L'Actu Sécurité n°6

Spécial BlackHat 2006

xmco Partners

PLAN

"Il n' y a pas que des casinos à Las Vegas..."

Pendant que le commun des mortels pensait à se ressourcer au soleil, quelques petits malins (environ 3000 !) se sont réunis cet été à Las Vegas, sous l'égide bienveillante de Microsoft, Cisco et d'Enrst and Young afin de présenter leurs nouvelles découvertes...

Eh bien tenez vous bien, cela promet : de la vulnérabilité du Wi-fi, toujours aussi mise à l'épreuve, au piratage de puces RFID (la clé de voûte des passeports modernes) en passant par les nouvelles attaques de flux RSS, l'avenir du piratage s'annonce radieux !
Vista, distribué en version béta à qui veut bien le tester, est d'ores et déjà sérieusement attaqué, par de nombreux chercheurs, si fiers de pouvoir s'attaquer au fer de lance du géant du logiciel.

Parallèlement, la riposte s'organise, puisque l'actualité principale de la rentrée concerne le rachat de ISS par IBM... Espérons juste que la X force demeure toujours aussi performante...
Vous découvrirez dans ce numéro une synthèse des plus grands moments de la Blackhat, ainsi que les différents liens qui vous permettront d'en savoir plus. Nous avons abordé également un sujet important : la corrélation d'événements. Tout le monde en parle, des offres existent de toute part, mais comment s'y retrouver aujourd'hui dans les méandres du marché ? Comment adapter ces solutions à vos systèmes pour en retirer une vraie valeur ajoutée ?

Cette problématique deviendra d'autant plus cruciale que les infrastructures de voix sur IP fleurissent dans les entreprises. J'en profite, d'ailleurs, pour vous annoncer que le numéro d'octobre abordera les risques liés à la Voip.

Je tiens à saluer le travail de mes collaborateurs qui participent chaque mois à la réalisation de cette newsletter. J'espère que ce numéro continuera d' apporter des réponses à vos questions.
Bonne rentrée.

Marc Behar

1. POINT ECONOMIQUE:

IBM RACHÈTE ISS...

Le 23 août dernier, IBM a annoncé le rachat de la société ISS (l'éditeur des fameuses sondes IDS Realsecure), après l'absorption de la société Filenet, Big Blue continue ses emplettes estivales.
Un rachat d'une valeur d'un milliard d'euros pour une société vielle de 12 ans. ISS devient alors une « business unit » de la branche sécurité de la division IBM Global Technology Services (Infrastructure Management Services). Avec ce rachat, IBM compte bien conforter sa place de leader et intervenir dans la sécurité informatique, domaine qui lui faisait défaut.

XMCO | Partners

ISS et la détection d'intrusion

Le début

Société emblématique de la sécurité informatique, ISS est créée en 1994 et s'intéresse alors au secteur porteur de la sécurité informatique. Christopher W. Klaus et Thomas E. Noonan développent le premier logiciel de détection d'intrusion en temps réel. Leur domaine de compétence s'élargit en 2003, avec la création d'un boitier tout en un Provencia : pare-feu, antivirus, VPN. Plus tard, ISS se spécialisera dans le filtrage web et les emails puis dans la sécurité des postes de travail. Une gamme de solutions managées (Managed Services) vient consolider ce portefeuille d'ISS, faisant de l'éditeur le numéro 1 du domaine. Cependant, ISS n'est jamais parvenu à prendre le dessus sur CHeckpoint, leader du secteur des pare-feux et des passerelles de sécurité.

La fin

Après avoir réalisé un chiffre d'affaire de 300 millions de dollars, ISS a céder aux avances de Big Blue .

Près de 1300 employés travaillaient pour ISS dans 35 bureaux répartis à travers le monde. Tom Noonan restera à la tête de la nouvelle division d'IBM où il compte construire « le standard global de la sécurité informatique».

IBM et la "sécurité à la demande"

IBM fait les soldes

Après le rachat de RSA par EMC en juin, IBM, sans doute vexé par l'insertion de Microsoft dans le monde de la sécurité, a décidé de continuer ses emplettes. Le mois de juillet avait déjà été marqué par l'appétit grandissant de Big Blue. Les sociétés Filenet (1,6 milliard de dollars), MRO software (740 millions) et Webify Solutions avaient déjà été racheté pour un total de plusieurs millards de dollars.

IBM, qui souhaitait depuis quelques temps entrer dans le domaine de la sécurité, engloutit cette firme aux 11000 clients d'ISS dont parmi eux les 17 plus grandes banques mondiales.

Objectif : les MSS "Managed Security Services"

Derrière ce rachat, il est facile de deviner la stratégie d'IBM : les MSS où l'externalisation de la surveillance sécurité.

IBM fournit déjà l'infrastructure et gère les parcs informatiques de nombreuses entreprises. Le géant compte ainsi jouer sur deux tableaux en proposant à la fois ses offres et des solutions de sécurisation des réseaux d'entreprises.
De plus, Big Blue possède les solutions de monitoring Tivoli Software. L'ajout à sa gamme des logiciels et des appliances ISS de détection d'intrusion permet d'imaginer une nouvelle gamme de services de management de solutions de sécurité à distance.

IBM possède en effet une grosse carte à jouer sur ce marché : avec les 17 plus grosses banques du monde déjà externalisées chez IBM Global Services, IBM souhaite se faire une place sur ce marché prisé des actionnaires américains.

Certains pensent que ce rappprochement consolidera la place d'ISS sur le secteur des appliances

Quelques citations commentées

Tom Noonan, CEO de la société ISS :
"Nos clients reconnaissent de plus en plus que la sécurité doit devenir un processus plutôt qu'un empilement de technologies et de réponses à des risques isolés".

Tom Noonan : PDG d'ISS

Cette citation dévoile le futur argumentaire commercial : externalisez votre sécurité chez nous, nous maîtrisons la détection d'intrusion.

Val Rahmani, Directeur général de l'unité Infrastructure Management Services d'IBM :
"Avec la faille de sécurité évoluant très vite et les contraintes de réglementations, les grandes sociétés font de la sécurité informatique une mission prioritaire ".

Derrière le mot "réglementation", nous pouvons imaginer qu'IBM compte appuyer sa future offre de solution sécurité managée sur les contrôles imposés par la loi Sarbanes-Oxley américaine.

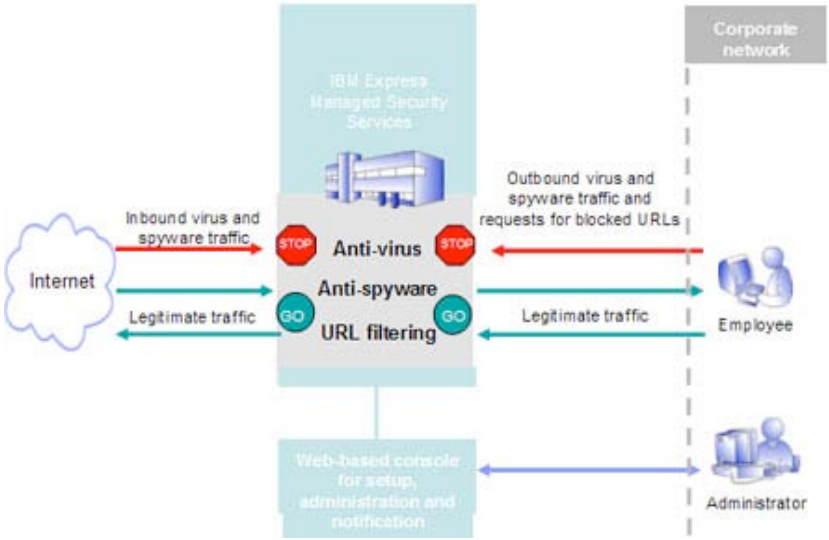
Les 3 vrais défis des MSS

Trois grands enjeux peuvent sont déjà perceptibles :

1 – Les solutions d'externalisation de la surveillance sécurité d'un réseau nécessitent qu'IBM sache former et conserver des ressources humaines compétentes en sécurité informatique.

2 – Installer des sondes et établir une liaison vers un centre de supervision à l'étranger ne suffit pas pour obtenir une solution de cyber-surveillance. Avec un fort turnover et des analyses automatisées décorrellées du contexte réel de l'entreprise, un tel service MSS n'apporte pas de valeur ajoutée.

3 – La configuration : Le prix des MSS est très attractif mais ce prix ne tient pas compte de la configuration des sondes. En effet, un système de détection d'intrusion performant nécessite une configuration adéquate et la création de signatures spécifiques aux serveurs ainsi qu'aux applications du client.



