

Dans le cadre de ***SECURIDAY 2009***

SECURINETS



Présente

Atelier : Méthodes d'infection et de propagation des malwares

Formateurs: 1. SFAXI Henda
2. BESSAIDI Cherifa
3. SALLEMI Dhia
4. Nabil
5. DHAYA Asma

1. Présentation :

Dans le domaine de sécurité informatique, Il existe plusieurs méthodes d'infection et de propagation des Botnets parmi lesquelles on cite les méthodes suivantes :

- **Les cracks et les Keygens :** Ce sont des programmes qui permettent d'utiliser les logiciels payants sans devoir se procurer les licences nécessaires. Ils sont assez répandus sur les réseaux p2p, et profitent de la confiance de l'utilisateur pour exécuter des codes malveillants qui permettent d'infecter le pc.
- **Les faux codecs :** De faux sites web demandent aux utilisateurs de télécharger de faux codecs ou des contrôles ActiveX pour visualiser des vidéos. Ces codecs sont en fait des malwares qui s'installent sur le pc.
- **Les rogues :** Ce mot désigne de faux logiciels de sécurités : anti-spyware, antivirus.... Une fois installé sur l'ordinateur, ils signalent que le système est infecté par un virus, même s'il est sain, et proposent à l'utilisateur d'acheter une version payante pour procéder à la "réparation". Outre l'escroquerie manifeste, ces programmes contiennent également une fonction de logiciel publicitaire.
- **La navigation sur des sites à haut risque d'infections :** Les pirates utilisent des sites web contenant un code malveillant qui exploite une faille du navigateur pour s'exécuter et installer un malware dans le système. L'exploitation des failles Web permet aux logiciels malveillants de s'installer silencieusement sur l'ordinateur sans s'en rendre compte.
- **Les mails piégés :** Ce sont des mails dont les pièces jointes (document PowerPoint, image, fichiers exécutables..) contiennent des vers et des bots cachés qui s'installent automatiquement dès qu'on télécharge et exécute les pièces jointes.
- **Propagation via les supports amovibles (Clé USB, Flash ...) :** En double cliquant sur un support amovible pour l'ouvrir, Windows vérifie d'abord s'il trouve un fichier nommé autorun.inf. Ce fichier, caché, contient des instructions qui seront exécutées automatiquement lors de l'ouverture du support. S'il ne trouve pas ce fichier, il ouvre l'explorateur windows. Les pirates exploitent ce fichier en y mettant des instructions qui

exécutent automatiquement un programme malveillant présent sur le support et ainsi infecter le pc dès que l'utilisateur double clique dessus.

Pour cet atelier, on va essayer de simuler quelques méthodes d'infection par des malware. La première catégorie concerne les pièces jointes attachées à des mails dont le destinataire peut être l'un de nos contacts (mail spoofing) ou une personne inconnue. Généralement, ce n'est pas l'un de nos contacts qui voudrait faire de nous une machine zombie (à moins qu'il soit un hacker et qu'il nous en veule pour quelque chose ^^), ce serait une personne malveillante qui usurpera l'identité de l'un de nos contacts ou nous contactera via un autre compte de messagerie dans le seul but de nous convaincre d'extraire la pièce jointe et d'installer ainsi le bot. Les pièces jointes peuvent varier d'une simple image à un fichier flash et par exemple, en cliquant sur l'animation flash, le bot s'installe en back-office.

2. Outils utilisés :

Pour réaliser notre atelier, nous aurons besoin des outils suivants :

- Mirc : client chat.
- IRCXpro : serveur chat.
- Hmail server : serveur mail sous Windows.
- Gspot : notre bot.

