Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE
HORS SERIE
Hors série N°001 - Prix : 7 € - mai 2008

SPECIAL

Black Hat
BRIEFINGS AND TRAINING
www.blackhat.com

INTERVIEW EXCLUSIVE
Jean-Marc Thoumelin

TREND MICRO 20 1988-2008 ANNIVERSARY

Promisec vous offre un audit gratuit de sécurité interne!

PROMISEC. CLIENTLESS ENDPOINT SECURITY MANAGEMENT.

Mesurez le niveau de conformité de vos politiques de sécurité en détectant les menaces et violations de politique de sécurité présentes sur vos postes et ayant pour origine votre réseau interne :

Promisec vous offre un audit gratuit réalisé à partir de ses solutions sans agents de management de la sécurité des postes clients et serveurs.

Pour en savoir plus et réserver votre audit, contactez un partenaire Promisec participant à l'opération :

Cyber Networks	Nes Conseil	NSIT	Vipawan
01 42 04 95 95	01 53 38 57 00	01 48 78 99 00	01 58 59 39 39
info@cyber-networks.fr	**info@nes.fr**	**info@nsit.fr**	**info@vipawan.fr**

PROMISEC
Securing The Internal Network

www.promisec.com

POENTA

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

Black Hat
BRIEFINGS AND TRAINING
www.blackhat.com

Hors série mai 2008
spécial **BLACK HAT**

REVUE TRIMESTRIELLE
Hors Série N°1 Spécial Black Hat 2008
www.globalsecuritymag.fr et
www.globalsecuritymag.com
ISSN : 1959 - 7061
Dépôt légal : à parution
Editée par SIMP
RCS Nanterre 339 849 648
17 avenue Marcelin Berthelot
92320 Châtillon
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : marc.jacob@globalsecuritymag.com

RÉDACTION
Directeur de la Publication :
Marc Brami
Rédacteur en chef :
Marc Jacob
Ont collaboré à ce numéro :
Emmanuelle Lamandé, Jean Baron,
Jean-Marc Grémy, Adrien Guinault,
Igor Herrmann, Philippe Humeau,
Thibault Koechlin, Jérémy
Lebourdais, Benjamin Tréheux
Assistante :
Sylvie Levy
Responsable technique :
Raquel Ouakil
Photos
Norbert Martiano, Marc Jacob
Comité scientifique :
Pierre Bagot, Francis Bruckmann
Eric Doyen, François Guillot
Mauro Israël, Olivier Iteanu,
Dominique Jouniot
Patrick Langrand, Yves Maquet
Thierry Ramard, Hervé Schauer
Wayne Sutton, Catherine Gabay
Zbigniew Kostur

PUBLICITE
SIM Publicité
Tél. : +33 1 40 92 05 55
Fax. : +33 1 46 56 20 91
e-mail : ipsimp@free.fr

PAO
Imadjinn sarl
Tél. : 09 75 45 71 65
e-mail : info@imadjinn.fr

IMPRESSION
Imprimerie Hauguel
8-14 villa Léger
92240 Malakoff
Tél. 01 41 17 44 00
Fax 01 41 17 44 09
e-mail : info@imprimerie-hauguel.fr

ABONNEMENT
Prix du Hors Série :
7 € TTC (TVA 19,60%)
Prix au numéro :
18 € TTC (TVA 19,60%)
Abonnement annuel :
50 € TTC (TVA 19,60%)

ÉDITO

La Black Hat est devenue au fil du temps une institution et son étape Européenne aussi. Toujours à Amsterdam, cette 8ème édition a réuni 43 nationalités, 450 participants, des sponsors fidèles et toujours autant d'effervescence. Elle a connu, aux dires de nos experts, moins de temps forts que les précédentes éditions. Pourtant, ils ont su en tirer la substantifique moelle que vous trouverez dans ce premier hors série. Comme l'a montré le Professeur Angell, lors de la keynote d'ouverture, citant le président Pompidou : « il y a trois manières d'arriver à la ruine la plus complète : la plus douce… les femmes, la plus rapide, le jeu et la plus certaine, la technologie ». Il semble qu'encore une fois, devant les actes de piraterie informatique, la technologie trouve ses limites, même si elle reste toujours indispensable. Il est donc plus que jamais recommandé d'informer et de former les utilisateurs.

Marc Jacob

Interview exclusive : Jean-Marc Thoumelin **TREND MICRO** **P. 13**

SOMMAIRE

N'AYEZ PAS UNE CONFIANCE AVEUGLE EN VOS ANTIVIRUS

Par Jérémy Lebourdais*,Groupe ON-X ▶

** Jérémy tient à remercier l'OSSIR qui lui a permis d'assister à la BlackHat.*

L'objectif de la présentation de Feng Xue n'était pas de juger de l'utilité des antivirus, mais de montrer que des vulnérabilités existent et peuvent être trouvées assez simplement, notamment à l'aide du fuzzing. Il a aussi souhaité attirer l'attention sur l'excès de confiance dans les antivirus, trop souvent perçus comme sûrs.
Cette présentation rappelle aussi que les antivirus ne sont qu'une ligne de défense, parmi un ensemble de moyens de sécurité. Comment se protéger d'un code malveillant si le seul moyen de détection est un antivirus et que celui-ci est compromis ?
Ainsi, Feng Xue a cité l'exemple : « d'un RSSI qui s'interrogeait sur le trafic important émis par son serveur de mail, pourtant à jour, et imaginait un 0day dans Exchange alors que c'était l'antivirus qui avait été compromis… »

Les antivirus sont connus et utilisés sur la majorité des SI actuels, que ce soit sur les serveurs mails ou sur les postes de travail. Qui n'a jamais recommandé à ses utilisateurs de contrôler à l'aide d'un antivirus les fichiers suspects ? Mais attention à ne pas tirer de conclusion hâtive : « l'antivirus ne détecte rien donc je ne risque rien ». C'est cette idée de bouclier invulnérable, remise en cause ces derniers temps, que Xue a voulu démystifier, en démontrant lors de sa présentation que les antivirus sont des logiciels comme les autres donc avec leurs vulnérabilités.

Le nombre de vulnérabilités des antivirus est passé de 9 à 60 en 3 ans

Le nombre de vulnérabilités découvertes dans les antivirus a considérablement augmenté ces quatre dernières années, passant de 9 en 2004 à 60 en 2007 (selon la National Vulnerability Database). Pourquoi cet engouement pour la recherche de faille dans les antivirus ? Un grand nombre d'utilisateurs (une majorité ?) ont trop confiance dans leur antivirus, et si ce dernier détermine un fichier comme sain, il est très généralement considéré comme tel par l'utilisateur. De plus, comme les systèmes d'exploitation sont de plus en plus sûrs, les attaquants déplacent leurs recherches sur les applications et donc les antivirus.

De surcroît, les antivirus doivent analyser, et donc « comprendre » plusieurs milliers de formats de fichiers (exécutables, documents, archives, fichiers multimédias, etc) ce qui les rend plus sensibles aux erreurs d'implémentations car chaque format a ses spécificités. Un exemple pourrait être une archive ZIP, déclarée comme malformée par l'antivirus, donc non utilisable, alors que le logiciel de décompression la lit sans problème.

Partant de ce constat et du peu d'études publiées sur le sujet, Feng Xue a présenté différentes démarches et axes de recherches de vulnérabilités dans les antivirus dans le but de sensibiliser les personnes présentes.
Xue a classé les vulnérabilités dans les antivirus en quatre catégories :
- Vulnérabilités d'implémentations dans le système,
- Vulnérabilités de conception ou de programmation des composants ActiveX,
- Vulnérabilités dans le moteur en lui-même,
- Vulnérabilités dans la gestion et l'administration de l'antivirus.

Sa présentation était en deux parties : la démarche et les outils d'audit pour chaque catégorie de vulnérabilité, puis des exemples d'exploitation de chacune.

Vulnérabilités d'implémentations dans le système lorsque les fichiers des antivirus sont trop permissifs

Cette catégorie regroupe les droits trop permissifs sur les fichiers de l'antivirus ou les services, ainsi que les drivers IOCTL. L'audit des droits peut se faire manuellement ou à l'aide d'outils tels que AccesEnum, l'objectif étant de modifier des fichiers ou services de l'antivirus afin d'obtenir un accès en tant que SYSYTEM.
La recherche de vulnérabilités dans les drivers IOCTL s'effectuant par fuzzing, à l'aide d'outils tels qu'ioctlizer ou Kartoffel.
La plupart des antivirus ont eu des vulnérabilités de ce type, notamment sur les droits par défaut des fichiers installés.

Vulnérabilités de conception ou de programmation des composants ActiveX

Les composants ActiveX sont généralement installés par les antivirus afin de contrôler et d'effectuer des opérations sur le système, telles que les mises à jour des signatures, ou bien lors des contrôles à distance offerts par de nombreux éditeurs sur leur site. De même que pour les drivers, la méthode proposée est le fuzzing et l'analyse manuelle.
Plusieurs vulnérabilités ont été citées en exemple, dont une de l'éditeur Kaspersky permettant à un attaquant d'envoyer n'importe quel fichier sur le serveur FTP de son choix !

Vulnérabilités dans le moteur antivirus : le fuzzing, une technique de test en pleine essor

Trois méthodes de recherche ont été présentées : l'analyse de code source, lorsque c'est possible, le « reverse engineering » et le fuzzing. Les deux premières nécessitent du temps et sont plus complexes que le fuzzing, technique de test en plein essor ces dernières années. Cependant, bien que de nombreux fuzzers existent pour tester différents types d'applications (serveurs Web, lecteurs multimédias, etc), seul vxfuzz existe pour tester les antivirus. Xue a donc expliqué quels étaient les principaux éléments nécessaires afin de réaliser ses propres tests, un fuzzer pour antivirus n'étant en partie qu'un générateur de fichiers. C'est cette technique qui a été privilégiée lors de ses tests et a permis de trouver plusieurs vulnérabilités dans différents moteurs, démonstration à l'appui.
De nombreuses vulnérabilités ont été trouvées dans les moteurs ces dernières années avec pour impact d'exécuter du code arbitraire avec les droits de l'antivirus, du déni de service ou l'absence de détection du code malveillant.
Il faut souligner que cette catégorie de vulnérabilité peut être exploitée sur un poste de travail, mais aussi sur un serveur mail, avec les conséquences que l'on imagine. Des attaques réussies de ce type ont déjà été réalisées comme il l'a démontré lors de sa présentation.

Vulnérabilités dans la gestion et l'administration des antivirus

L'administration à distance des antivirus est généralement basée sur un fonctionnement en mode client/serveur avec l'utilisation d'un protocole propriétaire. La recherche de vulnérabilités dans ces composants demande donc plus de temps et l'utilisation d'un fuzzer est encore une fois recommandée par Xue.
Plusieurs vulnérabilités ont été trouvées dans les composants d'administration des antivirus, mais aussi dans la gestion des licences, comme l'exemple des 6 vulnérabilités découvertes par iDefense Labs en 2005 dans le logiciel de licence de CA. ■■■

PHISHING ET STRATÉGIE DE SÉCURITÉ

Par Benjamin Tréheux, HSC ▶

Après une courte présentation des attaques de type phishing, Angelo P.E. Rosiello établit un panorama des types de protection existants et finalise son intervention par la présentation d'une solution de protection expérimentale orientée client (DOMAntiPhish) développée en collaboration avec Engin Kirda, Christopher Kruegel et Fabrizio Ferrandi.

Selon les statistiques du groupe de travail Anti-Phishing (APWG - http://www.antiphishing.org/), les attaques de type phishing ciblent majoritairement les institutions financières (96,9% des attaques recensées en Mai 2007). Sur cette même période, les statistiques évoquent 149 marques détournées pour mener des campagnes de phishing, une durée moyenne d'accessibilité des sites malveillants de 3,8 jours et placent les Etats-Unis en tête des pays hébergeant le plus grand nombre de ces sites.

Ces derniers mois, les attaques par phishing sont devenues de plus en plus efficaces et complexes à suivre. Récemment, des pages de phishing hébergées sur les sites de certains gouvernements ont été détectées. En juin 2007 par exemple, de telles pages ont pu être identifiées sur les sites des gouvernements de Thaïlande, d'Indonésie, de Hongrie, du Bangladesh, d'Argentine, du Sri Lanka, d'Ukraine, de Chine, du Brésil, de Bosnie, de Colombie et de Malaisie. Ces sites présentent un certain nombre d'avantages pour un phisher, notamment parce qu'ils génèrent un trafic très important masquant l'activité supplémentaire induite par le site de phishing. Ceci assure donc une détection moins rapide et un temps d'accessibilité au site supérieur. De plus, l'URL du site comportant le domaine d'un gouvernement induit un sentiment d'authenticité auprès des utilisateurs.

Toujours plus de spoofing, d'ingénierie sociale et d'exploitation des vulnérabilités des navigateurs…

Les attaques de type phishing peuvent être classées selon leur nature. Tout d'abord, les e-mails spoofés envoyés en masse aux victimes et leur demandant en général de mettre à jour le mot de passe ou les données de leur compte. La seconde forme d'attaque utilise les messageries instantanées de type MSN, ICQ, AOL, IRC… Ces canaux de communication permettent une diffusion rapide de l'information et sont aussi un moyen de collecter des informations sensibles auprès des victimes avec des techniques d'ingénierie sociale. La troisième forme d'attaque s'appuie sur le téléphone et utilise les mêmes techniques. Enfin, l'exploitation de vulnérabilités dans les navigateurs reste un bon moyen pour rediriger les utilisateurs vers des sites malveillants et collecter des informations sensibles.