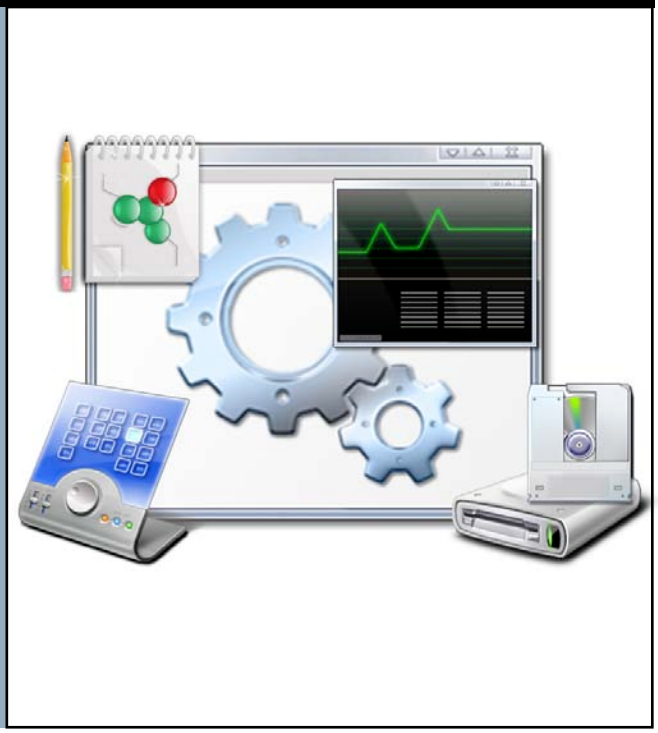
IBM devra s'assurer de répondre à ces attentes afin de devenir le leader incontesté de la sécurité des réseaux d'entreprises.

2. NOUVELLE TENDANCE :

LA CORRELATION DE LOGS.

La multiplication et la diversité des solutions de sécurité et d'administration ont conduit à l'apparition d'un nouveau problème : la gestion des logs. L'abondance et la corrélation de ces informations permettent d'optimiser les systèmes d'information et de retrouver les sources des pannes informatiques.
Cependant, ces données indispensables aux administrateurs deviennent de plus en plus nombreuses sans être forcément pertinentes. De ce fait, sans un traitement automatisé efficace, certaines alertes critiques se retrouvent inondées sous la masse de faux positifs.
Avec l'arrivée de nouveaux besoins, dont la mise en conformité avec les réglementations Sarbanes-Oxley et la Loi sur la Sécurité Financière, les responsables informatiques vont être obligés d'optimiser cette gestion.

XMCO | Partners



La journalisation

Les enjeux

Les journaux d'évènements sont des fichiers contenant des informations brutes sur les activités d'un réseau, d'un service ou d'une application. Les contenus des logs sont très variés car ils rassemblent aussi bien des opérations de fonctionnement normal que des erreurs survenues ou des tentatives d'utilisation frauduleuse.

Ces fichiers vont permettre aux administrateurs d'analyser les utilisations des différentes ressources du parc informatique afin de sécuriser, de fiabiliser et d'optimiser le système d'information. En outre, la journalisation permet d'offrir une garantie juridique lorsque la responsabilité de l'entreprise est engagée ou lorsqu'un individu malveillant s'introduit au sein de son réseau.

Les principaux enjeux de la gestion des logs sont donc :

- la validation de la politique de sécurité
- l'optimisation des coûts d'exploitation
- l'aide à la gestion des risques
- la protection juridique.

Limitations juridiques

Afin de lutter contre l'utilisation frauduleuse ou abusive des ressources informatiques, il est courant de journaliser toutes les connexions aux services et aux applications.

Il est donc important de rappeler que tous les utilisateurs doivent en être informés tout comme la durée pendant laquelle les données qui permettent d'identifier la source seront conservées.
Dans ce contexte, seule la trace de la connexion sera enregistrée, par exemple « L'utilisateur de la machine A s'est connecté à 12h00 sur la machine B pour accéder au fichier C». Aucune information sur le contenu de l'échange ne doit être sauvegardée.

Mis à part l'aspect sécuritaire, les logs peuvent être utilisés dans le but d'élaborer des statistiques. Dans ce cas, les journaux peuvent contenir des données privées (mot de passes, mails, etc.) uniquement si la source est anonyme. Le traitement de ces informations doit empêcher de retrouver le propriétaire.

En revanche la mise en œuvre d'un logiciel d'analyse des différentes logs (applicatives et systèmes), permettant de collecter des informations nominatives dans le but de contrôler l'activité des utilisateurs, est autorisée à condition d'être déclarée à la CNIL.

Les réglementations SOX et LSF

La gestion des logs constitue un point critique des recommandations Sarbanes-Oxley et de la Loi sur la Sécurité Financière. En effet, le besoin de traçabilité de ces

réglementations nécessite une parfaite maîtrise de tous les flux informatiques de l'entreprise.

De nombreuses solutions de corrélations des journaux d'évènements présentent aux administrateurs un journal préalablement traité dont les informations sont séparées et triées pour ne garder que les informations semblant essentielles. Or cette opération peut entrainer des pertes d'informations ou offrir des résultats non pertinents qui pourraient nuire à l'obtention de certaines certifications.

Pour remédier à cette problématique, il est important d'archiver, sur un support non réinscriptible, les logs « brutes » n'ayant subies aucune modification par un logiciel tiers et de les signer numériquement. Cette sauvegarde participera à la normalisation de la société ainsi qu'à sa protection juridique.

Le traitement des logs

Analyse de l'existant

Contrairement au suivi des flux applicatifs : processus parfaitement maîtrisé (voir la Figure 1), la corrélation des différentes données sensibles afin d'en ressortir une information pertinente, est une tâche beaucoup plus complexe.

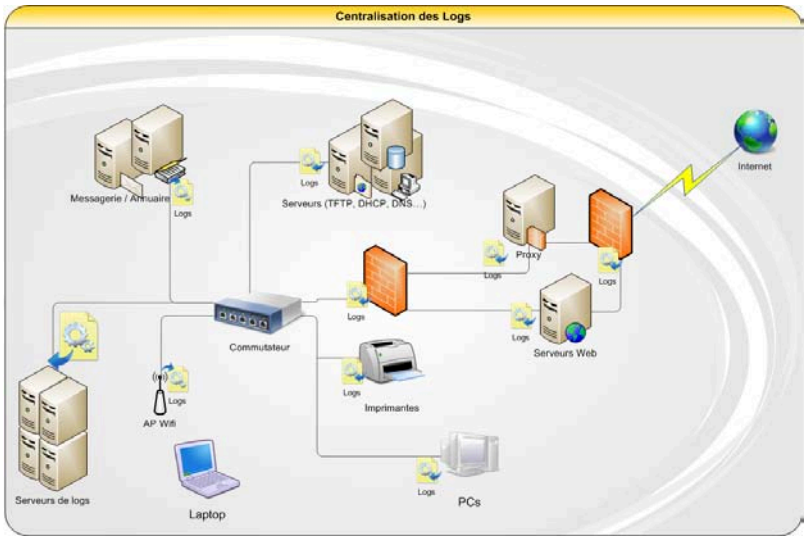


Figure 1: Centralisation des journaux d'évènements

En réponse à ce problème, de nombreuses solutions commerciales ont vu le jour. Une grande majorité des applications de centralisation et de corrélation des logs nécessite un déploiement lourd sur le périmètre informatique qui inclue l'installation d'agents sur des systèmes en production et l'ajout de machines dédiées. Les nouvelles incompatibilités logicielles et les coûts d'exploitation annexes contribuent alors à l'augmentation des risques de pannes plutôt qu'à leurs maîtrises.

Un exemple concret de solution « tout-en-un » serait celle de l'éditeur NetSecureOne : "NetSecure://LOG [3]". Les principaux avantages sont la qualité du reporting et la qualité du support en contrepartie d'une offre généraliste et d'une facturation plus onéreuse. Tous les processus d'intégration et de suivi du client sont ainsi parfaitement maîtrisés. L'éditeur propose même un forum dédié aux clients de ce produit[4]. Cependant, l'intégration de nouveaux agents au sein des différents serveurs pourrait altérer le fonctionnement global des services (voir la Figure 2).