Environnement de simulation :

- VMWARE
- Deux machines virtuelles sous WindowsXP

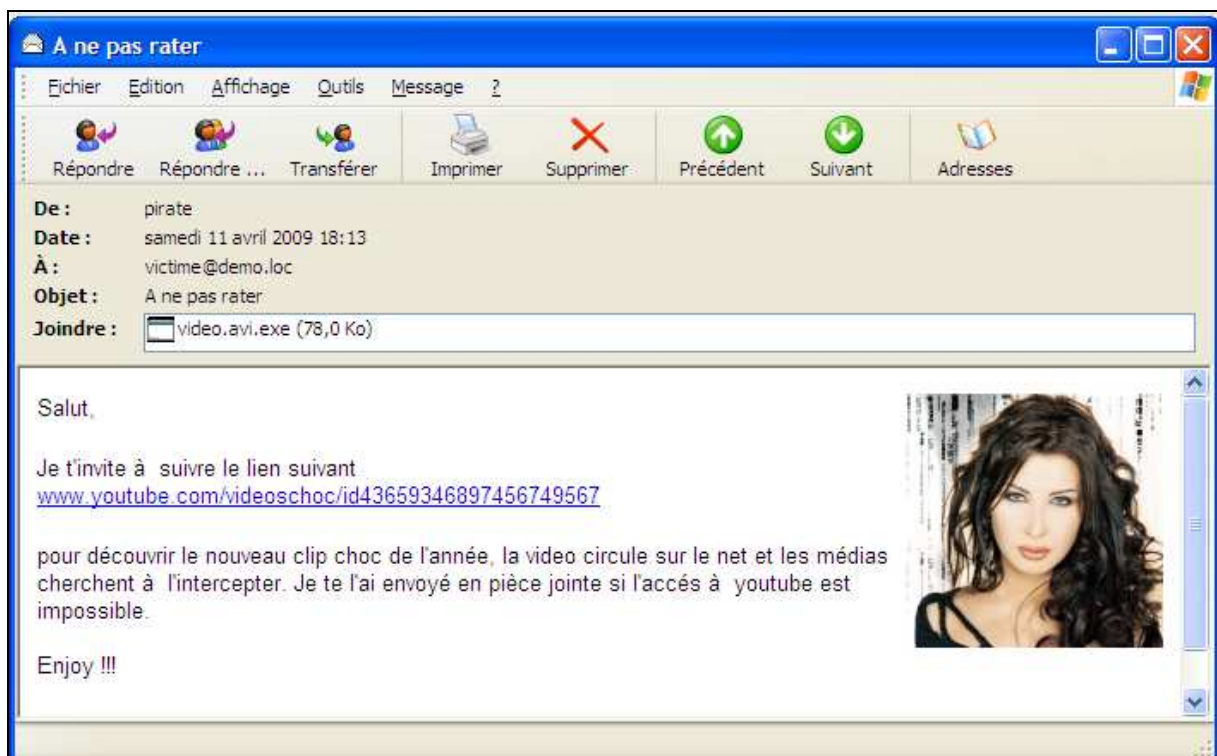
3. Simulation de la première méthode d'infection : Mails infectés :

Comme on l'a déjà cité, les mails infectés peuvent être sous deux formes : le mail spoofing et les spams.

En ouvrant la boîte mail, un internaute découvre un mail de l'un de ses contacts, son contenu est un peu bizarre mais la pièce qui y est jointe a l'air d'être fort intéressante et la curiosité de la découverte l'incite à l'extraire et à la lire. Mais, ce que ne sait pas, c'est que cette pièce jointe contient un bot caché qui s'est installé lors de l'ouverture de la pièce jointe.

Comment ceci a bien pu se passer. Découvrons un des scénarios possibles.

Le hacker a créé une animation flash par exemple, il a ensuite fusionné son bot avec cette animation à l'aide d'un logiciel dédié pour ces faits. Il l'envoie par la suite ce mail en usurpant l'identité d'un des contacts de la victime (mail spoofing) ou en se faisant passer pour une personne étrangère (spam). Et il peut même lui mettre un lien vers une fausse page (détaillée dans la section qui suit).

