admin	0755	0777
wp-content/	../wp-content	0755	0777

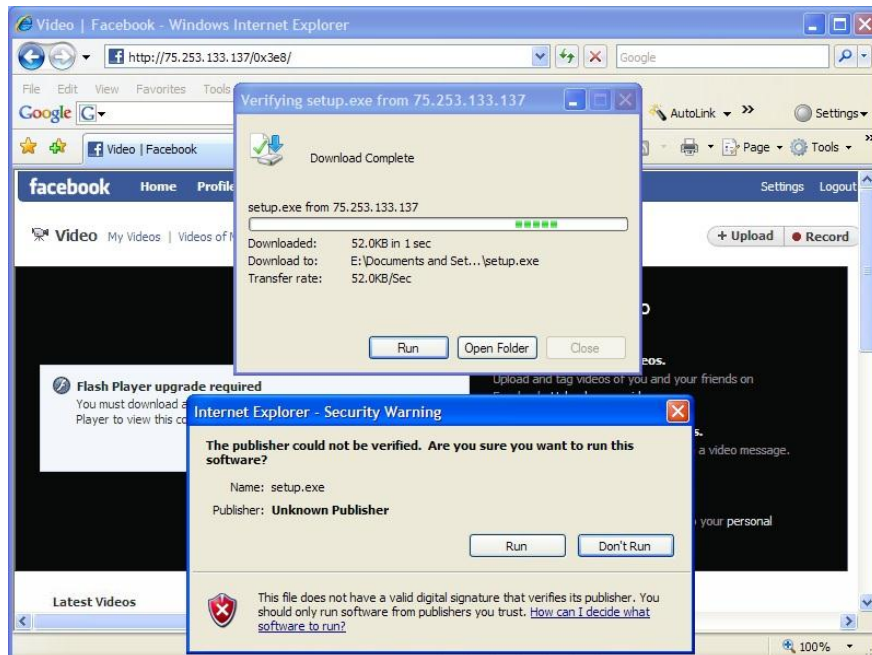
For comments, suggestions, queries and bug reports please visit the [WebsiteDefender Forums](#). Plugin by [WebsiteDefender](#)

4) Réseaux sociaux (facebook):

I. Attaque koobface:

Koobface est un ver informatique qui sévit sur le site communautaire Facebook. Ce ver se propage en envoyant des courriels aux amis des personnes dont l'ordinateur a été infecté, si l'utilisateur a la malheureuse idée de télécharger le programme, son ordinateur va être infecté et dirigera ses utilisateurs sur des sites contaminés lors de recherches

sur Google, Yahoo ou encore MSN. Il serait également capable de dérober des informations de nature personnelle comme un numéro de carte de crédit.



Ce vers peut être détecté par plusieurs antivirus (avast, mcfée, avg, kaspersky) sinon si on est déjà infecté on peut installer un anti-trojan (exple spybot) pour le supprimer.

II. Clickjacking ou Likejacking :

Le *clickjacking*, ou détournement de clic, est une technique malveillante visant à pousser un internaute à fournir des informations confidentielles ou à prendre le contrôle de son ordinateur en le poussant à cliquer sur des pages apparemment sûres.



Le plugin noscript pour firefox <http://noscript.net/> ou bien disconnect pour firefox, chrome et safari <http://disconnect.me/> permettent de se protéger de cette attaque.

Le plugin noscript permet aussi de gérer les permissions de javascript (lecture de vidéo)