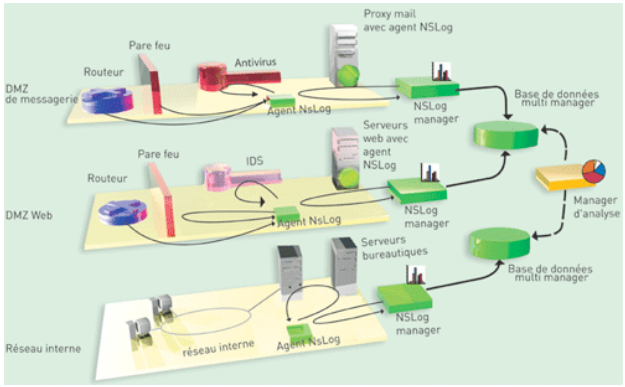


Figure 2: Déploiement de NetSecure://LOG

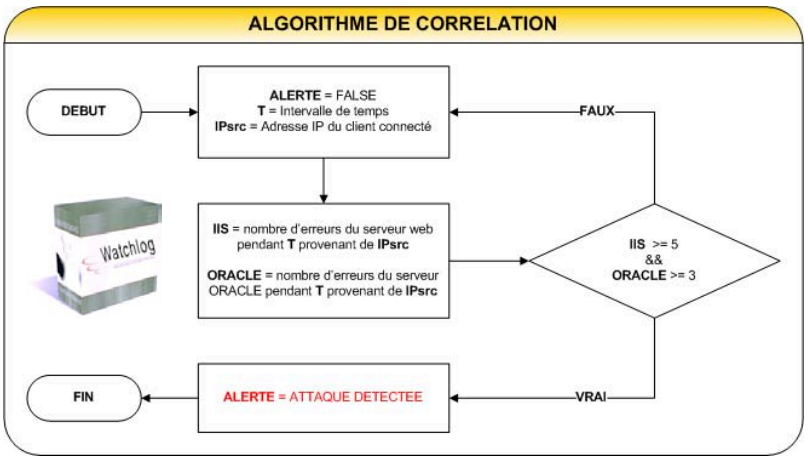
D'autre part, les grands éditeurs comme IBM et HP proposent aussi des modules de corrélations pour leurs suites d'administrations respectives TIVOLI et OPENVIEW. Ces solutions s'adressent toutefois à des administrateurs formés disposant d'une importante infrastructure et d'équipements spécifiques.

Les besoins réels

Toutes ces offres souffrent généralement d'un mode de fonctionnement statique et identique pour tous les environnements. Les particularités du parc informatique de chaque entreprise ne sont pas toujours prises en compte. Dans d'autres cas, les éditeurs fournissent des solutions « sur-mesure », cependant, le moindre changement de topologie ou de configuration peut entrainer l'inefficacité du système de corrélation.
L'aspect attractif de ses solutions repose sur la rédaction automatique des rapports contenant de jolis graphiques. Seulement, nous en oublions alors le besoin initial. L'analyse des journaux doit être réalisée par une application simple et évolutive qui permet d'identifier un évènement, sa portée et son impact.

Des logiciels qui ont une interaction avec l'outil, via un langage de haut niveau à l'instar du SQL, permettent de s'adapter à toutes les infrastructures mais demande une plus longue période d'intégration. Ainsi, n'est-il pas préférable de consacrer un peu plus de temps à la définition des réels attentes de la société plutôt qu'au déploiement d'un package « tout-en-un » dont les résultats ne seront pas ceux attendus car trop souvent aléatoires.

Voici un exemple d'algorithme illustrant le croisement des logs d'un serveur web et d'un serveur de bases de données à la suite d'une tentative d'intrusion :



La requête précédente est explicite et synthétique. Elle peut être optimisée et croisée avec d'autres informations sans être limitée par une quelconque restriction logicielle. Le principale avantage est de ne fournir une seule réponse complète et non un lot d'informations découpée et inutilisable.

Un bon compromis est, sans concession, une offre modulable et évolutive. Chaque environnement est unique, il n'existe donc pas de solution miracle. L'étude des attentes et des besoins de l'entreprise est une phase non négligeable mais il faut cependant toujours garder à l'esprit que ceux-ci peuvent évolués.

Centralisation et la corrélation de logs avec Watchlog

Centralisation des traces informatiques

Watchlog est un logiciel de centralisation des journaux d'évènements. Développé par les consultants du cabinet Xmco Partners, cet outil ne nécessite aucune installation d'agents sur les machines en production. La consolidation des logs permet de rapatrier toutes les logs d'applications brutes: serveurs web, proxy, IDS, contrôleurs de domaine, Active Directory, progiciel de gestion intégré, etc., au sein d'une base de donnée unique. En conformité avec les réglementations SOX et LSF, cet outil contribue à la certification des entreprises.

Développé en JAVA, Watchlog est compatible avec tous les environnements. Il apporte une visibilité instantanée de l'utilisation des applications du système d'information. La récupération des différents journaux est effectuée par des modules configurables qui supportent toutes les méthodes de connexions distantes (ssh, ftp, http, tftp…).

Solutions de corrélation "sur mesure"

Cette solution se différencie de la concurrence par la simplicité d'installation, de configuration et d'utilisation. Chaque implémentation est unique et l'évolution est assurée par l'ajout de nouveaux modules personnalisés. La force majeure de Watchlog est sa très grande flexibilité : l'outil s'adapte en quelques heures à toutes les applications et nous permet de construire, en collaboration avec les équipes de nos clients, un outil de corrélation et de reporting performant.

L'intégration complète de cette offre est parfois plus longue que certaines solutions industrialisées, cependant, ce laps de temps supplémentaire est indispensable pour répondre entièrement aux attentes et aux besoins de chaque infrastructure.

Mis à part les alertes et les configurations effectuées lors de l'intégration de Watchlog, tout administrateur peut ajouter et vérifier de nouvelles alarmes par le biais d'une interface simplifiée (voir la Figure 3). L'outil pourra ainsi évoluer en parallèle avec le système d'information de chaque entreprise.

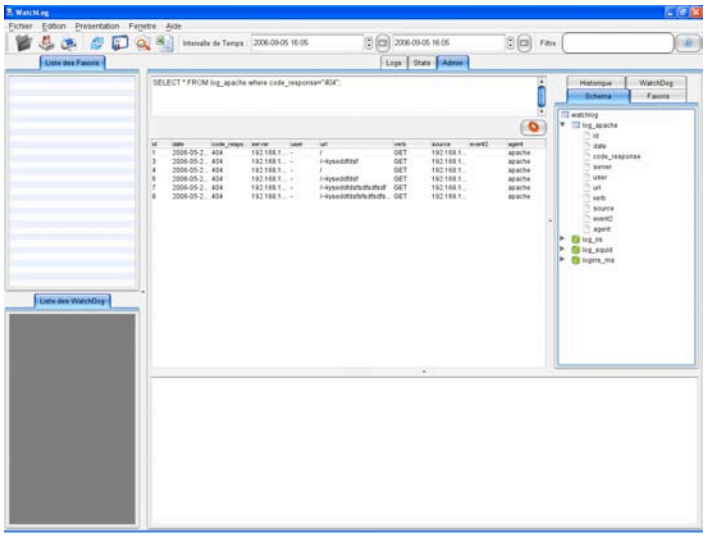


Figure 3: Capture d'écran de Watchlog

Bibliographie

[1] Sarbanes-Oxley
http://www.sarbanes-oxley.com/
Actu sécu du mois de mars:
http://www.xmcopartners.com/actu-secu/actu_secu_mars2006.pdf

[2] Loi sur la Sécurité Financière
http://www.legifrance.gouv.fr/WAspad/Visu?cid=613151&indice=1&table=JORF&ligneDeb=1

[3] NetSecure://LOG
http://www.netsecureone.com/fr/produits/gammenetsecurelog

[4] Forum Client NSLOG
http://www.netsecureone.com/fr/support/forumclientnslog

[5] Watchlog
http://www.xmcopartners.com/watchlog-fr.html

3. DOSSIER SPÉCIAL

LA BLACKHAT 2006

La Blackhat, célèbre conférence en sécurité informatique, a accueilli près de 3000 participants de tout horizon : hackers, developpeurs, consultants en sécurité durant le mois d'Août. Nous vous livrons en exclusivité les dernières nouvelles en provenance de Las Vegas…

XMCO | Partners

La BlackHat 2006

Tous les concernés par la sécurité informatique en ont forcément déjà entendu parler. La Blackhat est la conférence la plus renommée. 3000 participants : développeurs, consultants, RSSI, et les fameux hackers se réunissent dans un endroit prestigieux afin de dévoiler les dernières failles, présenter les nouvelles méthodes d'attaques et les futures technologies du marché.
Cette année, l'évènement tant attendu (et souvent craint) par les éditeurs a été organisé à Las Vegas et, pour la première fois, sponsorisé par Microsoft, Cisco et la société Ernst and Young.

De nombreux sujets ont été présentés : VoIP, sécurité Web, Vista, rootkits, forensics, Base de données. Tous les sujets et toutes les problématiques majeures auront été décortiqués par des experts.
Windows Vsta, qui devait être en proie à de nombreuses attaques, a finalement été relayé au second plan derrières les démonstrations de manipulation des puces RFID et la vulnérabilité des pilotes WIFI.

Voici les démonstrations qui ont marqué le salon.