Pour ne pas éveiller les soupçons de la victime, l'attaquant utilise un certain nombre d'astuces. La première consiste à inclure les liens du site original dans les pages du site malveillant, afin que les utilisateurs naviguent principalement sur le site officiel et n'effectuent qu'un nombre limité de requêtes sur le site falsifié. L'attaquant utilise également l'encodage et l'obfuscation d'URL afin de ne pas paraître suspicieux. Les malwares peuvent aussi être utilisés afin d'installer, par exemple, des BHO (Browser Helper Object) malveillants. Les BHO sont des DLL permettant aux développeurs (et aux attaquants) de personnaliser et contrôler Internet Explorer. Enfin, l'attaquant peut tenter de corrompre le fichier "hosts" de la machine de la victime. Ce fichier permet de mettre en correspondance des noms DNS et des adresses IP. Ce fichier étant généralement consulté en premier lieu lors du processus de résolution de noms DNS, l'attaquant cherche en général à faire correspondre un nom officiel à une adresse IP sous son contrôle. L'utilisateur établissant alors une connexion sur ce site légitime se connecte en réalité au site malveillant.

Des solutions de protection existent

Les solutions de protection contre les attaques de type phishing peuvent être mises en œuvre côté serveur ou côté client. Les solutions côté serveur sont généralement implémentées par les fournisseurs de services

(FAI, institutions financières...) et peuvent prendre plusieurs formes :
- Suivi de marque : exploration de site en ligne pour identifier des clones (en recherchant des marques légitimes). Les sites suspects sont alors ajoutés à une liste noire centralisée ;
- Détection de comportement : définition d'un profil pour chaque client (après une période d'observation) puis détection des anomalies par rapport à ce profil ;
- Suivi des événements de sécurité : analyse et corrélation des événements de sécurité pour identifier des activités anormales ;
- Authentification forte.

Les solutions côté client sont généralement développées sous forme d'extensions ou intégrées aux navigateurs Web et clients de messagerie. Ces solutions sont de plusieurs types :
- Analyse d'e-mail : utilisation de filtres et analyse de contenu ;
- Listes noires : utilisation de collections d'URL identifiées comme malveillantes. Ces listes sont interrogées par le navigateur à chaque chargement de page ;
- Flux d'informations : solutions basées sur le fait qu'un utilisateur peut être facilement trompé par l'obfuscation d'une URL ou par un faux nom de domaine, alors qu'un programme ne l'est pas (dans l'absolu) ;
- Similitudes de mise en page : techniques tentant de distinguer une page malveillante d'une page légitime en comparant leurs similitudes visuelles.
La suite de la conférence d'Angelo P. E. Rosiello se focalise sur les trois derniers types de solutions côté client.
La majeure partie des navigateurs du marché comporte désormais une solution anti-phishing, souvent basée sur le concept de liste noire. Des études ont notamment été menées par Microsoft et la fondation Mozilla pour mesurer l'efficacité de ces différentes solutions. Les résultats peuvent cependant être remis en cause, les commanditaires de ces études étant à la fois juges et parties. Pour les besoins de sa conférence, Angelo P. E. Rosiello s'appuie donc sur une évaluation indépendante réalisée par le laboratoire en sécurité de l'Université Technique de Vienne. Durant trois semaines, ce laboratoire a collecté 10 000 URL pour tester les listes noires de Microsoft et de Google.
L'étude basée sur trois indicateurs a montré que la liste noire de Google était meilleure que celle de Microsoft. Les trois indicateurs utilisés étaient les suivants :
- Couverture : pourcentage d'URL de phishing déjà incluses dans la liste ;
- Qualité : pourcentage d'URL légitimes incorrectement incluses dans la liste ;
- Temps de réponse moyen : temps moyen nécessaire pour insérer les URL non initialement incluses dans la liste.

Angelo P. E. Rosiello a présenté ensuite une autre technique anti-phishing : l'analyse de page statique. L'Université Technique de Vienne a démontré qu'un groupe de propriétés d'une page permettait actuellement de différencier si elle était malveillante (phishing) ou non. Le mode opératoire utilisé est le suivant :
- Sélection de 18 propriétés directement extraite du code HTML d'une page (ex. : formulaires, champs de saisie, liens, balise script...) ;
- Collecte d'un ensemble de pages (légitimes ou de phishing) à analyser pour extraire un modèle de classification (arbre de décision) ;
- Extraction du modèle de classification par exécution d'un algorithme ;
- Utilisation d'un outil automatique se basant sur le modèle de classification extrait pour distinguer les pages légitimes des pages malveillantes.

L'arbre de décision est extrait en utilisant l'outil Weka (algorithme J48) sur un ensemble de 4829 pages Web. Les tests effectués ont permis de détecter 80% des pages malveillantes avec un nombre de faux positifs relativement faible.

Le dernier type de solutions présenté repose sur l'analyse du flux d'informations. L'objectif est de protéger les utilisateurs en vérifiant où les informations sensibles qu'il saisit sont envoyées. Peu de solutions basées sur ce concept ont été implémentées. AntiPhish en est une, développée sous forme d'extension pour Firefox par Engin Kirda et Christopher Kruegel. Le mode de fonctionnement de cet outil est le suivant :
- L'utilisateur décide des informations qu'il souhaite protéger contre les attaques de type phishing. L'outil les met en cache et y associe le domaine sur lequel elles ont été utilisées ;
- Les interactions de l'utilisateur dans son navigateur (touche pressée, soumission de formulaire, clic de souris...) sont interceptées avant d'être envoyées au site ;
- L'outil vérifie si les informations entrées sont dans la liste de surveillance définie par l'utilisateur;
- Si c'est le cas, l'outil vérifie que le domaine associé à ces informations dans la liste est correct ;
- Si il l'est, le site est de confiance et les données sont envoyées, sinon l'outil génère une alerte et annule l'opération.

Toutefois, cette solution nécessite l'intervention de l'utilisateur et peut générer un nombre important de faux positifs. Les auteurs et Angelo P. E. Rosiello ont donc développé une extension à leur système appelée "DOMAntiphish" qui corrige un certain nombre de problèmes de l'outil initial. Il reprend le fonctionnement de l'extension AntiFish en y ajoutant une nouvelle approche basée sur les similitudes de mise en page. Le mode de fonctionnement de cette fonctionnalité est le suivant :
- La page Web est décomposée en blocs suivant des repères visuels ;
- La similitude visuelle entre les deux pages (légitime et suspecte) est mesurée ;
- La page Web suspecte est considérée comme du phishing si cette mesure est supérieure à un seuil.

L'outil calcule la valeur de cette similitude en extrayant l'arbre DOM des pages Web considérées. Quand un mot de passe associé à un certain domaine est réutilisé sur un autre domaine, le système compare la mise en page (l'arbre DOM) de la page courante et de celle du domaine pour laquelle le mot de passe avait originellement été mémorisé. Si le système détermine des similitudes dans les pages, il considère que l'attaque par phi-

Des outils encore imparfaits, reste la formation des utilisateurs

shing est vérifiée.

Les arbres DOM permettent de simplifier le problème du calcul des similitudes entre deux pages Web en le réduisant à l'isomorphisme des deux arbres.

Le prototype DOMAntiPhish est implémenté sous la forme d'une extension pour Mozilla Firefox 2.0 invoquant un programme Java pour calculer la similitude de la mise en page. Le mode de fonctionnement est le suivant :
L'extension Javascript extrait l'arbre DOM représentatif de chaque page Web stockée ;
- L'extension écrit deux fichiers textes contenant les arbres extraits et invoque le programme Java;
- Le programme calcule la similitude des arbres ;
- L'extension lit la valeur de similitude depuis un fichier texte et renvoie le résultat à l'utilisateur.

Angelo P. E. Rosiello a mené des tests sur environ 200 sites Web avec des résultats satisfaisants moyennant quelques ajustements sur l'algorithme de calcul de similitude.

Néanmoins, il précise que cet outil n'est pas parfait et que des limitations ont pu être identifiées :
- Un attaquant peut utiliser une combinaison d'images pour créer la page Web falsifiée, qui visuellement ressemblera à la page légitime. En revanche, l'arbre DOM de la page malveillante sera très différent de celui de la page légitime et la détection échouera dans ce cas.
- La détection pourrait également échouée en cas d'obfuscation de l'arbre DOM.

Quelques moyens de défense sont alors évoqués :
- Juger suspicieuse toute page contenant un très grand nombre d'images ou constituée exclusivement d'images ;
- Réduire le seuil de similitude (au risque d'augmenter les faux positifs).

Angelo P. E. Rosiello conclut finalement sa présentation en précisant que les attaques de type phishing peuvent être prévenues, détectées et limitées par la combinaison d'approches orientées serveurs et clients, mais également par la sensibilisation des utilisateurs.

TOUT SUR LE SPAM

Par Igor Herrmann, Vipawan ▶

Aseem "@" Jakhar, Technical Lead, IBM Internet Security Systems, a présenté une synthèse des techniques anti-spam. Pas de révélation fracassante à attendre ni de nouvelle voie dans la lutte anti-spam, mais un véritable travail d'inventaire commenté et exhaustif, des origines à nos jours.

Aseem part d'un constat : si le Spam n'a pas de définition formelle, il a pour les Entreprises des impacts sérieux : perte de productivité utilisateur mais également de bande passante et de capacité de stockage.
Il est d'autant plus difficile à contrer que sa nature ne relève pas d'une logique de langage « machine » (comme un spyware ou un virus) mais plutôt d'une logique de langage « humain » (compréhension du sens du contenu), ce qui lui permet d'adopter une large gamme de forme tout en préservant ses effets (susciter l'envie ou l'intérêt, souvent le mécontentement).
Pire, ses sources de diffusion sont très répandues car s'appuyant sur des réseaux de postes zombies (postes d'utilisateurs légitimes mais compromis) et il est le vecteur de diffusion privilégié des pandémies virales et, surtout, de chevaux de Troie.

Spam : objectif profit

Après un survol des protocoles de transport d'emails (de SMTP à POP en passant par IMAP) et des techniques de codage (MIME), Aseem nous propose d'entrer dans l'esprit d'un spammeur et de conclure sur sa motivation première : le profit.
Ainsi, la motivation d'un spammeur n'est pas ludique mais publicitaire et marketing (pour nous faire acheter quelque chose). Elle vise à propager une infection et surtout à piéger l'innocent Internaute (capture d'informations personnelles, de moyens de paiement, etc…).
Aseem enchaîne alors de manière très détaillée toutes les tactiques de lutte anti-spam et prodigue divers conseils. Outre les techniques classiques comme les filtres de type texte, de type expression régulière, d'analyses statistiques avec apprentissage (Bayesienne) et surtout filtres basés sur le hash de message (de type Nilsimsa, Ephemeral, ou simples), en voici quelques unes moins connues :
Le greylisting : il s'agit d'un refus temporaire signifié à l'émetteur pour forcer la réémission d'un email. Les outils de spammeurs ne supportant pas cette fonction de stockage temporaire et réémission, ils sont mis en échec alors que les relais légitimes réessaient quelques minutes plus tard.

SPF (Sender Policy Framework) : un mécanisme reposant sur des déclarations dans nos DNS et permettant d'associer à des domaines Internet les IP des relais sortants autorisés à expédier pour ces domaines (un peu le contraire des champs MX qui donnent les relais entrants).

DKIM (Domain Keys Identified Mail) : un système de signature d'email reposant sur une clé publique (publiée par un champ TXT du DNS) et une clé privée contenue sur le relais émetteur. Elle sert à chiffrer un HASH du corps du message, que le relais insère dans l'un des champs spécifiques de l'entête.

Reputation Systems : ces systèmes sont des bases de données consultables en ligne et en temps réel qui associe à une IP un score (la "réputation"), un niveau de confiance. Ce résultat est basé sur une combinaison heuristique des notes de différents critères comme le nombre de virus expédiés depuis l'IP vérifiée, ou le nombre de Spam de connexions avec plusieurs messages et quelques autres paramètres comme l'utilisation de SPF ou DKIM. La liste des critères n'est pas normalisée ni limitée.

HashCash : faire réaliser par le relais émetteur et receveur un calcul (comme un HASH) consommant beaucoup de ressources CPU. Par principe, un mail disposant d'un tel marqueur serait fiable car le process de création pour chaque mail d'un spammeur de ce marqueur ralentira de manière pénalisante tout le process de Spam le rendant inefficace.

Challenge / Response : le relais receveur génère une sorte de challenge (question ou demande d'action) qui sera soumise au relais émetteur ou à l'émetteur. Dans ce cas, cette technique pourra apparaître comme limitée car les emails des expéditeurs peuvent être forgés créant ainsi des risques de spam / déni de service par ricochet. Dans tous les cas, le processus de délivrance sera ralenti, car en attente d'une intervention humaine.