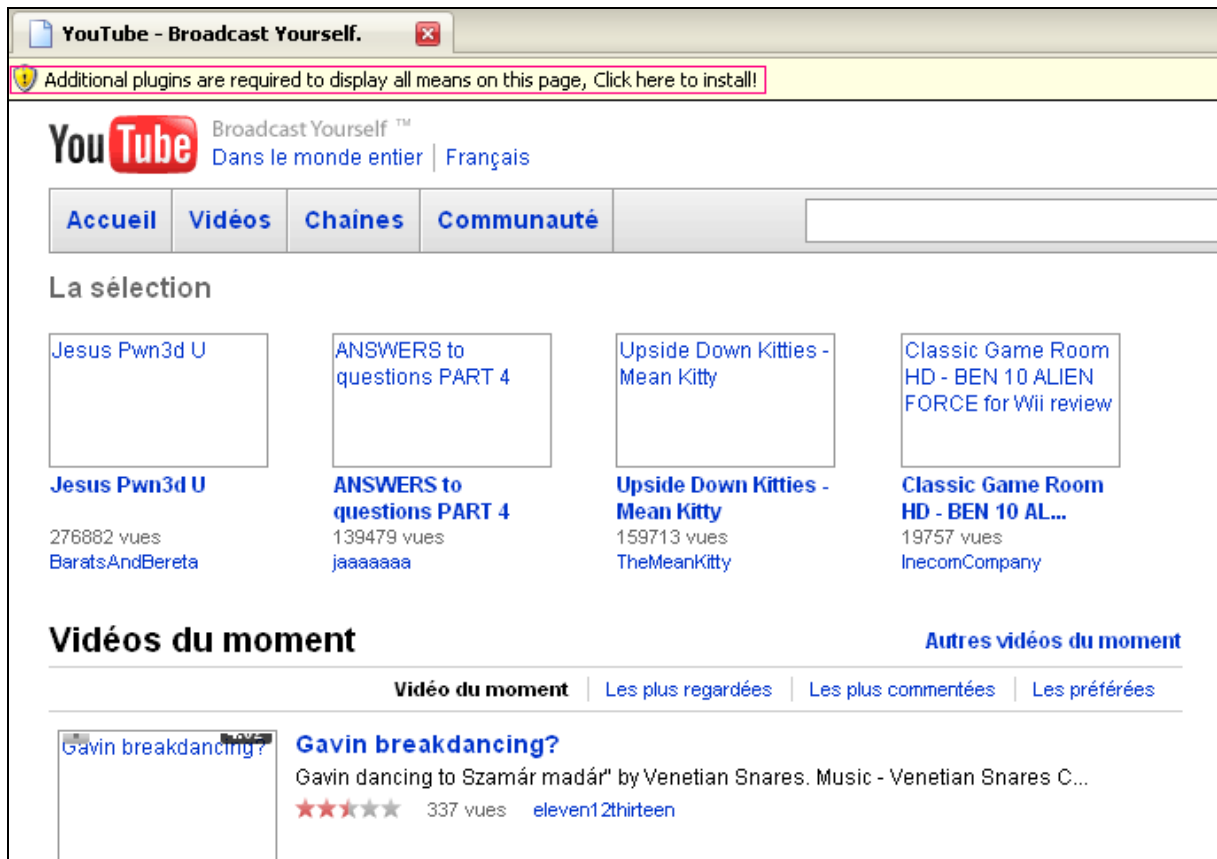


Une fois la machine infectée, le bot se connecte sur un serveur IRC pour recevoir et exécuter les instructions du hacker.

4. Simulation de la deuxième méthode d'infection : Site defacing :

Etant un mordant des vidéos, un addict du site YouTube reçoit un mail qui contient un lien vers une vidéo sur ce site. En cliquant sur le lien, il est redirigé vers une fausse page YouTube conçu spécialement par le hacker pour le piéger.

En ouvrant ladite page, il ne visualise pas très bien son contenu faute de codecs manquants.



-Site Youtube piraté-

Le hacker a joint le bot au soit disant plugin. La victime installe les plugins indiqués par le site et voilà le bot installé. Et encore une machine zombie !!

Le bot se connecte sur le serveur et le hacker fait de la machine zombie se dont il veut, comme cité dans la section précédente.

Conclusion :

Le nombre de malwares sur Internet a considérablement explosé ces dernières années. Pour éviter d'être infecté, chacun se doit de respecter quelques règles parmi lesquelles on cite :

- Mise à jour du système d'exploitation et des logiciels: navigateur, antivirus, bureautique, pare-feu personnel ...
- Eviter de cliquer trop vite sur des liens.
- Ne jamais utiliser un compte administrateur pour naviguer
- Contrôler la diffusion d'informations personnelles.
- Etre vigilant avant d'ouvrir des pièces jointes des emails.