Les pilotes Intel dans la ligne de mire des pirates

Un mac piraté en moins d'une minute

La grande attraction de cette conférence aura été, incontestablement, la présentation de Maynot, ingénieur en sécurité et d'Ellch, étudiant à l'école navale. Ces deux chercheurs, ont pu « démontrer » comment prendre le contrôle à distance d'un Mac équipée d'une carte WIFI vulnérable en moins de 60 secondes. L'exploitation ne se limiterait donc pas au Mac mais à toutes les plateformes. Le choix de la démo s'est porté sur Apple pour descendre la campagne de pub de son nouvel OS qui met principalement en avant sa sécurité.

La démonstration reste pourtant controversée puisque seule une vidéo [1] est venue appuyer leurs arguments très théoriques. De nombreux experts doutent de la véracité de cette faille et réfutent les propos des deux chercheurs. [2]

Cette faille a néanmoins ébranlé la communauté des spécialistes en sécurité informatique. N'importe quel ordinateur utilisant certaines cartes WIFI Intel et Atheros pourrait être piraté. Il faudrait seulement que la carte soit activée pour que des pirates puissent s'introduire tranquillement via un exploit sur le poste de la victime. Aucune association ou authentification à un réseau sans fil n'est nécessaire.
La vulnérabilité serait liée à des fuites de mémoire sur les pilotes chargés des connexions WIFI. La faille serait enfouie à un niveau très bas, proche du matériel ce qui ne mettrait cependant pas en cause le système d'exploitation. Les deux comparses auraient ainsi réussi à injecter un rootkit qui permettrait d'accéder aux fichiers de la machine cible [3].

Les développeurs au coeur du problème?

Les coupables seraient donc les développeurs de ces pilotes Wifi. Des accords sont souvent passés avec des sociétés spécialisées dans ce domaine (comme pour le MacBook d'Apple). Ces entreprises sont chargées de développer les pilotes pour les constructeurs. Cependant, la forte pression et les timing serrés inhérents à la commercialisation d'un produit engendreraient certaines négligences. John Ellch met en cause les procédures de tests qui ne seraient pas assez poussées ou suivies et qui laisseraient, de ce fait, des trous de sécurité évidents.

Cependant, pas de panique, personne ou presque n'est en mesure d'exploiter cette faille et les chercheurs confirment que l'exploit ne sera pas rendu public.

Plusieurs constructeurs d'équipements WIFI, comme Intel, ont donc pris au sérieux ce problème et ont publié, quelques temps après, une nouvelle version de leurs pilotes Wifi sans spécifiquement préciser pourquoi. Un rapport de cause à effet n'est certainement pas à exclure…

La sécurité des réseaux WIFI n'a donc pas finie d'être controversée. Après la remise en cause de la solidité des algorithmes de chiffrement comme le WEP (Wired Equivalent Privacy), les hackers s'aperçoivent que d'autres problèmes proviennent de niveaux encore plus bas et comme dirait Ellch surnommé Johnny Cash dans la communauté pirate : « Pourquoi bâtir une maison sur des fondations précaires ? » tout le problème repose ici…

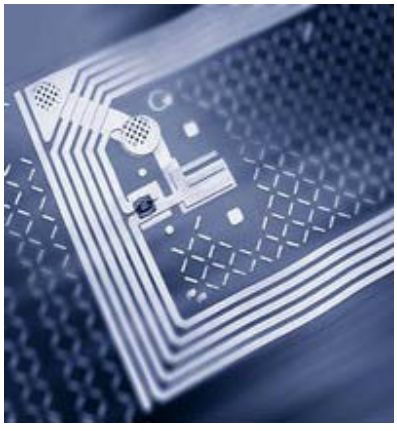
[1] Vidéo de la démonstration WIFI
http://news.com.com/1606-2_3-6101573.html?tag=ne.vid

[2] Hypothèses contre la faille WIFI
http://sid.rstack.org/blog/index.php/2006/08/26/113-du-lard-du-cochon-ou-juste-du-flan

[3] Site de Johnny Cash avec la présentation Powerpoint de son intervention à la BlackHat
http://www.802.11mercenary.net/~johnycsh/publications/

La sécurité des puces RFID remise en cause

Un autre sujet passionnant est venu enrichir les présentations de cette année. La sécurité de la technologie RFID serait remise en cause. Les passeports dotés d'une puce RFID pourraient être simplement modifiés ou, pire encore, utilisés comme des bombes et déclenchés à plusieurs mètres ! Inquiétant… ?



Qu'est ce que le RFID?

Rappelons tout d'abord le principe des ondes RFID qui envahissent peu à peu notre vie quotidienne.
Cette technologie (Radio Frequency Identification), développée il y a quelques années, est une méthode utilisée afin de récupérer, à distance, le contenu stocké dans des « Tags RFID ». Ces Tags se trouvent sous différentes formes (puces intégrées, étiquettes collées sur des produits…). Ces équipements miniatures sont dotés d'une antenne qui leur permet de recevoir et d'émettre des données.

Les passeports américains au centre des interrogations

Approuvée par le gouvernement américain, cette technologie est aujourd'hui implémentée dans la nouvelle génération de passeports. Ces "passeports intelligents" aideront à lutter contre leur vol et leur falsification. Avec une capacité de mémoire de 65 Ko, la puce pourra stocker des données, telles que le nom, la date, le lieu de naissance et une photo numérique.
Tout semble donc réuni pour lutter contre les personnes indésirables, « contrôler » les identités de manière irréfutables et donc combattre le terrorisme…

A moins que les pirates et les terroristes n'utilisent cette technologie à des fins malveillantes ? Deux problèmes majeurs ont été démontrés.

Premier problème : des passeports RFID explosifs!

Ces belles promesses annonçaient donc un principe imparable pour l'identification des personnes, ce qui est aujourd'hui réfuté par la communauté pirate…

En effet, de nombreux chercheurs se sont donc amusés à trouver les failles dont pourrait souffrir cette technologie. Le résultat est plus qu'alarmant ! Il serait possible de faire exploser un passeport équipé d'une telle puce à plusieurs mètres…Une vidéo [4] réalisée par les chercheurs a été présentée…de quoi effrayer le gouvernement américain qui a décidé de mettre en circulation ces nouveaux passeports dès le mois d'Octobre 2006.

La société Flexilis a prouvé que le scan, à distance, de puces RFID était possible. Kevin Mahaffey, représentant de Flexilis, démontre qu'avec un scanner RFID, il serait en mesure de détecter ces nouveaux passeports partiellement ouverts. Seule l'ouverture du passeport d'un angle

minimum permettrait la détection de la puce RFID. Ainsi plus un passeport est ouvert, plus le périmètre pour son identification est élevé.

En théorie, la détection pourrait être réalisée à plusieurs dizaines de centimètres mais il faudrait alors un scanner puissant.
Le vol de données n'est pas au centre des préoccupations car les informations sont chiffrées. Néanmoins, un pirate pourrait savoir si telle ou telle personne possède sur lui un passeport.
En se basant sur ce principe, ces chercheurs ont tourné une vidéo de l'explosion d'une bombe à l'aide de ces puces. [3]
Le principe est relativement simple. Un scanner est placé dans une poubelle avec une charge explosive qui sera déclenchée au moment où il détectera une puce RFID dans un périmètre défini.

Avec un peu de connaissance dans ce domaine, cette technique pourrait être utilisée par des terroristes pour la mise à feu d'une bombe. De plus, le « fingerprinting » (identification du constructeur de la puce via un scan), pourrait laisser penser que seuls les citoyens d'un pays ciblé pourraient devenir les victimes de ces attentats…

Deuxième problème : les malwares dans les tags RFID

Une autre présentation a continué à causer du tort à cette technologie. Melanie Rieback, docteur en informatique à l'université d'Amsterdam et spécialisée en RFID, a expliqué comment un virus pourrait facilement infecter une puce RFID puis se propager dans les réseaux informatiques [5].
Avec des connaissances basiques, des pirates seraient en mesure d'infecter des bases de données et de causer des dommages variés. Parmi la liste des menaces, on recense : la possibilité de causer des débordements de tampon, d'insérer du code, réaliser des injections SQL avec une modification des bases de données…
Bien que la capacité des puces soient limitées à 1024 bits, les débordements sur des systèmes « middleware » sont bel et bien possibles. En effet, certaines normes autorisent l'envoi de plusieurs blocs de données (ISO 15693) ce qui pourrait remplir un tampon alloué du système/lecteur RFID sous-jacent.

De plus, la chercheuse a créé un exemple de ver de 127 caractères seulement soit un peu moins d'un kilobit ce qui lui permet de se loger dans toutes les puces RFID. La démonstration se base sur l'injection de commandes SQL dont la preuve de concept est expliquée en annexes [7]

Plusieurs acteurs de ce secteur ont répliqué et ne considèrent pas cette menace comme effective.
Le président de l'infrastructure RFID au sein de la société Symbol affirme toujours : « Les tags RFID ne peuvent pas contenir des logiciels et des codes exécutables ce qui signifie qu'il n'est pas possible de les infecter avec des virus. De plus, les limitations du stockage restreignent considérablement les menaces. Il est impossible de créer un exécutable de 96 bits ! ». De plus, d'autres personnes confirment que les manipulations SQL ne seraient pas aussi simples à réaliser sur des lecteurs perfectionnées….
Affaire à suivre.