OCR / Reconnaissance de caractères et des images : cette méthode répond aux techniques de spam utilisant des images mais également aux tactiques de phishing exploitants des logos d'Entreprise.
Enfin, Aseem nous propose de relativiser la performance de détection antispam en prenant quelques exemples de contournement du greylisting, de l'OCR et, surtout, précise comment une campagne de spamming se constitue. Bref, la lutte antispam est une affaire d'hyper technologie qui se retrouve à combattre quelque chose de difficile : l'analyse de contenu non souhaité. ■■■

Tivoli

_LE JOURNAL DE NOTRE INFRASTRUCTURE

_93e JOUR : Nous n'avons pas la visibilité nécessaire pour maintenir nos contrats de service ! Impossible de tenir nos objectifs. On ne peut quand même pas travailler à l'aveugle !

_Gilles a loué un gigantesque projecteur...

_95e JOUR : J'ai trouvé mieux. Les matériels, logiciels et services d'IBM Service Management nous apportent la visibilité intégrée, l'automatisation et le contrôle dont nous avons besoin. Nous avons gagné en efficacité et réduit les risques. Et nous pouvons maîtriser les performances de nos services à chaque étape de leur cycle de vie avec un suivi en temps réel de nos engagements SLA (Service Level Agreement).

_J'ai remercié Gilles pour son idée lumineuse...

Découvrez les solutions IBM Service Management :
IBM.COM/**TAKEBACKCONTROL**/VISIBLE/FR

PDF : LA NOUVELLE ÉPÉE DE DAMOCLÈS

Par Thibault Koechlin et Philippe Humeau, NBS System

Durant cette Black Hat Europe 2008 parfois un peu terne, Eric Filiol a présenté les travaux de recherches du laboratoire « Virologie et cryptologie » de l'ESAT sur le thème des menaces qui pèsent sur le format PDF. Sa présentation a mis en exergue que le format PDF était en réalité particulièrement dangereux, contrairement à l'idée que s'en font la plupart des utilisateurs. Eric Filiol signe ici l'une des conférences les plus inquiétantes de cette Black Hat Europe 2008 tant les moyens de défense contre ces attaques semblent peu nombreux et faiblement efficaces. Une véritable épée de Damoclès semble ainsi peser sur les entreprises.

Par Jean Baron, NBS System

Un peu d'histoire : une complexification à la source de problèmes de sécurité

Le format de document portable (PDF) existe depuis 1982. Il a été créé par Warnock et Geschke, les créateurs de la société Adobe. Très vite, ce format va devenir incontournable, étant pour les utilisateurs synonyme de simplicité et de portabilité. Pour garantir la mise en forme du document, le format PDF va, par exemple, être capable d'embarquer la description de la police dans le document, si celle-ci est particulière.

Le succès de ce format dépassera même largement les attentes de ses créateurs, à tel point qu'aujourd'hui le PDF est utilisé par la quasi totalité des entreprises publiques et privées, ainsi que de très nombreux organismes officiels, comme par exemple les gouvernements français ou américain. La standardisation de l'utilisation de ce format risque encore de s'accentuer, puisque « Adobe Systems » a annoncé en 2007 son désir de soumettre les spécifications complètes de son format à l'AIIM pour une publication par le comité ISO.

Ce format de fichier est souvent considéré comme sécurisé dans la mesure où, pour l'utilisateur, il permet seulement de partager des données statiques.

En fait, il n'en est rien ! Au fil du temps, le format PDF s'est considérablement enrichi et complexifié. En effet, que de chemin parcouru depuis la version 1.0 (1992) qui ne possédait comme contenu dynamique que la possibilité d'avoir des liens ! Depuis 1994 et la version 1.1, il est désormais possible d'utiliser PDF pour surfer sur Internet et même de valider des formulaires depuis la version 1.2. Les versions 1.3 et 1.4 ont ajouté des fonctionnalités de sécurité telles que le chiffrement et l'authentification alors que les dernières versions de PDF intègrent des fonctionnalités multimédia toujours plus complexes permettant, par exemple, d'embarquer du javascript. Le format PDF peut aujourd'hui contenir de nombreux types de médias, objets graphiques, images ou vidéo.

Ainsi, nous sommes bien loin du format somme toute assez statique des débuts d'Adobe. Il convient donc désormais de traiter le format PDF comme une source de problèmes de sécurité au même titre que Word ou Excel.

Des attaques déjà répertoriées avant les travaux de l'ESAT

Durant la présentation, Eric Filiol a montré qu'il était possible, en utilisant le langage interne du format PDF, de créer un virus polymorphique dévastateur. Pourtant, il ne s'agit pas des premières tentatives pour

utiliser le format PDF à des fins malveillantes. En effet, même si l'attaque du colonel Filiol est de loin beaucoup plus dévastatrice, plusieurs attaques de moindre envergure ont vu le jour ces dernières années.
Dès 2001 déjà, était créé le virus Outlook_PDFWorm (Peachy) qui embarquait du code VBS dans un PDF envoyé en mail comme un attachement Outlook. L'attaque ne touchait toutefois que le logiciel Adobe Acrobat 5.
En 2003, le worm 'W32.yourde' fit son apparition. Cette attaque avait pour objectif d'exploiter une vulnérabilité dans le parseur Javascript. Une fois l'exploitation réussie, 2 fichiers servaient de charges finales et permettaient d'installer un malware sur la machine. Encore une fois, l'attaque ne touchait qu'Adobe Acrobat 5. Toutefois, contrairement à la première, ce n'était pas le mécanisme même de PDF qui était exploité mais une vulnérabilité. Cette attaque a donc été beaucoup plus facile à corriger pour Adobe.
Par la suite, entre 2003 et 2006, quelques autres attaques exploitant des vulnérabilités de design dans PDF furent recensées. Elles avaient majoritairement pour objectif d'effectuer des attaques de type XSS et d'exécuter des scripts malicieux sur le poste de la victime.
Toutefois, le nombre d'attaques contre les PDF est resté assez faible durant toutes ces années. C'est pourquoi la portée des attaques proposées par Eric Filiol est très importante.
En effet, outre leur grande variété, ces attaques n'utilisent pas de vulnérabilité dans tel ou tel logiciel compatible avec le format PDF, mais emploient uniquement des vulnérabilités de design. Cela implique que tous les logiciels qui peuvent lire des PDF sont vulnérables pour peu qu'ils soient compatibles avec les fonctionnalités du format PDF utilisées par les attaques.

De la récupération d'informations effacées dans les fichiers PDF ou comment faire parler un PDF…

Le format PDF contient de nombreuses fonctionnalités, dont la liste ne cesse de croître au fur et à mesure des révisions du format. Toutefois, certaines problématiques de sécurité existent depuis bien longtemps, en particulier sur la façon dont PDF gère les mises à jour des documents édités.
En effet, le format PDF inclut un système d'historique et de versions, qui permet de suivre l'évolution du document. Ainsi, lorsqu'il est édité directement en PDF, le document garde trace des différentes modifications effectuées par l'utilisateur, et sauvegarde donc de manière invisible dans le corps du document des informations effacées depuis longtemps.
Il est ainsi possible, en utilisant les bons logiciels, ou même en regardant à l'aide d'un éditeur de texte traditionnel le document, de découvrir des informations qui n'apparaissent pas lorsqu'on ouvre le fichier PDF avec par exemple Acrobat Reader.
De nombreuses autres informations peuvent également être découvertes dans les méta-informations présentes dans les documents PDF. Ces informations indiquent par exemple : date de création, nom de l'utilisateur ayant créé le document (son login), date de révision du document ainsi que le logiciel utilisé pour créer le document. Dans plusieurs scénarios d'attaques, ces informations peuvent malheureusement être très utiles à un pirate.
On retrouve ainsi des caractéristiques historiquement présentes dans les formats « doc » de Microsoft. Ceux-ci présentent des vulnérabilités similaires. On s'aperçoit aussi que les méthodes « d'obfuscation » de documents basées sur la modification de l'apparence d'un texte ne permettent pas de protéger réellement une information, celle-ci restant stockée en clair dans le corps du document.
A titre d'exemple, Eric Filiol a ainsi montré qu'en 2005 un document déclassifié du gouvernement américain, traitant de la mort d'un agent du SISMI (Service de renseignement Italien) avait causé une fuite d'information très sérieuse, à cause de la mauvaise utilisation de certaines fonctionnalités. Dans ce cas précis, le document avait été créé à partir de Word. Word offre la possibilité d'ajouter des ombres derrière les textes. Si cette ombre est suffisamment noire, cela rend le texte illisible, malheureusement la simple utilisation de la fonctionnalité «sélectionner le texte » avait permis de révéler les informations qui auraient du être masquées.

…Aux risques de vol d'information et de phishing

Trop peu d'utilisateurs connaissent la possibilité d'utiliser leur lecteur de fichier PDF comme browser Web. Toutefois, il est possible d'utiliser des fichiers PDF pour mener des attaques de type phishing, comme l'a montré Eric Filiol dans sa démonstration.
Depuis les dernières versions, le format PDF supporte l'utilisation de javascript pour augmenter l'interactivité avec les utilisateurs. Néanmoins, cet enrichissement de fonctionnalités amène son lot de risques associés : ingénierie

sociale, exploitation de composants, vol d'information etc.

Le javascript est un vecteur d'attaque possible qui s'est déjà illustré dans d'autres domaines, spécialement celui du Web. Il est ainsi tout à fait envisageable d'utiliser le format PDF pour réaliser des attaques de type phishing ou autre ingénierie sociale. Comme à l'habitude, la victime va se retrouver à envoyer des informations confidentielles à un site qu'elle croit être de confiance, ou va effectuer des actions dangereuses sans le savoir.

Il est également possible de récupérer des informations confidentielles sur la machine et de les envoyer sur un site pirate en utilisant simplement les fonctionnalités proposées par le format PDF.

Comment utiliser des fonctionnalités du langage PDF pour créer un virus dévastateur

Le langage PDF contient différentes instructions, qui, combinées ensemble, donnent la possibilité à un pirate de créer un virus dévastateur. On trouve ainsi 8 instructions dans ce petit langage.

Il est, par exemple, possible d'imprimer de manière totalement silencieuse un fichier présent sur la machine en faisant cliquer un utilisateur sur un PDF. Le pirate situé au sein de la même entreprise que la victime n'aura plus qu'à aller chercher le document sur l'imprimante choisie.

Il est également possible d'incorporer un document présent sur la machine de la victime au sein du document PDF lui-même. Ainsi, il sera possible pour le pirate ayant utilisé un peu d'ingénierie sociale de récupérer le fichier en demandant à la victime de lui renvoyer le document PDF en question.

Toutefois, l'attaque la plus impressionnante reste sans aucun doute celle qui avait pour objectif de modifier Acrobat Reader lui-même, de manière à ce que le pirate choisisse les messages de Warning qu'Acrobat Reader allait proposer à l'utilisateur. Tous les fichiers PDF sont alors modifiés sur l'ordinateur de manière à être infectés par le virus. Une fois ce travail effectué, la charge finale est activée. Seule l'imagination du créateur du virus limite ce qu'il est désormais en mesure de faire sur la machine en question.

Le plus impressionnant est que cette attaque nécessite seulement que la victime clique sur le fichier PDF que le pirate lui a proposé.

Peu de contre-mesures, si ce n'est la vérification systématique de l'intégrité des fichiers de configuration d'Adobe Reader

Malheureusement, bien peu de contremesures existent à l'heure actuelle. Il est toutefois conseillé de vérifier l'intégrité des fichiers de configuration de Adobe Reader tels que 'AcroRd32.dll et RdLang32.xxx'.

De la même manière, étant donné qu'une grande partie de la sécurité du langage PDF est gérée de manière contre intuitive par la base de registre Windows, il est conseillé de faire tourner régulièrement un scanner de configuration de base de registre capable de détecter les erreurs de configuration PDF. Ce scanner sera bientôt proposé par l'équipe de l'ESAT.

Il est également conseillé d'utiliser de manière systématique la signature électronique des documents lors de l'échange de fichiers PDF. Cela permettra, à défaut de bloquer les attaques, de s'assurer de l'identité de l'émetteur du document.

Un accroissement des attaques sur le PDF est certainement prévisible

Bien que très peu d'attaques publiques aient été exploitées pour le moment, des vulnérabilités de design du format PDF, on peut s'attendre à une recrudescence de ce type d'attaques dans les mois et années à venir. Actuellement, il n'existe pas de moyen de contrer ces attaques et aucun logiciel ne peut décréter qu'un fichier PDF donné est dangereux ou pas. Les malwares PDF sont actuellement indétectables par les antivirus et la possibilité de découper un fichier PDF en plusieurs fichiers PDF permettra de reproduire un mécanisme bien connu dans le monde de la sécurité informatique appelé la fragmentation, et qui complexifiera encore davantage la tâche des logiciels de défense.

De par l'utilisation qui en est faite aujourd'hui dans les entreprises et la puissance des attaques envisageables, on peut considérer que le format PDF est un vecteur de menace important à l'heure actuelle. Il suffit d'ailleurs de lancer Acrobat Professional pour s'en convaincre, le format PDF est désormais un support particulièrement puissant de menaces potentielles.