Troisième soucis : la réplication des données

Une dernière démonstration a été réalisée par Lukas Grunwald, ingénieur de la société DN-Systems Entreprise Internet Solutions Gmbh. La présentation vise toujours la sécurité des passeports qui utilisent les puces RFID.
Avec un équipement tout à fait banal trouvé dans le commerce, le consultant aurait été capable de copier le contenu d'un tag RFID sur une puce. Ces informations lues par le contrôle des douanes pourraient donc être « volées » et reproduites. Malgré cela, l'ingénieur allemand confirme la solidité de l'algorithme de chiffrement utilisé. Les données chiffrées peuvent être dupliquées mais en aucun cas modifiées.

Cette menace affecterait des millions d'utilisateurs dès la sortie des passeports RFID ce qui remettrait en cause l'usurpation d'identité possible…

De plus, la copie de données pourrait également être utilisée pour l'accès à des bâtiments.
Le chercheur a appliqué la même stratégie à des cartes RFID d'accès à des entreprises. Un pirate pourrait aisément s'introduire dans un bâtiment sécurisé en possédant une copie de la puce RFID d'un employé !

M.Grunwald s'était déjà fait remarquer en 2004, toujours lors d'une conférence BlackHat. Il avait alors présenté un logiciel capable de lire et de modifier les puces RFID non chiffrées. A l'origine, ce programme baptisé RFDump, a été développé dans le but de protéger les consommateurs. "Chacun devrait avoir le droit de pouvoir effacer les étiquettes RFID une fois l'achat réalisé" dit-il. Supprimer les données de ces puces permettrait de stopper toute traçabilité. Il laissait déjà entrevoir les limites de la technologie RFID qui pouvait être détournée. Ainsi les pirates pourraient modifier les informations des produits stockés dans les supermarchés. Des étiquettes RFID sont déjà utilisées au Etats-Unis. N'importe quel hacker pourrait donc modifier le prix ou changer l'identité des marchandises.

La RFID est au centre de nombreuses préoccupations. Même si l'usage de la cryptographie semble le meilleur moyen contre la modification des données, on peut imaginer qu'après plusieurs années (un passeport est valable 10 ans), cet algorithme pourra être cracké ce qui signifiera l'apparition d'actes de piratage difficilement contrôlables.

[3] **Vidéo de la démonstration de l'explosion d'une charge explosive déclenchée via une puce RFID**
http://news.com.com/1606-2_3-6103315.html

[4] **Analyse technique de la démontration par Flexilis**
http://www.flexilis.com/epassport.html

[5] **White paper de Melanie Rieback : « Is your cat infected with a computer virus ? »**
http://www.rfidvirus.org/papers/percom.06.pdf#search=%22is%20your%20cat%20infected%22

Les hackers à l'attaque de Windows Vista

Vista déjà piraté

La future sortie du système d'exploitation promet une lutte permanente de Microsoft contre les hackers. Joanna Rutkowska a démontré avec succès comment outre passer les mesures de sécurité prises introduites par Microsoft Windows Vista Beta 2 via deux attaques [7].

Microsoft utilisent des signatures pour les pilotes afin de faire savoir à l'utilisateur que ces derniers sont bien compatibles avec leur version de Windows et que tous les drivers du noyau soient valides.

La chercheuse pour une société singapourienne a réussi à contourner ce contrôle afin d'installer des pilotes non signés, chose impossible normalement avec l'apparition de l'UAC (User Account Control).
L'UAC (méthode sensée protéger le système des actions exécutées avec un compte Administrateur) détecte bien le code malicieux mais une simple confirmation de la boite de dialogue « Accepter » autorise le chargement du code au sein du noyau. L'installation de pilotes malveillants est alors possible…
Une porte est donc ouverte à tout type d'injection de code.

La seconde attaque repose sur l'utilisation d'un rootkit baptisé « Blue Pill » qui exploite la technologie de virtualisation Pacifica d'AMD pour injecter du code dans le noyau. Le programme malicieux devient alors indétectable.

Aucune vulnérabilité n'est mise en évidence, cependant, le cas de figure présenté n'a certainement pas été prévu par les développeurs.

« Le fait que le mécanisme ait été contourné ne signifie pas que Vista n'est pas sécurisé. C'est juste qu'il n'est pas aussi sécurisé qu'on nous le promet », précise-t-elle. « Il est très difficile de mettre en place un dispositif de protection du noyau fiable à 100% ».

Ce problème affecterait toutes les plateformes AMD 64 bits et pas seulement Vista. Microsoft promet de corriger prochainement ce problème en travaillant main dans la main avec les constructeurs. En attendant, Microsoft continue de proposer les dernières versions de Vista aux hackers en tout genre afin de renforcer la sécurité de son OS.

De flux RSS malicieux

Les flux RSS ont aussi fait l'objet de préoccupations diverses. Un spécialiste de sécurité de la société SPI Dynamics a montré que les fils RSS pouvaient contenir des parties de code malicieuses [8]. La popularité de cette technologie laisserait donc présager le pire.
Le but de la manipulation serait de modifier le code du flux RSS afin d'injecter un code Javascript vérolé.

L'exploitation de cette méthode nécessiterait de créer un flux malicieux et d'inciter les utilisateurs de s'y abonner. Cette première solution est peu probable (personne ne s'abonne à des flux douteux) mais il est possible d'imaginer que les attaquants essayeront de pirater les sites de grande envergure en changeant le code du flux RSS.

Fini les défacements, place au piratage silencieux !

Des actions telles que l'envoi d'informations à un serveur tiers, l'accès au poste de la victime ou des attaques de Cross Site Scripting (vol de session) seraient ensuite possibles. De plus, il faudrait également que le lecteur du flux soit également vulnérable.

Microsoft qui prévoit d'intégrer un lecteur RSS dans la version 7 d'Internet Explorer, est soucieux de ces différentes menaces. Cependant, le filtrage des codes sources afin d'éradiquer tout script malicieux et l'exécution des flux dans une zone protégée, permettent au géant de rester optimiste…mais pour combien de temps ?

[7]**"Subverting Vista kernel for fun and profit" de** Joanna Rutkowska
≈ http://blackhat.com/presentations/bh-usa-06/BH-US-06-**Rutkowska**.pdf

[8] **RSS security de Bob Auger (SPI)**
http://www.spidynamics.com/spilabs/education/presentations/**BobAuger**-RSS_Security.pdf

Les autres sujets

La valise Bluetooth

Pour terminer sur les technologies sans fils, deux chercheurs italiens ont présenté une invention assez intéressante qui permettrait de scanner les périphériques Bluetooth à plus de 200 mètres.

Plusieurs équipements Bluetooth et un ordinateur sont concentrés déns une valise. Ce projet, baptisé "Bluebag", est constituÈ d'une distribution Gentoo et de la pile bluetooth ´ Bluez '. L'ensemble peut être gérer à partir d'un équipement WIFI (ordinateur, PDA...).

Cette valise pourrait, selon les concepteurs, envoyer des vers, keyloggers ou autres logiciels malveillants. Actuellement, ce package n'est utilisé qu'en preuve de concept afin de n'envoyer que de simples fichiers. Leur expérience dans un aéroport montre que 70% des utilisateurs d'appareils, disposant de la technologie bluetooth, acceptent les transferts anonymes.
Plus d'un milliers d'équipements ont été scannés en moins de 24h dans des lieux publics (centre commercial, gare et aéroports).

Seul défaut : tous les réseaux sans fil à proximité de leur "Bluebag" ne sont plus accessibles dès que leur invention est mise en route.

Le bluebag

NAC, IPS/IDS, VoIP, Blackberry

Après ces présentations intéressantes, d'autres sujets sont venus compléter cette Blackhat.
La technologie NAC (Network Access Control), solution utilisée pour détecter la présence d'un nouveau poste et lui bloquer l'accès au réseau si son statut général de sécurité n'était pas satisfaisant, a été remise en cause. Plusieurs failles ont été montrées du doigt ce qui laisserait la possibilité à des attaquants de contourner le contrôle via l'usurpation d'identité.

David Endler et Mark Colliers se sont penchés sur la sécurité de la VoIP et ont présenté leurs outils Sipscan qui permettent de mener des actions intrusives classiques (prise d'empreinte, scans de ports, exploitation de vulnérabilité..).

L'auteur du célèbre framework Metasploit a présenté la dernière version 3.0. Il a également participé à une démonstration de contournement des outils de détection et de prévention d'intrusion (IDS/IPS).

La sécurité des infrastructures Blackberry a aussi été abordée. Felix Lindner, consultant, a démontré que les « PIN messages » entre les BlackBerry n'étaient pas chiffrés ce qui représente une menace évidente. De plus, d'autres failles, comme le compte SA/NULL installé sur la base de données SQL à chaque mise à jour et l'utilisation de logiciels libres et souvent vulnérables seraient des oints à prendre en compte lors de la configuration de l'environnement.

Enfin, parmi les autres sujets, on remarquera une présentation sur la sécurité Ajax, l'amélioration de la nouvelle pile Wifi de Vista, le bluetooth et d'autres attaques plus intéressantes les unes que les autres.

Cette année, la Blackhat aura donc tenu toutes ses promesses, avec toujours plus de démonstrations et la présentation de nombreuses vulnérabilités. Les Hackers n'ont jamais été aussi actifs. L'année 2007 s'annonce sportive, les éditeurs ont du soucis à se faire...

3. ATTAQUES MAJEURES :

TOP 5 DU MOIS DE AOÛT

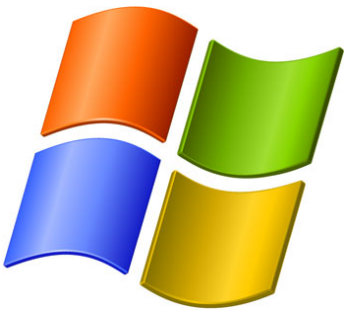
L'activité de la recherche en vulnérabilité aura été ralentie durant ce mois d'Août. Bien que Microsoft ait corrigé 12 failles affectant le système d'exploitation Windows, peu de failles critiques ont alerté notre service de veille. Certes, un exploit dangereux a affolé plus d'une entreprise, mais l'ensemble reste calme…Attendons le mois de septembre….

XMCO | Partners

Microsoft

Les failles du mois

Microsoft a publié 12 bulletins pour le mois d'Août 2006. Neuf failles « critiques » ont été corrigées. Les composants impactés sont variés : Powerpoint, Visual Basic Application, Internet Exploreur, noyau, console de management, service DNS…



La vulnérabilité la plus importante et à corriger le plus rapidement possible concerne le service « serveur », installé par défaut sur la plupart des plateformes Microsoft. En effet, ce service fournit le support de RPC : impressions et partage de ressources.
La faille provient d'une erreur de type débordement de tampon lors de la réception de certaines requêtes malformées.
Un attaquant distant pouvait exécuter du code arbitraire en envoyant des requêtes judicieusement forgées vers un système vulnérable.

Plusieurs exploits ont été publiés. Le logiciel Metasploit a d'ailleurs implémenté le module exploitant cette faille. Les plateformes Windows XP SP1 et Windows 2000 sont exposéess à une attaque qui pourrait compromettre le système vulnérable (accès à un shell distant, Bureau à distance…).

De plus, un nouveau ver extrêmement dangereux s'est propagé sur Internet et exploite toujours la faille liée au bulletin Microsoft MS06-040.
La vulnérabilité qui affectait le service "Server" sur de nombreuses plateformes aurait été savamment étudiée pour la création du ver baptisé "Cuebot", "Win32/Graweg" ou "Oscar".

Le ver recherche des ordinateurs non patchés et, une fois l'ordinateur cible infecté, il exécute un code appelé "wgareg.exe". Le programme malicieux ouvre alors le port 18067 et communique avec un serveur IRC (« forum.ednet.es"). Le pare-feu est désactivé à la suite de la modification d'une clef de registre. Une backdoor (ou porte dérobée) est également installée ce qui permettra la compromission ultérieure du système. Seules les plateformes Windows 2000 SP4 et NT4 seraient touchées par ce programme malicieux.

Les autres failles corrigées n'ont pas été très exploitées. On notera que la faille Power Point exploitée par un cheval de Troie durant le mois de Juillet a été corrigée.

On peut remarquera que l'application du correctif MS06-042 a posé quelques soucis. En effet, ce patch a introduit une nouvelle vulnérabilité au sein du navigateur web Internet Explorer 6 SP1.
La faille provient d'une erreur de dépassement de tampon lors du traitement des Urls de sites web implémentant le protocole HTTP/1.1 et la compression. Un pirate qui dispose d'un site web malicieux pourrait exécuter des commandes arbitraires en utilisant des Urls excessivement longues (supérieures à 500 octets).
Ce problème est maintenant corrigé avec la sortie de la deuxième version du correctif MS06-042.

On remarquera également l'apparition d'un programme malveillant pour la faille MS06-04. Ce cheval de Troie exploite la faille PowerPoint corrigée par Microsoft et se dissimule dans un document Word.

Plusieurs noms lui ont été attribués : W97M/ProjMod!exploit (eTrust-Vet), W32/Bgent.ZE!tr (Fortinet), Exploit-OleModule (McAfee), Exploit:Win32/Ponaml.gen (Microsoft),

Trojan.Mdropper (Symantec), TROJ_MDROPPER.BK (TrendMicro).

Le fichier infecté porte le nom de "syosetu.doc" et a une taille de 107.520 octets.

Programmes vulnérables :

- Toutes les plateformes Windows

Criticité : Elevée

Référence Xmco :

- Faille causée par l'application du correctif MS06-042 : 1156325671
- Nouvelle version du correctif MS06-042 : 1156232826
- Exploit MS06-040 : 1156146551
- Cheval de Troie pour la faille MS06-047 : 1155888925
- Ver pour la faille MS06-040 : 1155727584
- Correctif MS06-040 : 1155034370
- Correctif MS06-041 : 1155034401
- Correctif MS06-042 : 1155034434
- Correctif MS06-043 : 1155034536
- Correctif MS06-044 : 1155034558
- Correctif MS06-045 : 1155034579
- Correctif MS06-046 : 1155034599
- Correctif MS06-047 : 1155034624
- Correctif MS06-048 : 1155034643
- Correctif MS06-049 : 1155034665
- Correctif MS06-050 : 1155034685
- Correctif MS06-051 : 1155034707

Intel

Ces pilotes WIFI corrigés

Trois problèmes majeurs ont été identifés pour les pilotes WIFI. En effet, plusieurs cartes Wifi ne gèrent pas correctement certains paquets malformés. Un pirate était en mesure d'exécuter du code avec les privilèges System en envoyant des paquets spécialement conçus après avoir détecté un poste vulnérable.
Les drivers vulnérables étaient les suivants : w22n50.sys, w22n51.sys, w29n50.sys, w29n51.sys

La deuxième faille concerne le logiciel Intel® PROSet/Wireless, consacré à la gestion des connexions WIFI. La faille résulte d'un partage de mémoire non sécurisé qui permet à un attaquant local d'obtenir des informations sensibles comme la clef WEP [2].

Enfin une dernière permettait d'obtenir des privilèges élevés en injectant du code à l'aide de requêtes malformées [3].

L'ensemble de ces problèmes a été corrigé. Intel met ainsi à la disposition de ses clients les mises à jour de ses pilotes défectueux.

Programmes vulnérables :

- [1] Intel® PRO/Wireless 2200BG Network Connection
- Intel® PRO/Wireless 2915ABG Network Connection
-
- [2] Intel® PRO/Wireless 2100 Network Connection
- Intel® PRO/Wireless 2200BG Network Connection
- Intel® PRO/Wireless 2915ABG Network Connection
- Intel® PRO/Wireless 3945ABG Network Connection
- [3] Intel® PRO/Wireless 2100 Network Connection

Criticité : Elevée

Référence Xmco : n° 1142437567

GSM

Les virus pour la plateforme Symbian OS arrivent...

Les virus et les spywares en tout genre s'attaquent désormais aux téléphones portables. Plusieurs alertes nous laissent penser que le développement de ces programmes malicieux va peu à peu intéresser la communauté « underground ».
Trois malwares ont donc été identifiés. Seule la plateforme Symbian OS, système d'exploitation pour téléphones portables et PDA, est actuellement touchée.

Le premier virus se nomme "Commwarrior.Q". Ce ver se répand par MMS ou par bluetooth. Une fois installé sur l'équipement cible, il infecte les cartes mémoires insérées dans le téléphone et recherche les fichiers SYS afin de les contaminer
Ce virus se diffuse par l'échange de programmes entre utilisateurs (jeux, applications...).
L'infection est facilement identifiable, une page HTML s'affiche sur le téléphone victime de l'attaque avec le texte suivante en anglais :
"Surprise, votre téléphone est infecté par le ver CommWarrior v3.0. Ne paniquez pas, il est très intéressant d'avoir un virus sur son propre mobile. Ce vers n'effectuera aucune action malicieuse...."