INTERCEPTION D'APPELS GSM : LE MYTHE S'EFFONDRE

Par Jean-Marc Grémy, Cabestan Consultants ▶

Après l'exposé sur les menaces pesant sur les mobiles et sur les quelques moyens de s'en prémunir, le cœur vaillant pensant que plus rien ne pouvait m'arriver, je me suis rendu à la conférence sur l'interception d'appel GSM ! Stupeur ! Cela fait 10 ans que nous nous promenons avec des équipements que l'on pensait sécurisés, dans le pays qui a vu naître la carte à puce, dont nous sommes si fiers. Quelle déception, un mythe s'effondre.

David Hulton et Steve, deux chercheurs en sécurité pour Pico Computing, Inc., ont fait un rapide retour en arrière sur l'histoire et la technologie GSM. Faiblesse de l'implémentation des systèmes de gestion des clés symétriques, initialisation d'une partie des précieux bits de la clé de chiffrement avec des 0, chiffrement des communications voix uniquement sur la partie hertzienne (rien sur sa partie terrestre), avec des implémentations libres et hasardeuses des normes décrivant les concepts de sécurité du GSM, celles émises par l'ITU et l'ETSI. Bref le bonheur. Alors remis dans le contexte de la fin des années 90, où nous avions été bercés par la fin de la guerre froide, le bug de l'an 2000 et enthousiasmé par nos premières expérimentations du mobile en dehors des zones labellisées (i.e. bip-bop), la découverte (1998) de la faiblesse des algorithmes A5/1, A5/0 et A5/2 était alors passée inaperçue de la communauté, réduite à l'époque, à des hommes de la sécurité.

Comment intercepter des appels pour quelques dollars…

L'exposé qui a suivi avait pour objectif de démontrer tant la méthode de cryptanalyse pour attaquer l'algorithme A5/1, celui utilisé pour chiffrer la communication entre le mobile et l'antenne relais, que la facilité avec laquelle cela était devenu possible aujourd'hui. A chaque fois que l'on parle de cryptanalyse, on y associe toujours des moyens importants, coûteux et à la disposition de quelques nations. La démonstration d'aujourd'hui tenait à prouver qu'avec quelques dollars on pouvait intercepter le trafic et le décoder sur un « simple PC », un peu gonflé tout de même.

La méthode proposée :
- Récupération du trafic GSM (voix, SMS) quelques millisecondes ou 1 SMS suffisent,
- Utilisation d'une « Rainbow Table » contenant toutes les valeurs possibles pour les clés symétriques de chiffrement (stockée à demeure dans la carte SIM de l'abonné et dans la base de données de l'opérateur),
- Un peu de capacité CPU, local, ou l'usage d'un botnet, pour casser la communication interceptée en rejouant la Rainbow Table (attaque de cryptanalyse par brute force).

L'objectif était de démontrer qu'avec des moyens d'acquisition simples - quelques Dollars - on pouvait aujourd'hui intercepter des communications GSM. A l'aide d'un simple PC portable, un vieux GSM acheté sur E-Bay et un logiciel dédié à la capture (USRP). Il y a quelques années, au moment où les premières démonstrations ont été faites sur la vulnérabilité de l'algorithme, il fallait des équipements coûteux (>$1M) et quelques fois une infrastructure spécifique (fausse BTS par exemple). La nouveauté est donc ici la simplicité de la solution, quasiment accessible à tout le monde… des hackers.

…Une attaque en Brute Force… et quelques FGPA

Le crack de la session GSM enregistrée sur quelques secondes est possible par attaque de type brute force : on essaie toutes les combinaisons possibles de l'espace de clé. Pour cela, la difficulté est double : il faut une table contenant toutes les clés (c'est-à-dire 258 clés) et une machine testant avec la méthode de cryptanalyse chacune des clés.

Pour l'espace des clés, David et Steve construisent une table des possibles, une rainbow table. Nécessitant une grande puissance de calcul, ils utilisent l'aide de solutions d'un cluster de carte contenant des circuits programmables (FPGA), spécialement conçu pour l'occasion. Permettant ainsi un calcul massivement parallèle. L'idée est simple, dans l'état actuel de la technologie, il faudrait approximativement 33.000 années pour un PC pour calculer toutes les valeurs possibles de l'espace de clé utilisé par l'algorithme A5/1. Pour gagner un peu de temps, ils ont construit une machine utilisant des processeurs dédiés (sorte d'ASICS programmables) dont la seule fonction est le calcul des valeurs possibles de l'espace des clés. Avec cette machine, ils réduisent le temps nécessaire au calcul à seulement 3 mois !

Une fois la table en poche, de 2 TBytes, la démonstration n'est pas arrivée à son terme, il reste à déchiffrer la session préalablement interceptée. Pour ce faire, ils utilisent la même base matérielle pour réaliser cette opération de cryptanalyse. Avec un simple FGPA et 2 TBytes de disque, ils annoncent déchiffrer une communication en 30 minutes, voire en 30 secondes s'ils augmentent le nombre de FGPA !

CQFD ! Visitez leurs sites respectifs pour plus de détails sur les outils et méthodes de cryptanalyse : http://wiki.thc.org.gsm et http://www.openciphers.org

Quels risques pour les utilisateurs français ?

Le déploiement de la 3G est réalisé, la 4G en cours, donc pas de soucis ! Pas aussi serein que cela malgré tout et pour plusieurs raisons. La première est simple, la 3G (UMTS) n'est pas disponible sur tout le territoire. Il existe beaucoup de zones à faible densité de population, difficiles à couvrir, où la 3G n'est pas disponible, notamment les zones rurales. Seuls le GSM et le GPRS/EDGE sont disponibles, donc vulnérables. De plus, des chercheurs ont mis en évidence que l'algorithme de chiffrement de la 3G (A5/3, KUSUMI) était lui aussi vulnérable. A priori, David et Steve ne l'ayant pas évoqué, nous sommes tranquilles…
Et puis, même lorsque la 3G est disponible, il est relativement facile de brouiller sa fréquence pour contraindre le mobile à se replier en mode GSM, retour à la démonstration précédente ! ■■■

édito

La réussite d'une équipe !

Aujourd'hui, Trend Micro a 20 ans, et déjà plus de 10 ans de présence sur le marché français.
Autant d'années pendant lesquelles Trend Micro a obtenu d'excellents résultats et affiché chaque année une croissance soutenue.
Lorsque tout va bien, il est important d'attribuer le mérite de la réussite à d'autres facteurs qu'à soi-même.

Lorsque que l'on regarde par la fenêtre du 85 avenue Albert Premier, magnifique petit bâtiment du Siège Trend Micro France, il est très facile d'apercevoir les différents éléments qui ont contribués à cette réussite :
- Nos clients qui nous font confiance et sont chaque année de plus en plus nombreux
- Nos partenaires revendeurs qui, chaque jour, accompagnent nos clients dans la mise en place et la maintenance de nos solutions
- Nos distributeurs à valeur ajoutée présents pour supporter notre réseau de revendeurs prescripteur que ce soit sur le plan commercial ou sur le plan technique,…
- Parfois la chance…

Pour ce 20ème anniversaire, je souhaiterais, pour ma part, attribuer une grande partie de cette réussite à l'ensemble des collaborateurs de Trend Micro.

Dans un monde mené par des maniaques du management, des visionnaires fulgurants, des futuristes délirants ou des gourous du développement personnel, il est rafraîchissant de voir une entreprise réussir si brillamment grâce à une notion simple appliquée avec passion et imagination.

L'essence d'une profonde perspicacité est la simplicité.

La réussite consiste entièrement à faire progresser les autres. Elle consiste à rendre les collaborateurs encore plus intelligents, plus forts et plus audacieux. Rien de ce que l'on fait personnellement n'a d'importance, hormis la manière dont on anime, soutient et aide ses collaborateurs à prendre davantage confiance en eux.

Le succès n'est jamais venu de mon travail au quotidien mais de l'excellence des résultats de mon équipe.

Trend Micro a 20 ans

Fondée en 1988, Trend Micro est une société pionnière dans le domaine de la gestion de contenu sécurisé et dans le domaine de la gestion des menaces. Avec un siège social basé à Tokyo (Japon), Trend Micro est présente dans plus de 30 pays. Elle propose ses solutions dans le monde entier via son réseau de distribution.

En France, Trend Micro compte environ 35 personnes et dispose d'un des laboratoires des TrendLabs. Le bureau basé à Rueil regroupe les services commerciaux, marketing, et techniques.

Cette année, Trend Micro fête ses 20 ans. A cette occasion, Global Security Mag a demandé à Jean-Marc Thoumelin, Directeur des Opérations pour l'Europe du Sud, de dresser un bilan de ces deux décennies.

GS Mag : Qu'est-ce qui selon vous caractérise Trend Micro ?

Jean-Marc Thoumelin : Notre réussite repose sur 4 points forts : l'innovation, la croissance, le leadership et un engagement permanent auprès de nos clients et partenaires.

1- **L'innovation** continue comprend de nouvelles technologies basées sur le comportement et de nouveaux services gérés, ainsi que l'amélioration de nos produits traditionnels. Nous offrons donc des solutions complètes de gestion de contenu sécurisé tels que les antivirus, les anti-spywares, les anti-spams, l'anti-phishing, le filtrage de contenu, la prévention des fuites d'informations et nos capacités en termes de compatibilité.

INNOVATIONS PHARES

1995	Lancement de ServerProtect™ : le premier antivirus LAN basé sur serveur
1996	Lancement de InterScan™ VirusWall™ : le premier antivirus pour passerelle Internet basé sur serveur
1997	Lancement de ScanMail™ : le premier antivirus pour messagerie basé sur serveur
1998	Lancement de Trend Micro Virus Control System : la première console d'administration centralisée
2002	Lancement de Enterprise Protection Strategy : stratégie de gestion du cycle de vie des menaces
2003	Lancement de InterScan Messaging Security Suite avec Spam Prevention Solution : la première sécurité du contenu intégrée au niveau de la passerelle
2004	Lancement de Network VirusWall™ : le premier dispositif de contrôle d'accès au réseau
2005	Network Reputation Services : anti-spam au niveau de la couche réseau
2006	InterCloud Security Services : protection contre les zombies via le moteur de sécurité à analyse comportementale
2007	Protection totale contre les menaces Internet avec évaluation de la réputation des sites Web

QUELQUES MOTS SUR LES TRENDLABS

Les TrendLabs constituent le réseau mondial de centres de recherche, de services et d'assistance de Trend Micro. Ils sont destinés à surveiller les menaces et à prévenir les attaques en permanence. Des données précises fournies en temps réel leur permettent de fournir des règles de sécurité régulières et efficaces destinées à détecter, anticiper et éliminer les attaques.

Les TrendLabs disposent de plus de 800 experts sécurité à travers le monde et fonctionnent 24 h/24 et 7 j/7. Leur siège se trouve aux Philippines, mais la société compte des laboratoires régionaux aux États-Unis, au Japon, en France, en Allemagne et en Chine. Étant donné que ce groupe de recherche et d'assistance fonctionne en continu et est en mesure de comprendre les langues locales, il peut ainsi répondre à ces clients en temps réel, et surtout, réagir en temps réel contre les nouvelles menaces. En conséquence, les entreprises peuvent limiter les dégâts, réduire les coûts et garantir la continuité de leurs activités.

Les TrendLabs placent les menaces contre la sécurité au cœur de leur activité, depuis les menaces liées au courrier électronique et aux messageries instantanées jusqu'à la catégorie émergeante des menaces Internet. Parmi les menaces et les technologies de menaces courantes détectées par les TrendLabs, on trouve les spams, les logiciels publicitaires, les programmes espions, les logiciels malveillants, les crimewares, les zombies, les attaques de phishing et les rootkits.

La présence régionale des TrendLabs permet à Trend Micro d'identifier les menaces régionales ciblées et d'y répondre plus rapidement.

2- Une **croissance** continue grâce à de nouveaux programmes et des engagements plus forts avec nos précieux partenaires du secteur et du développement technologique, nous continuerons à chercher de nouveaux moyens d'étendre notre expertise à de nouveaux marchés ainsi que de nouvelles manières de servir notre clientèle.

3- Un **leadership** continu sur nos principaux marchés, notamment la sécurité Web et des messageries, ainsi qu'une expertise nous permettant d'aider nos clients à gérer leurs problèmes de sécurité dans l'environnement actuel.

4- Un **engagement** continu à conserver une longueur d'avance sur les nouvelles menaces et à offrir à nos clients la liberté d'utiliser leur ordinateur comme ils le souhaitent, sans avoir à se soucier de protéger leurs systèmes et leurs données contre un éventail toujours plus large de menaces Internet.

LES MENACES INFORMATIQUES SONT DEVENUES DES TUEUSES SILENCIEUSES

GS Mag : Comment ont évolué les menaces depuis 20 ans ?

Jean-Marc Thoumelin : En 20 ans, les menaces informatiques sont devenues des tueuses silencieuses, orientées profit et invisibles aux yeux des utilisateurs finaux. Les auteurs de logiciels malveillants ne cherchent plus à faire du bruit et à faire la une des journaux, ils veulent dérober des informations personnelles, manipuler des PC afin de les utiliser comme machines zombies et commettre des « cybercrimes ». La complexité croissante d'Internet dans nos vies quotidiennes a apporté avec lui son lot de menaces, mais également davantage de possibilités pour Trend Micro de développer des moyens de veiller à la sécurité de ses clients sans que ces derniers aient à s'en préoccuper. La nature du travail en réseau a également changé ; les réseaux n'ont plus de frontières. Les systèmes sans fil, les dispositifs mobiles, Web 2.0 et sa capacité de gestion d'énormes quantités de contenu utilisateur, ainsi que les bureaux virtuels ont permis au flux d'informations de traverser de nombreuses plateformes et de nombreux fournisseurs.