Cette variante du virus est inoffensive. Cependant, il est probable que des versions malicieuses soient prochainement disponibles sur Internet.

Par ailleurs, deux autres virus viennent de naître. Ces programmes malicieux pourraient infecter une machine Windows à partir d'un téléphone et vice versa. Aucune action malicieuse ne peut être menée sur le téléphone mais des dommages conséquents pourraient avoir lieu sur la machine Windows.

Les virus se composent d'un paquet d'installation Symbian et copient un exécutable Windows malveillant sur la carte mémoire du téléphone. Ainsi lorsque cette même carte est lue a partir d'un ordinateur (connexion Bluetooth, câble ou autre), l'utilisateur pourrait exécuter le fichier dangereux qui se trouve être un cheval de Troie.

L'une des variantes nomme "Mobler" copie plusieurs fichiers malicieux sur la machine Windows (windows.exe, system.exe, Black_Symbian.SIS + Cracked By .exe) et plusieurs autres fichiers autorun.inf (fichier qui pointe vers system.exe), black.app (fichier texte), black.html (une page HTML avec un message du créateur), black.ico , black.jpg, black.txt, makesis.exe (un archiveur SIS).

Enfin, certains laboratoires de recherche antivirale comme F-Secure ont relevé une recrudescence de petites applications présentées comme légitimes mais qui joueraient le rôle d'espions. Certaines sociétés qui développent ce genre de produits, ciblent, soit disant, les mères de famille susceptibles de contrôler les appels et les messages de leur fils ou encore les utilisateurs désirant garder une trace de l'utilisation de leur téléphone.

Méfiez-vous de toutes ces applications qui, espérons-le, n'envahiront pas nos téléphones d'ici quelques temps…

Programmes vulnérables :

- Symbian OS

Criticité : Elevée

Référence Xmco :

- n° 1155737213
- n°1155798989
- n°1154505385
- n°1157033624

Symantec

Vulnérabilités dans les produits Veritas Backup et NetBackup Pure Disk

Deux vulnérabilités pour des produits Symantec ont été corrigées.

La première faille a été découverte et corrigée au sein du produit Symantec VERITAS Backup Exec. Elle provient d'une erreur de type débordement de pile mémoire au sein des interfaces RPC. En exploitant la vulnérabilité, un attaquant pouvait exécuter du code arbitraire ou causer un déni de service.

Une seconde vulnérabilité a été identifiée dans Symantec Veritas NetBackup PureDisk Remote Office Edition. Cette dernière résulte d'une erreur inconnue au sein de l'interface de gestion. L'exploitation de celle-ci permettrait à une personne malveillante de contourner la procédure d'authentification et d'accéder à un serveur en disposant de privilèges élevés.

Programmes vulnérables :

- Symantec Veritas NetBackup PureDisk Remote Office Edition (toutes plateformes) version 6.0 GA MP1
- Symantec Backup Exec CPS Remote Agent 10.x
- VERITAS Backup Exec 10.x
- VERITAS Backup Exec 9.x
- VERITAS Backup Exec Remote Agent 10.x for Windows Servers
- VERITAS Backup Exec Remote Agent 9.x for Windows Servers

Criticité : Elevée

Référence Xmco :

- n° 1155737213
- n° 1155798989

5. OUTILS LIBRES :

FOCUS SUR 5 PRODUITS LIBRES

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

Ce mois-ci, nous avons choisi d'analyser des logiciels Internet, deux programmes antispyware et antirootkit et un scanner de vulnérabilités :

- *Internet Explorer 7 : cette nouvelle mouture semble très intéressante*
- *Outil de suppression de logiciels malveillants de Microsoft*
- *Blacklight : antirootkit développé par F-Secure*
- *Writely : une petite application développée par Google*
- *Nessus : un scanner de vulnérabilités*

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

XMCO | Partners

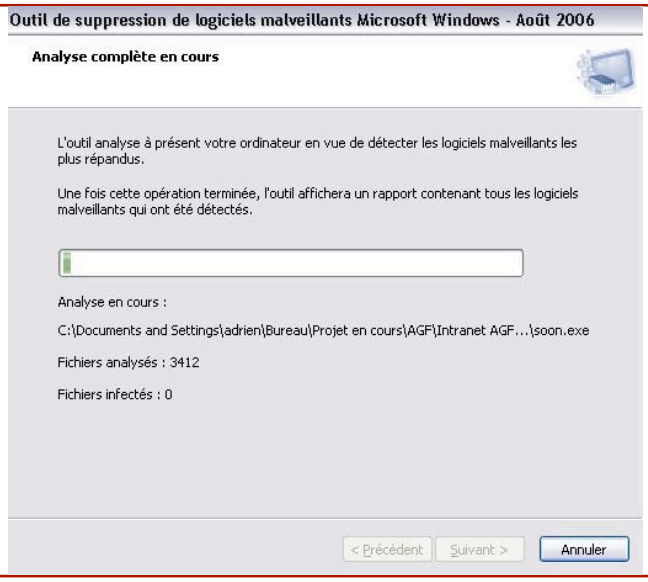
Internet Explorer 7

Navigateur web

Version actuelle	Internet Explorer 7 Release Candidat
Utilité	★★★★★
Type	Navigateur Web
Description	Microsoft a publié une première version « Release Candidate » de la nouvelle édition de son navigateur Internet Explorer. Le code source entre donc dans sa phase finale. L'éditeur a épuré au maximum l'interface afin de ne laisser que la barre d'adresse et les fonctions essentielles. Les principales innovations proviennent de l'ajout d'un lecteur de flux RSS, d'une gestion des onglets (tous deux déjà présents au sein des navigateurs concurrents) et d'un système de protection contre le phishing. Microsoft annonce également des performances et une stabilité accrues.
Capture d'écran	
Téléchargement	Internet Explorer 7 RC1 : http://www.microsoft.com/windows/ie/downloads/default.mspx
Sécurité de l'outil	Quelques preuves de concept ont été publiées et permettent de causer des dénis de service sur le navigateur. L'outil étant encore en phase de développement, ces failles devraient d'être corrigées.
Avis XMCO	Devant la publication massive de vulnérabilités durant le mois de juillet (http://browserfun.blogspot.com/), la version 6 d'Internet Explorer commence à montrer des signes de fin de vie. Microsoft a annoncé que la sécurité de sa nouvelle mouture est accrue tout en élevant le degré de compatibilités applicatives.Ceci devrait supprimer un bon de nombre de sources de problèmes.

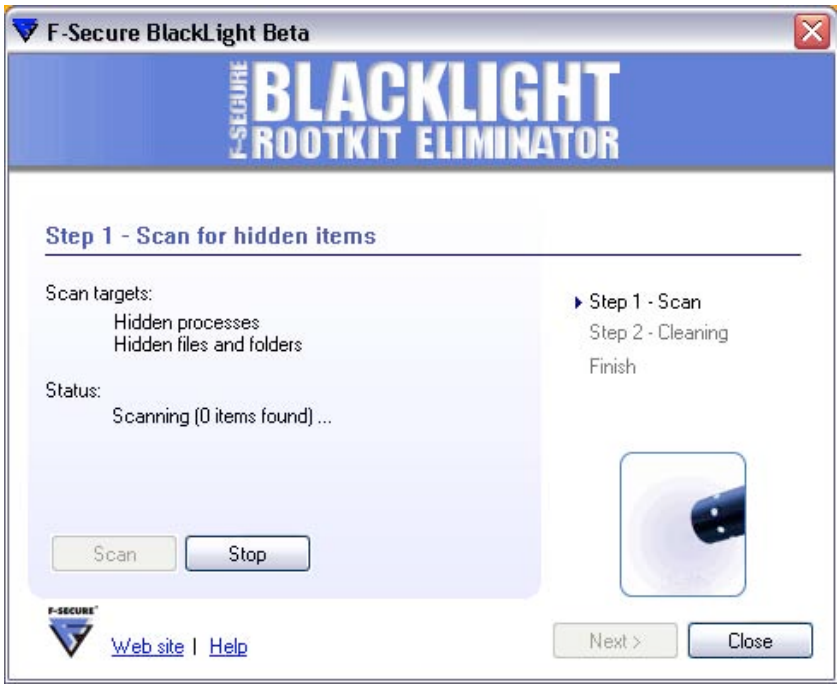
Outil de suppression de logiciels malveillants

Anti-spyware

Version actuelle	V1.19
Utilité	
Type	Logiciel de détection de programmes malveillants
Description	Après la sortie de Windows Defender, Microsoft a choisi de développer un logiciel de détection des programmes malveillants. Il identifie les programmes malicieux comme Sasser, Blaster, Mydoom et les supprime immédiatement. Cet outil se présente sous la forme d'un exécutable. Tous les deuxièmes mardi du mois, Microsoft publie une nouvelle version de cet outil à l'adresse citée ci-dessous.
Capture d'écran	
Téléchargement	Utilisable sur les plateformes Windows 2000, 2003 et XP, ce logiciel est disponible à l'adresse suivante : http://www.microsoft.com/downloads/details.aspx?FamilyId=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=fr
Sécurité de l'outil	Aucune faille n'a été répertoriée depuis la première publication du logiciel.
Avis XMCO	Cet outil est le complément parfait des antivirus classiques. Il ne se charge pas d'identifier les spyware (contrairement à Spybot Search and Destroy présenté dans le précédent numéro d'Actu Sécu) mais éradique les menaces les plus dangereuses. Aucune installation n'est nécessaire ce qui simplifie son utilisation.