NOUS VOULONS CRÉER UN UNIVERS D'ÉCHANGE D'INFORMATIONS NUMÉRIQUES SÉCURISÉ

GS Mag : Quelle est votre stratégie aujourd'hui pour faire face à ces dernières ?

Jean-Marc Thoumelin : Notre objectif est le même depuis des années : créer un univers d'échange d'informations numériques sécurisé.
Notre technologie de protection contre les menaces Web est le levier majeur de différentiation de notre stratégie et de nos passerelles de sécurité. Elle s'impose à ce titre en tant qu'approche plus intelligente aux véritables « bombes à retardement » que sont les méthodes traditionnelles de sécurité.

Trend Micro capitalise, en effet, sur la puissance de l'approche « In the Cloud », qui fait appel à des notations de réputation en amont du réseau d'entreprise. La détection du spam et des logiciels malveillants, ainsi que les informations fournies par tous nos produits TIS, SMB et Enterprise renforcent les lignes de défense et concrétisent une protection réseau en temps-réel.

À chaque fois que l'un des millions de clients Trend Micro dans le monde fait face à une menace ou reçoit un nouveau message de spam ou de phishing, la solution Trend Micro à l'origine de cette détection notifie cette nouvelle source de menace à un réseau étendu de moteurs de corrélation. Cette notification sera alors évaluée par rapport à des bases existantes contenant des informations supplémentaires sur la réputation de l'adresse Web incriminée. Si la réputation est négative, tous nos clients seront automatiquement notifiés du danger que présente un accès à ce site, et donc protégés.

Trend Micro dispose des bases de données de réputation Web les plus fiables et complètes au monde : plus d'un milliard de sites Web malveillants et de sources de spam évalués en temps-réel pour neutraliser les emails et sites web malveillants. En associant les technologies de sécurité Web et de messagerie de Trend Micro, les entreprises bénéficient d'un feedback permanent entre les bases de réputation. Tous les services de réputation s'adossent à des technologies In The Cloud et non à des mises à jours statiques, ce qui matérialise une veille en temps-réel sur les menaces Web et les sources de spam.

Cette approche protège contre toutes les variantes d'une attaque Web, qu'il s'agisse de sources de spam, de liens malveillants intégrés aux emails ou de sites Web malveillants. Cette approche en temps réel et multi-protocole devient un impératif pour neutraliser efficacement toutes les menaces Web actuelles et répondre dès à présent à leur évolution future.

Trend Micro fait ainsi la différence en disposant de toutes les technologies de sécurité utilisées par ce processus collaboratif de protection. Nous intégrons ainsi efficacement tous les feedbacks sur le spam, les logiciels malveillants, les « webcrawlers », « honeypots » et autres menaces similaires.

Contrairement à un simple filtrage des URL, les moteurs de corrélation sont alimentés par un réseau toujours plus important de sondes, à savoir les produits Trend Micro utilisés par nos clients. Lorsqu'un client accède à un site Web, il déclenche une notification vers le réseau de bases de réputation le plus important et complet au monde.

Résultat : une protection en temps réel contre le plus grand nombre de menaces Web, dans un délai le plus court possible.

Les enjeux de sécurité sont à la hauteur des menaces

Laurent Delattre, Directeur Commercial
Grands Comptes Europe du Sud, Trend Micro

Global Security Mag : Quelles sont les préoccupations des grandes entreprises ?

Laurent Delattre : Le challenge à relever pour les grandes entreprises est très important. L'objectif étant d'optimiser la sécurité à tous les niveaux du système d'information bien sûr mais aussi de mettre en œuvre et de respecter une politique de sécurité en conformité avec de nouvelles normes, type Sarbanes Oxley, HIPAA… C'est un enjeu considérable compte tenu de la nature même des menaces actuelles qui ne sont plus aussi visibles qu'avant (de ce fait, la justification des investissements en matière de sécurité est également un enjeu considérable au sein même des entreprises). Ainsi, il faut adapter une architecture informatique globale existante avec une architecture de sécurité qui va permettre une visibilité accrue sur tous les événements qui pourraient constituer une menace. Cela est, bien sûr, conjugué très fréquemment avec une architecture très décentralisée pour les grands groupes et un nombre d'utilisateurs très important. Par conséquent, l'optimisation par la centralisation de la gestion des outils de sécurité est devenue un souci majeur. Sans oublier que le compromis à trouver entre production et sécurité est toujours le « nerf de la guerre ». Notre métier est de permettre à nos clients de faire le leur.

GS Mag : Quelles sont les principales menaces qui pèsent sur les grandes entreprises ?

Laurent Delattre : Nous assistons à plusieurs phénomènes adjacents au sein de nos grandes entreprises, par exemple, la mobilité des utilisateurs et l'ouverture grandissante des accès Internet pour les employés. La démocratisation de l'accès au Web multiplie les sources possibles d'infection par pure opération mathématique, tout en précisant que le Web est devenu le vecteur le plus important de malwares. La propagation des menaces par mail étant devenue de plus en plus difficile de par la fiabilité des outils existants, le Web est désormais la source la plus aboutie pour les hackers et autres acteurs malveillants. Facile, rapide, invisible et très efficace puisque très ciblée. Le résultat étant que l'utilisation massive du Web doit être contrôlée et maîtrisée. La mobilité est également une problématique grandissante. Même si maintenant la communication à distance est quasi maîtrisée (VPN, PKI etc..), la fuite d'information est une menace très sérieuse. Les outils mobiles, tels que les ordinateurs portables, PDA ou autres Smartphones, sont de vrais outils de communication et de stockage, inutile de préciser l'impact de la perte ou du vol des données qu'ils contiennent, surtout que la plupart des utilisateurs mobiles sont les VIP des grandes entreprises.
En passant de l'autre côté de la barrière, une menace sous-jacente et silencieuse existe bel et bien. Compte tenu de la multiplication du type de menaces sur le Web, virus, chevaux de Troie, spywares, …. les signatures antivirus se multiplient également, ce qui implique une croissance importante des besoins en ressource des machines et serveurs a protéger afin de pouvoir être efficaces. Ceci implique également des organisations très importantes en termes de ressources chez les éditeurs de solution de sécurité afin de permettre une réponse optimale. Les chiffres ne font qu'augmenter et de manière considérable. Nous sommes passés de 1.738 virus en 1998 à 1.100.000 en 2008 ! La croissance est exponentielle et les outils traditionnels ne seront bientôt plus en mesure de jouer leur rôle. Un virage très important se profile.

GS Mag : Quelles sont les tendances du marché de la sécurité aujourd'hui ?

Laurent Delattre : Le marché s'oriente donc vers des solutions déportées en temps réel. Le « Software as a Service » est une tendance forte aujourd'hui. Le principe étant tout simplement de déporter les outils de sécurité directement chez les éditeurs tout en gardant la maîtrise et la gestion de la politique de la sécurité. Les clients s'affranchissent ainsi de toute la gestion logistique des outils de sécurité « hardware, mises a jour des soft de sécurité, des OS etc..).

La « réputation » est également une réponse importante. L'objectif étant de pouvoir traiter en temps réel toute source d'infection potentielle grâce à des procédés de réputation d'un site Web, d'un émetteur de mails, etc.

Nous notons également d'une manière plus globale une tendance forte dans les grandes entreprises à se tourner non plus vers le « best of breed » mais vers un interlocuteur unique. La multiplication des éditeurs multipliant les outils de gestion et d'administration, ce changement de cap permet de rationaliser l'administration d'un parc antivirus par exemple. Ceci étant dit, cette tendance est beaucoup plus forte dans certains pays comme les Etats-Unis, le Japon, l'Allemagne et le Benelux. En France, nous sommes encore en période de transition ou le réflexe multi éditeurs est encore très implanté.

TREND MICRO FRANCE

Siège : Rueil Malmaison
Site Web : www.trendmicro-europe.com
Nombre personnes : 35
1 TrendLab

2008, le « péril Web » est en marche

Rik Ferguson, Trend Micro ▶

Depuis 2007, les pirates informatiques ont concentré leurs attaques sur les sites Web. Rik Ferguson, Solutions Architect de Trend Micro, constate que cette tendance s'est renforcée en 2008. Les hackers utilisent des techniques classiques qui tirent avantage des failles du langage Cross Site Scripting (XSS), de l'injection SQL et de l'exploitation de vulnérabilités dépourvues de patch correctif. Pour remédier à ces menaces, il propose d'utiliser des technologies de sécurité "In the cloud" qui permettent de neutraliser les menaces à la source et de sensibiliser les utilisateurs.

Global Security Mag : Durant la Black Hat, les chercheurs ont dressé un bilan de l'évolution des techniques des pirates, quelles principales nouveautés avez-vous recensé pour 2008 ?

Rik Ferguson : 2007 a été l'année des menaces Web qui sont devenues les principaux risques de sécurité. Ces attaques utilisent notamment l'infrastructure d'Internet et le port HTTP 80 comme un levier d'infection. Le protocole SMTP est également souvent un vecteur de diffusion du spam qui constitue une première étape pour inciter les utilisateurs à se rendre sur des sites Web malveillants. Les attaques s'effectuent désormais sur une région géographique cible et de manière localisée (utilisation d'une langue locale, ciblage d'une population ou d'une communauté spécifique, etc.). Elles utilisent de nombreuses techniques d'ingénierie sociale : messages ou sites relatifs à des événements récents, ou d'intérêt pour une communauté spécifique. Les menaces Web ont également pour particularité de se présenter sous différentes variantes, ce qui permet de contourner les anti-virus classiques et de rester indétectable aussi longtemps que possible. À l'opposé donc des épidémies initiales de logiciels malveillants dont l'intention était de maximiser les infections et les dommages, aussi rapidement et visiblement que possible. La multiplication des menaces Web a également eu pour conséquence directe une forte croissance et une expansion continue des réseaux de PC piratés, appelés également bots ou zombies, et utilisés dans un but lucratif. Ces différents constats témoignent du caractère de plus en plus criminel de telles exactions. 2007 révèle également une tendance qui s'accentue en 2008, à savoir la mise en péril du nombre de sites Web par ces menaces. Les sites Web sont, en effet, piratés à l'aide de techniques classiques qui tirent avantage des failles du lan-

gage Cross Site Scripting (XSS), de l'injection SQL et de l'exploitation de vulnérabilités dépourvues de patch correctif. Un site piraté est utilisé pour recueillir frauduleusement certaines données, lorsqu'il n'héberge lui-même un logiciel malveillant qui redirigera le visiteur vers un site à risque. Cette méthode est proche de celle qui fait actuellement ses preuves et qui consiste à utiliser des bannières publicitaires sur des sites Web « innocents » pour rediriger les visiteurs vers un logiciel malveillant. Enfin, n'oublions pas la multitude de sites Web malveillants mis en ligne pour infecter les utilisateurs confiants via des téléchargements à leur insu, ainsi que les sites de phishing qui visent à détourner les identifiants confidentiels des utilisateurs.

UNE GESTION INTELLIGENTE DES RISQUES PLAIDE EN FAVEUR D'UN LOGICIEL CORRECTEMENT INSTALLÉ ET MAINTENU

GS Mag : Lors de la Black Hat Conference, Johanna Rutokowska, un chercheur en virologie, a conseillé de ne plus utiliser d'antivirus car ils diminuent la sécurité en ajoutant des bugs, que répondez-vous à cette affirmation ?

Rik Ferguson : Voilà le type de conseils qui ne fait qu'alimenter davantage les ambitions des cybercriminels ! Il est vrai que les logiciels de sécurité ne sont pas exempts de failles, comme tout logiciel d'ailleurs. Je reste néanmoins convaincu qu'une gestion intelligente des risques plaide en faveur d'un logiciel correctement installé et maintenu. Après tout, il est fort probable qu'un système non protégé connecté à Internet soit infecté en l'espace de quelques heures. Pour préciser la réponse à la question précédente, tous les produits de sécurité contre les menaces Web doivent disposer à minima d'une forme de technologie de réputation, qui renforcera les méthodes anti-virus classiques, pour ainsi proposer une sécurité de type « In the cloud », active directement sur Internet et en amont du réseau d'entreprise. En effet, les logiciels malveillants se déclinent en variantes à une vitesse tellement rapide que les solutions basées sur des signatures de virus deviennent rapidement obsolètes, compte tenu des ressources systèmes consommées et des délais de mise à jour des nouvelles signatures.

GS Mag : Lors de ce même événement, un autre chercheur en virologie, Feng Xue, a montré que les pirates informatiques se servaient des vulnérabilités des antivirus pour attaquer les SI, quels sont vos conseils pour éviter ce type de problèmes ?

Rik Ferguson : Comme tout logiciel, un produit de sécurité peut avoir des failles, une situation qui s'est d'ailleurs avérée vraie dans le passé. Les éditeurs sont particulièrement attentifs à cette problématique lors des phases de tests d'assurance qualité, et nous nous engageons à proposer des patchs de mise à jour aussi rapidement que possible lorsque ces failles sont identifiées après la commercialisation du produit. Les utilisateurs doivent donc s'assurer que leur solution est toujours à jour, un point essentiel pour juguler les risques. Au-delà, une solution de sécurité adossée à des services de réputation minimise davantage les risques face aux attaques de type Zero-day.

GS Mag : Dans le domaine de la lutte contre le spam, quelles réponses technologiques apportez-vous ?

Rik Ferguson : Face à la prolifération des menaces Web, et compte tenu des liens entre le spam, les logiciels malveillants et la cybercriminalité, nous ne pouvons nous contenter d'un outil qui ne ciblerait que le spam. Le spam n'est effectivement plus cette attaque bénigne de ses premières heures : bien qu'intrusif et gourmand en ressources systèmes, le spam n'a pendant longtemps pas été considéré au titre des menaces et logiciels malveillants. C'est désormais le cas et nous devons repenser les solutions et privilégiant une approche intégrée pour combattre des menaces elles aussi intégrées. Cette approche associe plusieurs savoir-faire et techniques : vérification des URL et des domaines, veille sur les adresses IP, services de réputation, fichiers de signatures, veille comportementale de certains protocoles, etc.

GS Mag : Le phishing est toujours plus virulent, quels sont vos conseils pour y remédier ?

Rik Ferguson : Le phishing continue à cibler les entreprises commerciales ou institutions financières majeures. La nouveauté réside dans la localisation linguistique du contenu et le ciblage des victimes sur un secteur géographique précis. Les menaces Web substituent de plus en plus les noms de domaines pour rediriger le trafic vers des sites criminels. Le traditionnel mail de phishing a laissé la place à la technologie DNS fast flux ou le kit Universel Man-in-the-Middle pour initier leurs attaques. Ces nouveaux outils aident les criminels à collecter des informations confidentielles en amenant les victimes potentielles à communiquer avec un site Web légitime via une fausse URL mise en ligne par le pirate. Les kits de phishing de type Man-in-the-middle proposent une interface utilisateur pour créer une copie d'un site Web légitime, cible d'une opération de phishing. Cette copie de site Web communique avec le site légitime et télécharge les pages Web d'origine. La victime communique donc toujours avec le site légitime tandis que le pirate détourne simplement toutes les informations fournies par l'utilisateur. Face à l'évolution des menaces traditionnelles (logiciels malveillants, spam, phishing, etc.) vers un modèle de menaces Web évoluées, les produits de protection classiques connaissent des limites et il est plus que jamais urgent de passer à une protection qui sache corréler les différents vecteurs de menaces et y répondre efficacement.

CONTRE LES VIRUS CIBLÉS, IL FAUT DES SOLUTIONS PRO-ACTIVES ET MENER DES ACTIONS DE SENSIBILISATION AUPRÈS DES UTILISATEURS

GS Mag : Les virus sont de plus en plus ciblés, comment peut-on se protéger de ces nouveaux types d'attaques ?

Rik Ferguson : On compte parmi les menaces à fort impact celles qui ciblent un profil prédéfini de victimes, qu'il s'agisse de communautés qui se regroupent autour d'intérêts communs, d'une population à l'échelle régionale ou locale, ou encore de certains segments de la société. Les pirates échafaudent des stratégies de plus en plus évoluées et capables de convaincre toujours plus de personnes quant à l'authenticité des produits et des services mis en avant par le pirate. Les services de communication tels que l'email, la messagerie instantanée et le partage de fichiers continueront à subir des menaces telles que le spam image, les URL malveillantes et les fichiers joints douteux. Ces menaces utiliseront des techniques d'ingénierie sociale dans différentes langues cibles, des techniques choisies selon leur efficacité à attirer des victimes potentielles. Les cybercriminels, quant à eux, continueront à renforcer leurs réseaux de PC zombies et à détourner des informations confidentielles. Le dénominateur commun de ces menaces réside dans leur capacité à tirer avantage d'Internet et de ses fonctionnalités. En clair, au-delà des pratiques de bon sens qui consistent, par exemple, à ne jamais ouvrir un email ou un fichier douteux, une solution de sécurité sur PC doit être suffisamment agile et dynamique pour garantir une protection en temps réel aux utilisateurs qui font face à des menaces émergentes. La détection des virus à base de signatures n'est désormais plus suffisante.

GS Mag : Aujourd'hui, les politiques commencent à prendre au sérieux le problème de la cybercriminalité, comment un éditeur comme Trend Micro peut apporter son concours à ces initiatives ?

Rik Ferguson : Trend Micro collabore déjà activement avec de nombreux organismes nationaux et internationaux de lutte contre la criminalité, comme Interpol. Nous leur fournissons des informations sur les incidents identifiés et participons lorsque nécessaire à leurs enquêtes. Nous intervenons également régulièrement lors de conférences et séminaires organisés par des institutions.

GS Mag : Que peuvent faire les PME qui ont peu de temps et de moyens pour répondre à ces menaces ?

Rik Ferguson : Les PME, tout comme les entreprises plus importantes, doivent valider la pertinence de la solution dans laquelle ils investissent compte tenu de la rapide évolution des menaces Web. Les PME connaissent des contraintes supplémentaires en matière de temps et de ressources et elles ne peuvent pas mobiliser des personnes à plein-temps sur le sujet de la sécurité de leurs informations. Les PME feront ainsi de plus en plus appel à des éditeurs capables de proposer une solution de sécurité gérée et mise à jour à distance, ce qui leur permet de se repositionner sur leur cœur de métier et de déléguer leur sécurité à des mains expertes.

LA TECHNOLOGIE « IN THE CLOUD » EST UN REMÈDE POUR SÉCURISER LE WEB

GS Mag : Les réseaux sociaux semblent être de nouveaux vecteurs de menaces, que doivent faire les entreprises pour remédier à ce problème ?

Rik Ferguson : Au cours des dernières années, les réseaux sociaux et outils similaires ont permis aux utilisateurs de participer plus activement à Internet. Avec cette évolution, les entreprises se sont de plus en plus ouvertes à l'idée de proposer des fonctionnalités, applications et des accès distants via leur site Web corporate. Parallèlement, les entreprises souhaitent tirer avantage de ces nouveaux outils pour créer des communautés d'utilisateurs et favoriser une participation plus active de ces derniers. Ces fonctionnalités rendent le Web plus interactif et séduisant, mais témoignent néanmoins de nouveaux risques, comme le souligne l'explosion des attaques via le Web : on se souvient notamment du logiciel « Secret Crush » qui s'est installé en toute autonomie en tant que Widget de Facebook sur environ un million de PC à la fin 2007 et au début 2008.
Les entreprises doivent, aujourd'hui, choisir entre une restriction de leur accès Web à une poignée de sites définis comme essentiels, ou l'activation d'une couche de sécurité « In the cloud », particulièrement évolutive, et qui sécurise les processus métiers de l'entreprise. Cette solution semble la plus pertinente compte tenu de la croissance des collaborateurs nomades et distants et de frontières de plus en plus floues entre les réseaux.

GS Mag : Pour conclure, quelle est la stratégie de Trend Micro en matière de protection ?

Rik Ferguson : La mutation majeure des menaces Web contribuera à faire évoluer les technologies nécessaires pour protéger efficacement les utilisateurs. Un simple antivirus qui utilise des signatures n'est plus suffisant. Aujourd'hui, les auteurs de logiciels malveillants collaborent entre eux pour échapper à toute détection et génèrent de multiples variantes de ces menaces pour déjouer les méthodes de détection traditionnelles.
Cette criminalité, active à l'échelle mondiale, se veut collaborative et donc plus malveillante. Elle remet en cause les fonctionnalités d'analyse et de neutralisation proposées par les logiciels basés sur les signatures, et qui ont été adoptés par les utilisateurs depuis maintenant 20 ans. La croissance exponentielle des fichiers de signatures rend les mises à jour plus complexes tandis que le taux de neutralisation

n'est plus un indicateur clé de la capacité d'une solution à protéger efficacement ses clients.

Actuellement, l'approche traditionnelle doit être utilisée en conjonction avec d'autres techniques pour ériger une ligne de défense multicouche et qui tire avantage de la nature interactive d'Internet.
L'activation d'outils de sécurité à l'échelle de la passerelle Internet et des postes client n'est plus suffisante. Pour mettre en échec les cybercriminels, la protection classique de base doit désormais s'adosser à une sécurité « In the cloud » qui apporte une réponse proactive aux nouvelles menaces émergentes.

Les technologies de sécurité "In the cloud" neutralisent les menaces à la source, en amont de la passerelle réseau. Les bases de données « In the cloud » sont mises à jour en temps réel, ce qui permet d'être moins dépendant des bases locales et de la fréquence de leur mise à jour, tout en allégeant les charges mémoires et d'analyse. ■■■

UNE TECHNOLOGIE DE SÉCURITÉ « IN THE CLOUD » PERFORMANTE DOIT PROPOSER LES FONCTIONNALITÉS SUIVANTES :

Une technologie de réputation Web :
■ Surveillance des URL des sites Web en utilisant le filtrage, la localisation des adresses IP liées aux URL à risque, et la vérification des URL par rapport à une notation de réputation fournie par une base.
■ Mises à jour de la base de données en temps réel et en permanence, permettant aux éditeurs de sécurité de répondre et de maîtriser rapidement les messages suspects et les menaces Web.
■ L'accès aux sites Web malveillants est neutralisé en cas de mauvaise notation de réputation du domaine hôte.

Technologie de réputation email :
■ Valide les adresses IP par rapport à un service de réputation et à un service qui surveille en temps réel les comportements du trafic Internet et les IP sources des emails suspects. Cette approche constitue une parade contre les réseaux de PC zombies et les sources de spam.

Technologie d'identification de zombies et des bots :
■ Analyse du trafic réseau et des comportements des bots pour identifier les commandes serveur de contrôle du bot.
■ Surveillance permanente de ces serveurs pour identifier et neutraliser ceux qui sont actifs.
■ Mise à disposition en temps réel d'un flux d'adresses IP avec leur degré de confiance et le type de menace identifiée.
■ Neutralisation des communications vers et à partir des serveurs de commande et de contrôle, compte tenu de l'adresse IP.

La prévention des fuites de données par le filtrage, l'empreinte numérique et la sensibilisation

La perte d'informations privées ou relevant de la propriété intellectuelle peut aussi bien entraîner des amendes et des procès, que nuire à l'image de marque et susciter une mauvaise presse. Pour sécuriser les données sensibles, les entreprises ont besoin d'une solution de protection contre les fuites d'informations potentielles. LeakProof™ de Trend Micro maîtrise la diffusion de données sensibles en appliquant des règles de sécurité aux postes clients, via des technologies d'empreinte numérique, de filtrage de contenu et d'outils de sensibilisation. De surcroît, LeakProof permet de réaliser un audit complet des informations sensibles sur les postes surveillés.

Selon le Gartner, 47 % des données d'entreprise sont stockées sur des supports mobiles. 350.000 d'entre eux ont fait l'objet de perte ou de vols aux Etats-Unis, en deux ans. Et ce n'est qu'un début ! Quant au possesseur de l'objet perdu, sa plus grande frustration réside dans la disparition d'un outil bien pratique oubliant l'essentiel : la valeur du contenu.

La conformité aux réglementations relatives à la gestion des entreprises et à la confidentialité nécessite des stratégies de sécurité complètes permettant de conserver la confidentialité des informations et de protéger la vie privée des clients. Face à ces défis, les entreprises ont besoin de solutions intelligentes de filtrage du contenu qui appliquent des règles de sécurité et informent les employés sur la bonne gestion des informations.

Trend Micro LeakProof protège contre les pertes de données grâce à une approche qui allie une application des règles sur les terminaux finaux à un contrôle des empreintes précis et une technologie de classification du contenu. LeakProof permet de réaliser des audits complets des postes surveillés pour identifier les informations sensibles. Ainsi, les machines dont le contenu sera le plus critique seront répertoriées. Les RSSI – DSI… pourront ainsi quantifier la diffusion, (dilution) des données sensibles et identifier au cas par cas les listes de documents concernés.

Cette solution se compose d'un logiciel client et d'un serveur sous forme d'appliance :

• **LeakProof Anti-Leak Client :** ce logiciel non intrusif, de contrôle et d'application des règles détecte et protège contre les pertes de données au niveau de chaque poste de travail. Le client communique avec le serveur DataDNA pour recevoir les mises à jour des règles et des empreintes numériques, et rapporte les violations à l'administrateur.

• **LeakProof DataDNA™ Server :** ce système offre un point névralgique pour la visibilité, la configuration des règles et l'extraction des empreintes numériques depuis des sources de contenu.

Une interface Web prend en charge les stratégies de sécurité pour l'exploration, la classification, la configuration des règles, la surveillance et la création de rapports.