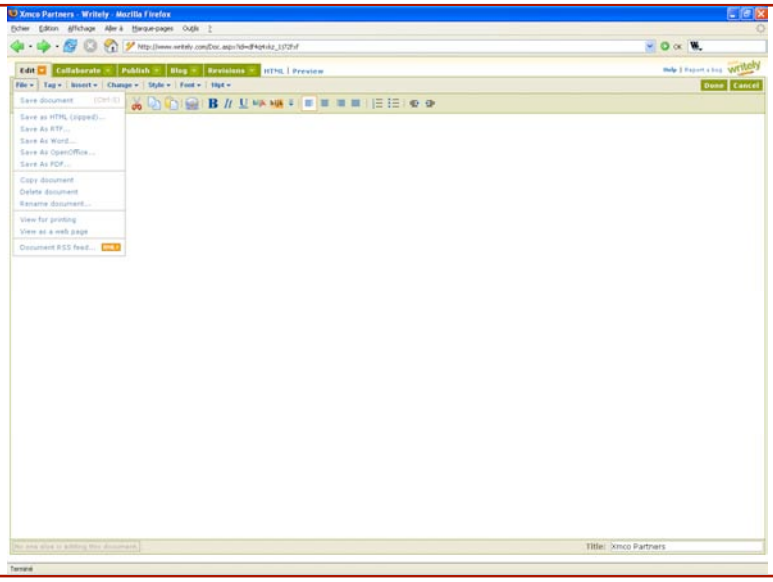
F-Secure Blacklight

Anti-rootkit

Version actuelle	Blacklight Beta
Utilité	
Type	Programme de suppression de rootkits
Description	Blacklight est le dernier petit programme gratuit conçu par le laboratoire de F-Secure. Cet outil se présente sous la forme d'un exécutable. Il examine le système à un niveau bas et détecte les logiciels malveillants et rootkits cachés.
Capture d'écran	
Téléchargement	Blacklight est disponible gratuitement sur le site de F-Secure à l'adresse suivante : http://www.f-secure.com/blacklight/try_blacklight.html
Sécurité de l'outil	Aucune faille n'a été répertoriée depuis la première publication du logiciel.
Avis XMCO	Cet outil est un excellent programme. Il élimine les menaces persistantes et non détectées par les antivirus classiques. Il est fortement recommandé d'utiliser ce genre de produits en complément de son antivirus.

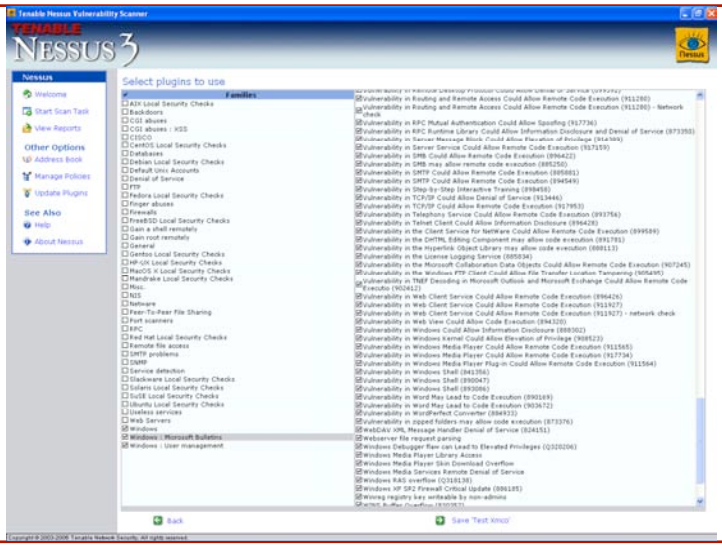
Writely

Traitement de texte en ligne

Version actuelle	Writely beta
Utilité	
Type	Logiciel de traitement de texte en ligne
Description	Writely est un outil de traitement de texte totalement en ligne publié par le GOOGLE. Cette application « web 2.0 » basé sur AJAX et XML bénéficie de toutes les options indispensables présentes au sein des logiciels concurrents telles que l'insertion de tableaux et d'images, l'enregistrement du fichier dans plusieurs formats (word, openoffice, pdf, html) ou encore la possibilité de partager un document. Cette version bêta devrait remplir toutes les attentes de la plupart des utilisateurs.
Capture d'écran	
Téléchargement	Ce logiciel ne nécessite aucun téléchargement. Il est accessible directement depuis l'URL suivante http://www.writely.com
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Writely est une bonne solution de traitement de texte de secours cependant le produit possède une grosse faiblesse. Cette dernière est liée au manque de confidentialité. Tous les échanges entre le navigateur web et l'outil en ligne s'effectuent en clair. Le contenu du document peut ainsi être récupéré aisément. Puisque la version actuelle est une « bêta », nous espérons que l'une des prochaines évolutions de l'outil en ligne sera l'implémentation du protocole HTTPS.

Nessus

Scanner de vulnérabilités

Version actuelle	Nessus 3.0.3
Utilité	
Type	Scanner de vulnérabilités
Description	Nessus est un scanner de vulnérabilités qui permet d'auditer de multiples plateformes. Simple à utiliser et à installer, il permet de scanner de nombreuses machines simultanément. Nessus comprend 2 composants : - une partie serveur permettant de stocker des profils d'analyses (adresses IP, ports, comptes d'utilisateurs, etc.) et les différents plugins : chacun d'eux représentant une vulnérabilité potentielle ; - une partie cliente consacrée au lancement des scans. Chaque script est écrit en NASL Ceci permet de développer ses propres modules de vulnérabilités rapidement. A la suite des scans, l'outil permet de générer des rapports, sous différents formats, décrivant les différentes failles suspectées ainsi que des propositions de corrections.
Capture d'écran	
Téléchargement	Nessus est téléchargeable gratuitement pour les plateformes Linux, Mac OS X, Windows, Saloris et FreeBSD: http://www.nessus.org/download/
Sécurité de l'outil	Peu de vulnérabilités ont été découvertes. http://secunia.com/product/1397/
Avis XMCO	Nessus est un outil évolutif et performant. Utilisé par les administrateurs, celui-ci permettra de lister toutes les machines vulnérables à certaines failles précises. Il pourra fournir, par exemple, la liste des machines ne disposant pas des derniers correctifs publiés. Couplé au langage de script NASL, Nessus est un logiciel d'administration complet et évolutif. Cependant, comme tout scanner automatique. Il peut retourner de nombreux faux-positifs et ne remplacera jamais un véritable audit.

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents.

Nom	Dernière version	Date	Lien
Debian Sarge	Version stable 3.1 r2	19/04/2006	http://www.debian.org/CD/netinst/
Snort	2.6.0.1	20/08/2006	http://www.snort.org/dl/
MySQL	5.0.24		http://dev.mysql.com/downloads/mysql/5.0.html
	5.1.11-Bêta		http://dev.mysql.com/downloads/mysql/5.1.html
Apache	2.2.3		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.11	01/04/2005	http://www.insecure.org/nmap/download.html
Firefox	2 beta 2	06/2006	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	1.5.0.5	06/2006	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.1.5	30/08/2006	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.58		http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV	0.88.4	07/08/2006	http://www.clamav.net/stable.php#pagestart
Ubuntu	6.06 Drapper Drake	06/2006	http://www.ubuntu-fr.org/telechargement
Postfix	2.3	06/06/2006	ftp://ftp.club-internet.fr/pub/mirrors/ftp.porcupine.org/postfix-release/index.html
Squid	2.6	29/05/2006	http://www.squid-cache.org/Versions/v2/2.5/
Filezilla	2.2.27		http://filezilla.sourceforge.net/
OpenSSH	4.3	01/02/2006	http://www.openssh.com/
Search and Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
GnuPG	1.4.5	06/2006	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.2a		http://www.truecrypt.org/downloads.php

Nom	Dernière version	Date	Lien
Back-Track	V1		http://www.remote-exploit.org/index.php/BackTrack_Downloads
MBSA	2.0	20/08/2006	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1,7		http://www.sysinternal.com/Utilities/PsExec.html
Helios	3.1.10a	6/10/2003	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.01		http://www.opera.com/download/