LE FILTRAGE DES DONNÉES, PORTS, FLUX, RÉSEAUX

LeakProof offre une couverture des périmètres réseau et postes de travail. Elle inclut des flux de réseau, tels que HTTP/S, SMTP, la messagerie Web, FTP et la messagerie instantanée, ainsi que les entrées/sorties des postes de travail comme les transferts de fichiers sur des clés USB ou leur gravure sur des CD/DVD. Des modules de filtrage intégrés inspectent le contenu avant son cryptage afin de protéger l'activité transmise via un navigateur Web et les applications de messagerie électronique. Les responsables informatiques peuvent désactiver des périphériques en toute simplicité.

DATADNA™ : LA PROTECTION PAR L'ADN DES DOCUMENTS

Cette technologie détecte les données sensibles avec des niveaux de précision et de performances élevés. Plusieurs moteurs de classification fournissent un filtrage en temps réel à l'aide d'empreintes numériques, d'expressions régulières, de mots clés et de métadonnées. Des algorithmes extraient des informations à partir du contenu pour créer une séquence ADN unique pour chaque document. Cette « empreinte numérique du document » permet une application des règles sur les postes de travail connectés ou hors ligne.

SANS OUBLIER L'INDISPENSABLE SENSIBILISATION DES UTILISATEURS

Des « alertes » interactives permettent aux responsables informatiques de créer des boîtes de dialogue au contenu sensible qui s'affichent directement sur l'écran d'ordinateur de l'employé. Ces boîtes de dialogue contiennent des liens URL personnalisés qui informent les employés sur la gestion appropriée des informations confidentielles en relation avec la politique de sécurité du système d'information. Les transferts non autorisés sont bloqués ou les employés sont invités à utiliser le module intégré de cryptage des données pour copier des données sur des périphériques USB. ■

LES CONSEILS DE TREND MICRO AUX UTILISATEURS

1. Suivre les recommandations et processus dictés par le règlement de l'entreprise.
2. Sauvegarder les données en lieu sûr (base d'informations centralisée) pour conserver une copie récente.
3. Se doter d'une solution de chiffrement (on parle aussi de cryptage) du disque dur et des données pour éviter toute consultation et exploitation par des tiers non-autorisés en cas de vol ou de perte.
4. Minimiser les risques en n'emportant avec soi que les seules données nécessaires.
5. Eviter l'emploi de toute connexion Internet "sensible" comme les messageries publiques ou instantanées, qui véhiculent en permanence des codes malveillants.
6. Ne laisser aucune trace de ses données personnelles après envoi (suppression des pièces jointes et du message).

Le collaborateur doit garder en mémoire qu'il est responsable des données perdues ou volées avec à la clé des conséquences financières directes, voire des mesures prises à son encontre (mise à pied, licenciement). Une grande vigilance s'impose donc !

SecureCloud™, la plate-forme de sécurité SaaS* de Trend Micro

* Software as a Service

Qu'elles disposent ou non de ressources informatiques, de plus en plus d'entreprises se tournent aujourd'hui vers un modèle SaaS et choisissent d'externaliser leur sécurité pour bénéficier de mises à jour en temps reel. Pour répondre à cette tendance, Trend Micro met ses solutions de protection à la portée de toutes les entreprises à travers son offre SecureCloud. Cette plateforme de sécurité SaaS propose aux entreprises de toute taille des solutions de protection contre les menaces liées au courrier électronique et au Web.

SECURECLOUD POUR ALLÉGER LE TRAVAIL DES ÉQUIPES INFORMATIQUE

SecureCloud héberge des services qui bloquent les menaces « in the cloud » (au niveau d'Internet). Ainsi, elles ne peuvent pénétrer les réseaux des clients et endommager l'infrastructure informatique. Les clients et les partenaires du réseau de distribution centralisent la gestion de ces services depuis la console Web de SecureCloud, ce qui simplifie l'administration et coordonne la gestion des risques.

SecureCloud est la plate-forme de gestion intégrée avec les services de Trend Micro. Sa console d'administration à connexion unique montre tout son intérêt lorsque l'on utilise plusieurs services Trend Micro.

Le SaaS permet de maintenir les menaces à l'écart du réseau tout en se déployant aisément, sans avoir besoin de changer l'infrastructure en place. De ce fait, l'équipe informatique peut se consacrer à d'autres projets. Ainsi, Trend Micro fournit un portail en ligne pour l'administration centralisée de tous les services SecureCloud. Cette plate-forme gère les règles de sécurité pour toutes les solutions, de la passerelle à l'ordinateur de bureau. Elle utilise les moteurs d'analyse de Trend Micro et ses méthodes de protection contre les menaces.

SecureCloud s'appuie sur l'expertise de Trend Micro en matière de sécurité, la maintenance et la surveillance étant effectuées par ses équipes. Totalement évolutif, il permet d'ajouter de nouveaux services et utilisateurs en fonction des besoins. Ainsi, il simplifie l'administration et permet de coordonner la gestion des risques pour les divers services. Enfin, il offre une plate-forme de gestion intégrée des services.

LES TECHNOLOGIES ET LES SOLUTIONS SaaS

1 - Email Reputation Services
Unique service d'évaluation de réputation des messages électroniques à proposer une console d'administration, ERS permet de consulter des rapports en temps réel sur l'activité des spams.

2 - Botnet Identification Service
Ce service identifie et contrôle les PCs zombies. Il leur devient alors impossible de générer des spams et de lancer des attaques criminelles susceptibles de nuire à votre image de marque, et de dégrader les performances du réseau.

3 – Web Reputation Service
Cette fonction vous protège contre les attaques de type « zero-day » avant qu'elles ne puissent atteindre votre réseau. En les analysant, en fournissant des mises à jour continues et instantanées et des informations actualisées sur la réputation des sites, Trend Micro évalue le degré de confiance d'un site Web, d'une page ou d'un lien avant que l'utilisateur ne clique dessus.

4 - InterScan Messaging Hosted Security
Cette solution intègre des systèmes anti-spam et anti-phishing combinés à une technologie antivirus et anti-spyware primée. Ce système hébergé complet de sécurité de messagerie bloque les menaces avant qu'elles n'atteignent le réseau. Les entreprises peuvent choisir entre une administration simplifiée, ou un accès et un contrôle granulaires. Quel que soit le niveau sélectionné, la gestion s'effectue via une console unique à interface Web. ■

QUAND LES NAVIGATEURS PERDENT LA TÊTE

Par Adrien Guinault, Xmco Partners ▶

Petko D. Petkov, plus connu comme le fondateur du groupe Gnucitizen Cutting Edge Think tank, a présenté durant la Black Hat Amsterdam un florilège des vulnérabilités découvertes par son groupe durant l'année 2007 et en janvier 2008. Pour les fans de son blog, rien de nouveau, par contre les autres ont été de surprises en « effrois »… car aujourd'hui les pirates au travers des navigateurs ciblent les utilisateurs finaux.

Petko Petkov, chercheur et consultant, s'est bâti une solide réputation dans le milieu de la sécurité, en participant à de nombreux ouvrages, ainsi qu'en publiant, chaque jour sur son blog **[1]**, des réflexions sur de nouveaux axes d'attaque ou encore des vulnérabilités "0-day" toujours accompagnées de preuves de concepts intéressantes.
Après avoir consacré une bonne partie de son temps dans la recherche de nouvelles vulnérabilités, Petko a donc choisi de résumer et décrire les différentes vulnérabilités découvertes au long de l'année 2007 par le groupe Gnucitizen Ethical Hacker.
Les passionnés et adeptes de son blog n'ont, certes, rien appris de nouveau en assistant à cette présentation. Cependant, les autres ont pu découvrir les nombreux problèmes dont souffre la partie cliente du modèle client/serveur, appliquée aussi bien aux logiciels (navigateur Internet par exemple) qu'aux ordinateurs, considérés également comme des clients d'un réseau.

Quatre grands thèmes ont été abordés brièvement durant son intervention. Le but n'était pas de présenter toutes les vulnérabilités découvertes l'année passée, mais plutôt de dresser un constat alarmant dans quatre domaines distincts avec des preuves de concept simples.

Cross Site Request Forgery, 4 méthodes pour forcer un navigateur à agir à « l'insu de son plein gré »

Le premier sujet traité concernait les attaques CSRF (Cross Site Request Forgery). Ce type d'attaque largement exploité sur Internet a pour but de forcer un navigateur à exécuter des commandes ciblées à l'insu de la victime **[2]**.
Pour cela, Petko a décortiqué plusieurs vulnérabilités. Les plus intéressantes furent découvertes en septembre 2007 et janvier 2008.
La première, baptisée "Hijack Gmail" **[3]**, consistait à installer une backdoor au sein d'un compte Gmail. En incitant un utilisateur à suivre un lien malicieux, le pirate pouvait ajouter, à l'insu de sa victime, un filtre Gmail qui transférait ensuite tous les emails reçus vers l'adresse du pirate. Cette faille de sécurité, corrigée rapidement par Google, avait permis à l'époque de pirater le compte Gmail d'un célèbre designer graphique. Le pirate avait pu lire les emails de sa victime et demander à son hébergeur de libérer le nom de domaine.

Toujours dans le même registre, des recherches poussées ont été menées sur le routeur le plus utilisé en Angleterre : BT Home hub afin de dresser un bilan inquiétant sur la sécurité des routeurs personnels.
Plusieurs erreurs d'autorisation permettent encore aujourd'hui de contourner l'authentification de l'interface Web du routeur et de modifier sa configuration via une simple URL. Les attaques CSRF prennent ici tout leur sens et deviennent alors particulièrement utiles et dangereuses. Un lien HTML pourrait reconfigurer totalement le routeur en question. Le pirate peut donc aisément changer, par exemple, la configuration DNS afin de rediriger le trafic vers des serveurs pirates ou encore activer l'administration via Internet…
Une autre étude a également pointé du doigt les lacunes du protocole UpNp en présentant les techniques d'attaques associées. En étudiant avec attention un routeur implémentant UpNp, Petko a prouvé comment une simple requête SOAP camouflée au sein d'une animation flash pouvait reconfigurer n'importe quel routeur de ce type **[4]**.

Les vulnérabilités « Command/Shell fixation attack » pour contrôler QuickTime et Firefox

Dans un second temps, Petko s'est intéressé aux vulnérabilités appelées "Command/Shell fixation attack". Ce terme désigne les erreurs de validation que l'on peut retrouver au sein de nombreux logiciels permettant de passer des commandes système, sans contrôle préalable.
Un tel bug lors du traitement de liens QTL (QuickTime Media Link) insérés au sein de pages HMTL avait été découvert en septembre 2007. Cette célèbre vulnérabilité affectait conjointement Firefox et QuickTime **[5]**. En effet, QuickTime ne contrôlait pas correctement les URLs passées au sein du paramètre "qtnext" lors de l'appel de fichier QuickTime intégré au sein de pages HMTL.
L'ouverture d'une telle page Web incluant un lien QTL malicieux permettait alors d'exécuter un code JavaScript pour faire appel à des fonctions Firefox, telles que 'ShellExecute'.

Cette utilisation conjointe de QuickTime et de Firefox permettait à l'époque de prendre le contrôle d'une machine vulnérable.
Petko a également mis en évidence d'autres problèmes liés au traitement des fichiers '.RDP' (Bureau à distance) ou '.ICA' (Citrix) [6]. En effet, certaines propriétés méconnues pouvaient être insérées au sein d'un fichier de connexion RDP ou ICA afin de lancer des commandes lors d'une connexion distante à un serveur Windows ou Citrix. Toute la difficulté de l'attaque consistait alors à inciter une victime (possédant un compte sur un serveur Windows ou Citrix) à ouvrir un fichier de ce type.
D'autres problèmes de ce type ont également été rapidement traités (Cross Site Scripting via Skype [7], utilisation de la fonction chrome au sein de Firefox [8]…).

L'avenir des pirates appartiendra au Web 2.0

Enfin, la présentation de Petko s'est terminée sur les différentes possibilités d'utilisations malicieuses du protocole JAR [9] ainsi que sur une réflexion à propos de la future génération de rootkits. Petko prévoit un développement de rootkit de 4ème génération. Intégrés au sein des navigateurs, ils utiliseront les nouveautés du Web 2.0.
Au travers d'exemples précis, de preuves de concept variées et d'explications détaillées, Petko a voulu mettre l'accent sur les nouvelles menaces dont sont victimes les applications clients au sens large. Les pirates concentrent de plus en plus leurs efforts sur ce genre de vulnérabilités afin de cibler les "end users".
La sécurité des applications client et, en particulier, celle des navigateurs doit donc être au centre des préoccupations au même titre que la sécurité des serveurs. ■■■

[1] http://www.gnucitizen.org/blog
[2] http://fr.wikipedia.org/wiki/Cross-Site_Request_Forgeries
[3] http://www.gnucitizen.org/blog/google-gmail-e-mail-hijack-technique/
[4] http://www.gnucitizen.org/blog/hacking-with-upnp-universal-plug-and-play/
[5] http://www.gnucitizen.org/projects/0day-quicktime-pwns-firefox/
[6] http://www.gnucitizen.org/blog/remote-desktop-command-fixation-attacks/
[7] http://www.gnucitizen.org/blog/vulnerabilities-in-skype/
[8] http://www.gnucitizen.org/projects/firebug-goes-evil/
[9] http://www.gnucitizen.org/blog/severe-xss-in-google-and-others-due-to-the-jar-protocol-issues/

MALTEGO : L'INVESTIGATEUR DU WEB

Par Thomas Gayet, Cert-Lexsi ▶

Un peu en marge des sujets traditionnels que l'on peut attendre lors de la Black Hat Conference, une présentation de la société Paterva a eu pour but de discuter de la recherche d'informations ciblées par Internet sur des entreprises ou des personnes. En effet, le risque induit par les fuites d'information, qu'elles soient délibérées ou non, est aujourd'hui bien connu des entreprises. Pour autant, répondre à cette menace n'est pas une chose aisée, tant on se bat encore et toujours contre les menaces traditionnelles qui pèsent sur un Système d'Information, telles les attaques externes mettant en œuvre des techniques de hacking bien connues et balisées.

Si on souhaite se faire une idée, ou finalement établir un rapide bilan des informations déjà publiées sur une personne ou sur une entreprise, cette présentation de l'outil Maltego de la société Paterva aurait provoqué chez vous, comme chez tous ceux qui y ont assistés, une envie de trouver rapidement une machine connectée et de tester cet outil.
De même, tous ceux qui ont déjà eu l'occasion d'effectuer des investigations en ligne sur des personnes ou des « éléments Internet » (Adresse IP, noms de domaine, etc.) ont tout de suite vu l'intérêt d'un tel outil, notamment dans la rapidité avec laquelle il peut vous fournir les informations intéressantes.

Comment retrouver rapidement des informations ciblées sur le Web

Le constat initial de Paterva est finalement très simple : si l'être humain est efficace pour distinguer un motif dans un ensemble, la machine est rapide pour traiter de gros volumes de données. La réciproque n'étant pas vraie, une voie médiane devait être possible pour permettre à l'homme d'exploiter les caractéristiques de la machine dans la recherche efficace d'informations.
Autrement dit, de nombreuses informations sur une personne ou une entreprise étant publiées sur le Web, encore faut-il une solution pour tirer, de cette masse de données, des informations pertinentes ou à valeur ajoutée, et cela dans un temps relativement restreint.

Maltego pour récolter facilement des informations sur le Web

C'est là qu'intervient l'outil Maltego, en réalité sujet principal de cette présentation, développé pour récolter et traiter, à partir de points de départ précis, des informations intéressantes, les liens souvent invisibles qui les relient entre elles, et surtout de les présenter dans un format commode et exploitable par l'utilisateur.
Concrètement, par le biais de l'interface graphique mise à disposition, il est possible de choisir comme élément de départ un nom de domaine, un site Web, une adresse IP, un « netblock » ou encore une identité, sur lesquels l'outil va appliquer des transformations. Ces sortes de plugins vont alors effectuer une recherche d'information à partir de la donnée initiale, et représenter graphiquement le lien entre la source fournie et l'information obtenue.
Par exemple, d'un nom de domaine sera identifié les adresses IPs correspondantes, puis le « netblock » associé, et pourquoi pas les autres domaines présents sur ces adresses. Le test effectué « en live » par les présentateurs à partir de l'information

« blackhat.com » était parfaitement concluant, et a eu le mérite de provoquer des sourires et des étonnements dans la salle, au vu des informations obtenues.
En effet, un joli graphique s'est alors dessiné à l'écran, identifiant et montrant les liens entre des informations aussi diverses que des noms de domaine, des adresses de courriels, des adresses IPs, des identités, des documents ou encore des clefs GPG, et le tout sous la forme d'un arbre structuré très rapidement construit.

Quelques plugins et une recherche massive sur Yahoo…

Pour réaliser ce travail, les plugins de transformations de l'outil vont chercher des données sur différentes sources spécialisées (tels que les sites sociaux et autres Web 2.0, serveur Whois, etc.), mais exploite également massivement le moteur de recherche Yahoo. Pourquoi Yahoo ? Car Google n'a pas accepté les demandes de Paterva qui aurait souhaité pouvoir effectuer, de manière -selon eux - raisonnable, des requêtes sur le célèbre moteur de recherche.
Bien évidemment cette problématique est connue, car envoyer des requêtes en masse vers de tels sites est en principe prohibé. Paterva propose donc une nouvelle architecture, pour la seconde version de son outil bientôt téléchargeable, où les plugins de transformations ne sont plus directement utilisés par le logiciel client, mais sont exécutés de manière distribuée, depuis des serveurs appelés serveurs de transformation.

…et les sites sociaux sont une nouvelle fois un outil de recherche utile mais permettant aussi éventuellement de manipuler les opinions

Dans la même idée, une hypothèse – pour ne pas dire un contournement … – a également été présentée pour extraire les informations des sites sociaux, à travers la création de multiples identités fictives (des « bots ») à partir desquelles les recherches seraient effectuées. Les présentateurs en ont alors profité pour nous faire imaginer comment et combien il est possible de manipuler des opinions par ce biais, en créant par exemple des commentaires positifs / négatifs sur des blogs, en surveillant la présence de personnes sur le Web par l'étude de leurs statuts de clients de messagerie instantanée, ou encore en récupérant les liens créés entre les personnes sur les sites sociaux.
Cette présentation, quoi qu'un peu trop centrée sur l'outil Maltego, avait donc le mérite de démontrer la facilité, avec les outils appropriés, d'obtenir quantité d'informations sur les personnes ou les entreprises et les liens entre eux, ainsi que de mettre en garde sur les dangers de l'existence même de tels outils à travers tout ce que l'on peut imaginer comme usage malveillant.

JUIN

10 juin – Maison de l'Amérique Latine, Paris
CSO Interchange
Web : www.csointerchange.org

10 - 12 juin - Toronto (Canada)
Infosecurity Canada
Tél. : 416.756.0303
Web : www.infosecuritycanada.com

11 - 12 juin - Palacio de Congresos, Madrid (Espagne)
Infosecurity Ibéria Spain
Tél. : +34 93 45 20 722
E-mail : infosecurity@reediberia.com
Web : www.infosecurity.com.es

11 - 12 juin - Centre Etoile Saint-Honoré, Paris
Forum IDC « Telecoms et Entreprises »
IDC - Valérie Rolland
Tél. : 01 55 39 61 24
E-mail : vrolland@idc.com
Web : www.idc.com/france/events/forum-telecoms08/index.jsp

11 - 12 juin - Grand Palais, Lilles
ICTF : l'International Contactless Technologies Forum
Tél. : 01 42 46 21 21
Web : www.ictf-forum.com

12 juin - Prim'X Trocadéro, Paris
Matinée Aladdin, OpenTrust et Prim'X Technologies: « Trois clés de succès d'un projet de sécurité »
Web : www.primx.eu/matinee_primx_renault.aspx

18 - 19 juin - Casablanca (Maroc)
Med-IT@Casablanca
XCOM
Tél. : +33 (0)4 42 70 00 66
Sylvie Reforzo
Tél. : +33 (0)4 42 70 95 10
Mob : +33 (0)6 62 48 22 29
E-mail : sreforzo@xcom.fr
Web : www.xcom.fr

19 juin - Hôtel Le Parc - Trocadéro, Paris
Business Intelligence
IDC - Valérie Rolland
Tél. : 01 55 39 61 24
E-mail : vrolland@idc.com
Web : www.idc.com/france/events/bi08/index.jsp

19 juin - Maison des Arts et Métiers, Paris
Séminaire Forensics Verizon Business
E-mail : France-marketing@fr.verizonbusiness.com

23 au 27 juin - HSC Levallois-Perret
HSC : Formation RSSI
Lynda Benchikh
Tél. : +33 141 409 704
E-mail : formations@hsc.fr
Web : www.hsc.fr/services/formations/formationsRSSI.html.fr

24 - 26 juin - Tel Aviv (Israël)
Security Israël
Tél. : +972 3 648 9339
E-mail : sigmatim@netvision.net.il
Web : www.securityisrael.com ou www.idc.lic.org

30 juin au 4 juillet - Hôtel Novotel Centre Acropolis, Nice
HSC : Formation certifiante ISO 27001 Lead Auditor
Lynda Benchikh
Tél. : +33 141 409 704
E-mail : formations@hsc.fr
Web : www.hsc.fr/services/formations/certification_iso27001.html.fr

30 juin au 4 juillet - HSC Levallois-Perret
HSC : formation pratique aux Tests d'Intrusion
Lynda Benchikh
Tél. : +33 141 409 704
E-mail : formations@hsc.fr
Web : www.hsc.fr/fti

AOUT

2 - 7 août - Las Vegas (USA)
Black Hat Training & Briefings USA
E-mail : rossi@montaramountain.com
Web : www.blackhat.com

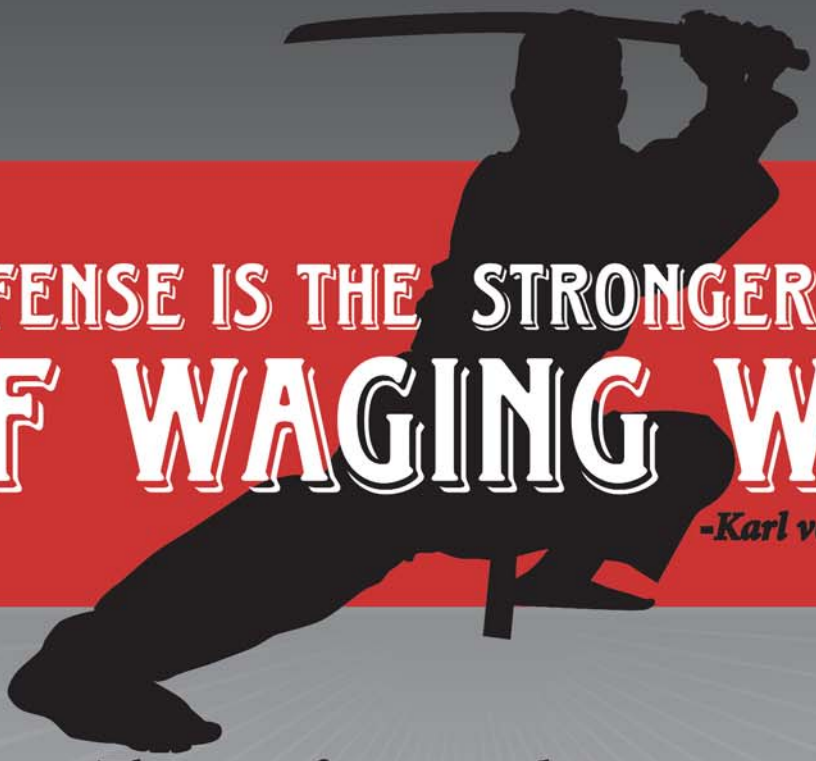
SEPTEMBRE

16 - 19 septembre - Sophia Antipolis
Smart Event
Web : www.strategiestm.com/-Evenements-.html

18 septembre - Espace Georges V, Paris
Eurosec
Web : www.forum-eurosec.com

30 septembre - 2 octobre - CNIT Paris La Défense
E-Procurement - ERP - MVI - SOLUTIONS CRM - Serveurs & Applications
Infopromotions
Tél. : +33(0) 1 44 39 85 00
E-mail : info@infopromotions.fr
Web : www.groupesolutions.com

Black Hat USA 2008



"DEFENSE IS THE STRONGER FORM OF WAGING WAR"

-Karl von Clausewitz

The war for your data rages on.
Be certain your defenses are up to the job.

Black Hat USA convenes the best infosec minds on the planet for six days of intense, hands-on security education and peer-to-peer networking. Our speakers and trainers are the world's leading voices from academia, research and the underground. The breadth and depth of topics is unmatched. You will gain actionable knowledge, discover new tools, and learn expert techniques for digital self defense.

12 tracks **80** presentations **40** training sessions

August 2-7 2008
Caesars Palace

Black Hat
BRIEFINGS AND TRAINING
www.blackhat.com

Las Vegas
Nevada, USA

Diamond Sponsor: Microsoft

Platinum Sponsors: Cisco, Qualys

Gold Sponsors: Configuresoft, Core Security Technologies, Google, IOActive, Norman

Silver Sponsors: ArcSight, Breach, BigFix, Cenzic, edgeos, Fortify, HP, nCircle, NetWitness, Ounce Labs, Radware, SAINT, SecureWorks, Soteria, StillSecure, Tipping Point

Pour le e-commerce :

Pour de nouveaux partenariats :

Pour la mobilité de vos équipes :

Pour vos solutions réseaux :

Pour votre prochain audit de sécurité :

Communiquez et échangez :

En toute confiance.

VERIZON BUSINESS SOLUTIONS DE SECURITE OPERE PAR CYBERTRUST.

Une couverture Internet mondiale associée à 15 années d'expertise dans la sécurité de l'information.

Verizon Business peut vous aider à protéger vos données critiques, et préserver la confiance de vos clients, depuis vos équipements, à travers vos réseaux et partout dans le monde. C'est l'association unique d'un réseau IP mondial à 15 années d'expertise en sécurité—dans les domaines de l'infogérance de services de sécurité, la gestion des identités électroniques et l'investigation—qui nous ont permis de gagner la confiance de milliers de clients dans le monde, y compris 72% des entreprises Fortune 100. Nous possédons l'expertise pour vous accompagner, en toute sécurité et en toute confiance.

Découvrez comment sur : verizonbusiness.com

verizonbusiness

Security Solutions powered by Cybertrust